Web 应用程序报告

该报告包含有关 web 应用程序的重要安全信息。

安全报告

该报告由 IBM Security AppScan Standard 创建 9.0.3, 规则： 1957
扫描开始时间： 2019/6/24 10:53:44

目录

修订建议

- 查看危险字符注入的可能解决方案
- 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。
- Configure your server to allow only required HTTP methods
- 登录之后更改会话标识符值
- Config your server to use the "Content-Security-Policy" header
- Config your server to use the "X-Content-Type-Options" header
- Config your server to use the "X-XSS-Protection" header
- 除去 HTML 注释中的敏感信息
- 除去虚拟目录中的旧版本文件
- 将“autocomplete”属性正确设置为“off”
- 将适当的授权应用到管理脚本
- 请勿接受在查询字符串中发送的主体参数
- 验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

咨询

- 使用 SQL 注入的认证旁路
- 已解密的登录请求
- Authentication Bypass Using HTTP Verb Tampering
- 会话标识未更新
- Missing "Content-Security-Policy" header
- Missing "X-Content-Type-Options" header
- Missing "X-XSS-Protection" header
- 查询中接受的主体参数
- 归档文件下载
- 检测到文件替代版本
- 临时文件下载
- 直接访问管理页面
- 自动填写未对密码字段禁用的 HTML 属性
- HTML 注释敏感信息泄露
- 应用程序错误

应用程序数据

- cookie
- JavaScript
- 参数
- 注释
- 已访问的 URL
- 失败的请求
- 已过滤的 URL

介绍

该报告包含由 IBM Security AppScan Standard 执行的 Web 应用程序安全性扫描的结果。

高严重性问题：	5
中等严重性问题：	12
低严重性问题：	107
参考严重性问题：	3
报告中包含的严重性问题总数：	127
扫描中发现的严重性问题总数：	127

一般信息

扫描文件名称：	重点污染源自动监控企业端
扫描开始时间：	2019/6/24 10:53:44
测试策略：	Default
主机	172.20.7.168
操作系统：	未知
Web 服务器：	Apache
应用程序服务器：	任何

登陆设置

登陆方法：	记录的登录
并发登陆：	已启用
JavaScript 执行文件：	已启用
会话中检测：	已启用
会话中模式：	>退出
跟踪或会话标识 cookie：	JSESSIONID
跟踪或会话标识参数：	j_logintype _ _ search_mpId search_psID search_regionCode

search_startTime
search_endTime
search_pollutants

_
search_startTime
search_endTime

登陆序列：

http://172.20.7.168:8083/amOnline/app/AppLogin.page
http://172.20.7.168:8083/amOnline/app/j_spring_security_check
http://172.20.7.168:8083/amOnline/app/AppMain.page
http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!listPsInfo.page?psid=&_=1561344683129
http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!getPollutantsWithPsID.page?psID=510101055565
http://172.20.7.168:8083/amOnline/app/mpoint/mpAction!getMpByPS_ID.page?psid=510101055565&_=1561344693179
http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!getHistData.page?PageNo=1&PageSize=10000000&search_mpId=51010105556514&search_mpType=4&search_psID=510101055565&search_regionCode=510101000&search_startTime=2019-06-18+00:00:00.000&search_endTime=2019-06-24+10:51:34&search_dataType=1&search_pollutants=060,B01,072,001,101,011&search_incineratorFlag=0&_=1561344693180
http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!findAcceptInfos.page
http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!findStopInfos.page
http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!list.page
http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page
http://172.20.7.168:8083/amOnline/app/account/accountAction!list.page
http://172.20.7.168:8083/amOnline/app/account/accountAction!jsonList.page

摘要

问题类型 15

TOC

	问题类型	问题的数量
高	使用 SQL 注入的认证旁路	1
高	已解密的登录请求	4
中	Authentication Bypass Using HTTP Verb Tampering	11
中	会话标识未更新	1
低	Missing "Content-Security-Policy" header	17
低	Missing "X-Content-Type-Options" header	17
低	Missing "X-XSS-Protection" header	17
低	查询中接受的主体参数	2
低	归档文件下载	5
低	检测到文件替代版本	13
低	临时文件下载	23
低	直接访问管理页面	12
低	自动填写未对密码字段禁用的 HTML 属性	1
参	HTML 注释敏感信息泄露	2
参	应用程序错误	1

有漏洞的 URL 25

TOC

	URL	问题的数量
高	http://172.20.7.168:8083/amonline/app/j_spring_security_check	9
高	http://172.20.7.168:8083/amonline/app/applogin.page	9
中	http://172.20.7.168:8083/amonline/app/abnormity/admin/abnormityaction!jsonlist.page	5
中	http://172.20.7.168:8083/amonline/app/abnormityadmin/abnormityaction!jsonlist.page	5
中	http://172.20.7.168:8083/amonline/app/monitorspot/admin/spotaction!findacceptinfos.page	5

中	http://172.20.7.168:8083/amonline/app/monitorspot/admin/stopaction!findstopinfos.page	5
中	http://172.20.7.168:8083/amonline/app/monitorspotadmin/spotaction!findacceptinfos.page	5
中	http://172.20.7.168:8083/amonline/app/monitorspotadmin/stopaction!findstopinfos.page	5
中	http://172.20.7.168:8083/amonline/app/onlinemon/admin/onlineaction!getpollutantswithpsid.page	5
中	http://172.20.7.168:8083/amonline/app/onlinemonadmin/onlineaction!getpollutantswithpsid.page	5
中	http://172.20.7.168:8083/amonline/app/psinfo/admin/psinfo!listpsinfo.page	5
中	http://172.20.7.168:8083/amonline/app/psinfoadmin/psinfo!listpsinfo.page	5
低	http://172.20.7.168:8083/amonline/app/abnormity/abnormityaction!jsonlist.page	7
低	http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!findacceptinfos.page	7
低	http://172.20.7.168:8083/amonline/app/monitorspot/stopaction!findstopinfos.page	7
低	http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!getpollutantswithpsid.page	7
低	http://172.20.7.168:8083/amonline/app/psinfo/psinfo!listpsinfo.page	7
低	http://172.20.7.168:8083/amonline/app/account/accountaction!list.page	3
低	http://172.20.7.168:8083/amonline/app/loginfo/loginfoaction!list.page	3
低	http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!list.page	3
低	http://172.20.7.168:8083/amonline/app/monitorspot/stopaction!list.page	3
低	http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!history.page	3
低	http://172.20.7.168:8083/amonline/app/psinfo/psinfo!view.page	3
低	http://172.20.7.168:8083/amonline/app/revisedmanage/revisedaction!list.page	3
低	http://172.20.7.168:8083/amonline/app/appmain.page	3

修订建议 13

TOC

	修复任务	问题的数量
高	查看危险字符注入的可能解决方案	1
高	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。	4
中	Configure your server to allow only required HTTP methods	11
中	登录之后更改会话标识符值	1
低	Config your server to use the "Content-Security-Policy" header	17
低	Config your server to use the "X-Content-Type-Options" header	17
低	Config your server to use the "X-XSS-Protection" header	17

低	除去 HTML 注释中的敏感信息	2
低	除去虚拟目录中的旧版本文件	41
低	将“autocomplete”属性正确设置为“off”	1
低	将适当的授权应用到管理脚本	12
低	请勿接受在查询字符串中发送的主体参数	2
低	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常	1

安全风险 8

TOC

	风险	问题的数量
高	可能会绕开 Web 应用程序的认证机制	2
高	可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息	4
中	可能会升级用户特权并通过 Web 应用程序获取管理许可权	23
中	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置	79
中	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务	1
低	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息	53
低	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息	28
参	可能会收集敏感的调试信息	1

原因 8

TOC

	原因	问题的数量
高	未对用户输入正确执行危险字符清理	1
高	诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递	4
中	Web 应用程序编程或配置不安全	66
低	在生产环境中留下临时文件	41
低	Web 服务器或应用程序服务器是以不安全的方式配置的	12
参	程序员在 Web 页面上留下调试信息	2
参	未对入局参数值执行适当的边界检查	1
参	未执行验证以确保用户输入与预期的数据类型匹配	1

WASC 威胁分类

TOC

威胁	问题的数量
传输层保护不足	4
会话定置	1
可预测资源位置	40
认证不充分	12
信息泄露	70

按问题类型分类的问题

高 使用 SQL 注入的认证旁路 1 TOC

问题 1 / 1 TOC

使用 SQL 注入的认证旁路

严重性:	高
CVSS 分数:	9.0
URL:	http://172.20.7.168:8083/amonline/app/j_spring_security_check
实体:	j_password (Parameter)
风险:	可能会绕开 Web 应用程序的认证机制
原因:	未对用户输入正确执行危险字符清理
固定值:	查看危险字符注入的可能解决方案

差异: **cookie** 已从请求除去: `57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去: `front_user`
参数 从以下位置进行控制: `13981937605` 至: `4ppSc4n`
参数 从以下位置进行控制: `hfjcd` 至: `4ppSc4n`
参数 从以下位置进行控制: `hfjcd` 至: `A%27+OR+%277659%27%3D%277659`
参数 从以下位置进行控制: `hfjcd` 至: `s3ct3amy`

推理: 测试结果似乎指示存在脆弱性，因为在发送四种类型的请求（有效登录、无效登录、SQL 攻击和另一个无效登录）时，两个无效登录的响应相同，而 SQL 攻击的响应似乎与有效登录的响应类似。

测试请求和响应:

```
POST /amOnline/app/j_spring_security_check HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/AppLogin.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
```

```
Content-Length: 39

j_username=13981937605&j_password=hfjcd

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=ISO-8859-1
Content-Length: 61
Date: Mon, 24 Jun 2019 03:54:08 GMT
Set-Cookie: JSESSIONID=6993440D022BCC5B7FC8A795591A8460; Path=/amOnline; HttpOnly

{
 "result": "success",
 "targetUrl": "/amOnline/app/AppMain.page"
}

POST /amOnline/app/j_spring_security_check HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/AppLogin.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
Content-Length: 37

j_username=4ppSc4n&j_password=4ppSc4n

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 136
Date: Mon, 24 Jun 2019 03:54:08 GMT
Set-Cookie: JSESSIONID=452DB504E7F4B4962319E1CE7FD1661B; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       用户不存在,请联系客服帮您解决"
}

POST /amOnline/app/j_spring_security_check HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/AppLogin.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
Content-Length: 62

j_username=13981937605&j_password=A%27+OR+%277659%27%3D%277659

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=ISO-8859-1
Content-Length: 61
Date: Mon, 24 Jun 2019 03:54:08 GMT
Set-Cookie: JSESSIONID=150F62850C5663D09B0CC496DB346E56; Path=/amOnline; HttpOnly

{
 "result": "success",
 "targetUrl": "/amOnline/app/AppMain.page"
}

POST /amOnline/app/j_spring_security_check HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/AppLogin.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
```

```
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
Content-Length: 38

j_username=4ppSc4n&j_password=s3ct3amy

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 136
Date: Mon, 24 Jun 2019 03:54:08 GMT
Set-Cookie: JSESSIONID=F0598FAE1CD7BE312D16F9AB32CB943A; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       用户不存在,请联系客服帮您解决"
}
```

高 已解密的登录请求 4 TOC

问题 1 / 4 TOC

已解密的登录请求	
严重性:	高
CVSS 分数:	8.5
URL:	http://172.20.7.168:8083/amonline/app/j_spring_security_check
实体:	j_spring_security_check (Page)
风险:	可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息
原因:	诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递
固定值:	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异:

推理: AppScan 识别了不是通过 SSL 发送的登录请求。

测试请求和响应:

```
POST /amOnline/app/j_spring_security_check HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: hasshown=1; JSESSIONID=4801DD573D4D329FBF176E117991946F
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppLogin.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Content-Length: 123

j_logintype=front_user&j_lt=2c9487286b79d3e4016b8767113e12eb&j_slt=&loginType=front&j_username=1.
..
```

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: /amOnline/app/AppMain.page
Content-Length: 0
Date: Mon, 24 Jun 2019 02:53:27 GMT
Set-Cookie: JSESSIONID=898FFF2A3BE84AF807D06E6FBED6B74D; Path=/amOnline; HttpOnly



GET /amOnline/app/AppMain.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=AE1E776BF33CD2F26A4429E80DCAFFAA
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 02:53:27 GMT
x-ua-compatible: IE=edge,chrome=1

<!DOCTYPE html>
<html lang="zh-cn">
<head>
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
    <title>重点排污单位自动监控与基础数据库系统（企业端）</title>
    <link rel="stylesheet" href="/amOnline/static/layui/css/layui.css"  media="all">
    <style>
        .layui-body{
            left:0px;
        }
        .layui-side{
            width:0px;
        }
        .layui-layout-admin .layui-body{
            bottom:0px;
        }
    </style>

</head>
<body class="layui-layout-body">
<div class="layui-layout layui-layout-admin">
    <div class="layui-header layui-bg-blue">
        <div class="layui-logo">重点排污单位自动监控与基础数据库系统(企业端)</div>
        <!-- 头部区域（可配合layui已有的水平导航） -->
        <ul class="layui-nav layui-layout-right    layui-bg-blue">
            <li class="layui-nav-item layui-this"><a href="#"
onclick="loadIframe('app/psinfo/psInfo!view.page')">基本信息维护</a></li>
            <li class="layui-nav-item"  id="historyLine"><a href="#"
onclick="loadIframe('app/onlinemon/onlineAction!history.page')">数据监控</a></li>

            <li class="layui-nav-item">
                <a href="javascript:;">现场端管理</a>
                <dl class="layui-nav-child" id="xcdzhgl">
                    <dd><a href="#" onclick="loadIframe('app/monitorspot/spotAction!list.page')">
设备验收</a></dd>
                                <dd><a href="#"
onclick="loadIframe('app/monitorspot/stopAction!list.page')">停运管理</a></dd>
                                <!--<dd><a href="#"
onclick="loadIframe('app/viewmonitor/monitorDataAction!list.page')">信息填报</a></dd>   -->
                </dl>
            </li>
            <li class="layui-nav-item" id='reviseLi'><a href="#"
onclick="loadIframe('app/revisedmanage/revisedAction!list.page')">数据标记</a></li>
          <!--  <li class="layui-nav-item" ><a href="#"
onclick="loadIframe('app/revisedmanage/revisedAction!list.page')">数据标记</a></li>
            <li class="layui-nav-item" ><a href="#"
onclick="loadIframe('http://m.envsc.cn/WXIndexPSForQYD.aspx?
key=wPLFgACAKGA&pscode=140000000223&... -->
            <li class="layui-nav-item">
                <a href="javascript:;">
```

```
                    <img src="/amOnline/static/layui/images/ooopic_1509436490.png" class="layui-
nav-img">
                    黄智欢
                </a>
                <dl class="layui-nav-child">
                    <dd><a  href="#" onclick="loadIframe('app/account/accountAction!list.page')">
账户管理</a></dd>
                    <dd><a  href="#" onclick="loadIframe('app/loginfo/loginfoAction!list.page')">
操作日志</a></dd>
                    <dd><a onclick="logoutSys()" href="javascript:void(0);"  >退出系统</a></dd>
                </dl>
            </li>


        </ul>
    </div>


    <div class="layui-body">
        <iframe id="frame_lgpblpww"   src="/amOnline/app/psinfo/psInfo!view.page"
                style='width:100%; margin-right:-15px!important;margin-bottom:-14px!important;
overflow-y:scroll; overflow-x:hidden;'     >  </iframe>
    </div>



</div>
<script src="/amOnline/static/layui/layui.js" charset="utf-8"></script>
<!-- 注意：如果你直接复制所有代码到本地，上述js路径需要改成你本地的 -->
<script>


    layui.use('element', function(){
        var element = layui.element; //导航的hover效果、二级菜单等功能，需要依赖element模块

        //监听导航点击
        element.on('nav(demo)', function(elem){
            layer.msg(elem.text());
        });
    });

    function changeFrameHeight(){
        var ifm= document.getElementById("frame_lgpblpww");
        ifm.height=
...
...
...
```

问题 2 / 4

TOC

已解密的登录请求	
严重性：	高
CVSS 分数：	8.5
URL：	http://172.20.7.168:8083/amonline/app/applogin.page
实体：	comfirmPwd (Parameter)
风险：	可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息
原因：	诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递
固定值：	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异：

推理： AppScan 识别了不是通过 SSL 发送的密码参数。

测试请求和响应：

```
POST /amOnline/app/AppLogin.page?loginError=auth_failed HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: hasshown=1; JSESSIONID=4801DD573D4D329FBF176E117991946F
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppLogin.page?loginError=auth_failed
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Content-Length: 187

loginType=front&j_lt=2c9487286b79d3e4016b8767117d12ed&cmUsername=1234&verificationCode=1234&logi.
..

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 02:53:27 GMT
Set-Cookie: JSESSIONID=167E4BA3604AB80CF03E4E18B0398447; Path=/amOnline; HttpOnly
x-ua-compatible: IE=edge,chrome=1
cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
pragma: no-cache
expires: 0

<!DOCTYPE HTML>
<html style="height:100%">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<title>重点排污单位自动监控与基础数据库系统（企业端）</title>
<link rel="shortcut icon" href="/amOnline/static/images/favicon.ico"
mce_href="/amOnline/static/images/favicon.ico" type="image/x-icon"/>
<link rel="icon" href="/amOnline/static/images/favicon.ico"/>
<meta http-equiv="Content-Type" content="text/html;charset=utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta http-equiv="Cache-Control" content="no-store, no-cache, must-revalidate, post-check=0, pre-
check=0" />
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Expires" content="0" />
<link href="/amOnline/static/script/themes/default/ui.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/themes/default/login.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/script/themes/icon.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/themes/default/app.css" type="text/css" rel="stylesheet"/>
<script src="/amOnline/static/script/jquery2.js" type="text/javascript"></script>
<script src="/amOnline/static/script/jquery-migrate-1.2.1.js" type="text/javascript"></script>
<script src="/amOnline/static/script/jquery.ui.js" type="text/javascript"></script>
<script src="/amOnline/static/script/locale/ui-lang-zh_CN.js" type="text/javascript"></script>
<script src="/amOnline/static/script/core.js" type="text/javascript"></script>
<script type="text/javascript">
var context = '/amOnline';
var authorizeType = '1';
var enableCaptcha = 'false';
var loginTicket = '2c9487286b79d3e4016b8767136112f0';
</script>

<script src="/amOnline/static/script/common.js" type="text/javascript"></script>
<script src="/amOnline/static/script/AppLogin.js?v=20171023" type="text/javascript"></script>

<!-- 在线客服  -->
<script src="/amOnline/static/am/vendor/zxkf/kefu.js"></script>
<link href="/amOnline/static/am/vendor/zxkf/zxkf.css" rel="stylesheet" />

<!-- 扫码登陆 -->
<script src="/amOnline/static/script/jquery.qrcode.min.js" type="text/javascript"></script>
<script src="/amOnline/static/script/qr.code.login.js" type="text/javascript"></script>

<style type="text/css">
.floatTool {
 width: 110px;
 height: 138px;
 position: absolute;
 right: 0px;
```

```
 top: 50%;
 margin-top: -69px;
 vertical-align: middle;
 text-align: center;
}

.messager-text{
    width:200px;
}
.qr_login_sm_fs{height:100px;width: 288px;margin:0px auto;text-align: center; }
.login_type_fs{float:left; width:33%;}
a.a-login-sm {text-decoration: none; color:#5b5b5b; cursor: pointer;font-size: 16px;}
a.a-login-sm:hover {color:#FF8800 ; text-decoration:none; }
</style>
</head>

<body class="login_bg">
<div style="position:absolute;width:100%;height:100%; text-align: center;">
   <img src="/amOnline/static/themes/default/images/l_m_title_info.png" style="margin-
top:270px;"/>
</div>




 <!--在线客服Begin-->
<div id="floatTools" class="rides-cs">
 <div class="floatL">
         <a style="display: block" id="aFloatTools_Show" class="btnOpen" title="       查看在线客
服" onClick="javascript:$('#divFloatToolsView').animate({width: 'show', opacity: 'show'},
'normal',function(){ $('#divFloatToolsView').show();kf_setCookie('RightFloatShown', 0, '', '/',
'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:none');$('#aFloatTools_Hide').attr('style','disp.
.. href="javascript:void(0);">
                展开</a>
         <a style="display: none" id="aFloatTools_Hide" class="btnCtn" title="       关闭在线客服"
onClick="javascript:$('#divFloatToolsView').animate({width: 'hide', opacity: 'hide'},
'normal',function(){ $('#divFloatToolsView').hide();kf_setCookie('RightFloatShown', 1, '', '/',
'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:block');$('#aFloatTools_Hide').attr('style','dis.
.. href="javascript:void(0);">
                收缩</a> </div>
 <div id="divFloatToolsView" class="floatR" style="display: none">
                 <p><img src="/amOnline/static/8.jpg" width=
...
...
...
```

问题 3 / 4

TOC

已解密的登录请求	
严重性:	高
CVSS 分数:	8.5
URL:	http://172.20.7.168:8083/amonline/app/applogin.page
实体:	newPwd (Parameter)
风险:	可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息
原因:	诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递
固定值:	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异:

推理： AppScan 识别了不是通过 SSL 发送的密码参数。

测试请求和响应：

```
POST /amOnline/app/AppLogin.page HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: hasshown=1; JSESSIONID=2F054296B22CF446C215F74AF599D847
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppLogin.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Content-Length: 187

loginType=front&j_lt=2c9487286b79d3e4016b8766909512e0&cmUsername=1234&verificationCode=1234&logi.
..

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 02:53:26 GMT
x-ua-compatible: IE=edge,chrome=1
cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
pragma: no-cache
expires: 0

<!DOCTYPE HTML>
<html style="height:100%">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<title>重点排污单位自动监控与基础数据库系统（企业端）</title>
<link rel="shortcut icon" href="/amOnline/static/images/favicon.ico"
mce_href="/amOnline/static/images/favicon.ico" type="image/x-icon"/>
<link rel="icon" href="/amOnline/static/images/favicon.ico"/>
<meta http-equiv="Content-Type" content="text/html;charset=utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta http-equiv="Cache-Control" content="no-store, no-cache, must-revalidate, post-check=0, pre-
check=0" />
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Expires" content="0" />
<link href="/amOnline/static/script/themes/default/ui.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/themes/default/login.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/script/themes/icon.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/themes/default/app.css" type="text/css" rel="stylesheet"/>
<script src="/amOnline/static/script/jquery2.js" type="text/javascript"></script>
<script src="/amOnline/static/script/jquery-migrate-1.2.1.js" type="text/javascript"></script>
<script src="/amOnline/static/script/jquery.ui.js" type="text/javascript"></script>
<script src="/amOnline/static/script/locale/ui-lang-zh_CN.js" type="text/javascript"></script>
<script src="/amOnline/static/script/core.js" type="text/javascript"></script>
<script type="text/javascript">
var context = '/amOnline';
var authorizeType = '1';
var enableCaptcha = 'false';
var loginTicket = '2c9487286b79d3e4016b8767113e12eb';
</script>

<script src="/amOnline/static/script/common.js" type="text/javascript"></script>
<script src="/amOnline/static/script/AppLogin.js?v=20171023" type="text/javascript"></script>

<!-- 在线客服 -->
<script src="/amOnline/static/am/vendor/zxkf/kefu.js"></script>
<link href="/amOnline/static/am/vendor/zxkf/zxkf.css" rel="stylesheet" />

<!-- 扫码登陆 -->
<script src="/amOnline/static/script/jquery.qrcode.min.js" type="text/javascript"></script>
<script src="/amOnline/static/script/qr.code.login.js" type="text/javascript"></script>

<style type="text/css">
.floatTool {
 width: 110px;
 height: 138px;
 position: absolute;
 right: 0px;
 top: 50%;
```

```
 margin-top: -69px;
 vertical-align: middle;
 text-align: center;
}

.messager-text{
    width:200px;
}
.qr_login_sm_fs{height:100px;width: 288px;margin:0px auto;text-align: center; }
.login_type_fs{float:left; width:33%;}
a.a-login-sm {text-decoration: none; color:#5b5b5b; cursor: pointer;font-size: 16px;}
a.a-login-sm:hover {color:#FF8800 ; text-decoration:none; }
</style>
</head>

<body class="login_bg">
<div style="position:absolute;width:100%;height:100%; text-align: center;">
   <img src="/amOnline/static/themes/default/images/l_m_title_info.png" style="margin-
top:270px;"/>
</div>



 <!--在线客服Begin-->
<div id="floatTools" class="rides-cs">
 <div class="floatL">
         <a style="display: block" id="aFloatTools_Show" class="btnOpen" title="       查看在线客
服" onClick="javascript:$('#divFloatToolsView').animate({width: 'show', opacity: 'show'},
'normal',function(){ $('#divFloatToolsView').show();kf_setCookie('RightFloatShown', 0, '', '/',
'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:none');$('#aFloatTools_Hide').attr('style','disp.
.. href="javascript:void(0);">
                展开</a>
         <a style="display: none" id="aFloatTools_Hide" class="btnCtn" title="       关闭在线客服"
onClick="javascript:$('#divFloatToolsView').animate({width: 'hide', opacity: 'hide'},
'normal',function(){ $('#divFloatToolsView').hide();kf_setCookie('RightFloatShown', 1, '', '/',
'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:block');$('#aFloatTools_Hide').attr('style','dis.
.. href="javascript:void(0);">
                收缩</a> </div>
 <div id="divFloatToolsView" class="floatR" style="display: none">
                 <p><img src="/amOnline/static/8.jpg" width="100px" height="100px"/></p>
                 <p><span style="text-align: left; color: rgb(255, 255, 255); font-size:
18px; font-weight: bold;
...
...
...
```

问题 4 / 4

TOC

已解密的登录请求

严重性:	高
CVSS 分数:	8.5
URL:	http://172.20.7.168:8083/amonline/app/j_spring_security_check
实体:	j_password (Parameter)
风险:	可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息
原因:	诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递
固定值:	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异：

推理： AppScan 识别了不是通过 SSL 发送的密码参数。

测试请求和响应：

```
POST /amOnline/app/j_spring_security_check HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: hasshown=1; JSESSIONID=4801DD573D4D329FBF176E117991946F
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppLogin.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Content-Length: 123

j_logintype=front_user&j_lt=2c9487286b79d3e4016b8767113e12eb&j_slt=&loginType=front&j_username=1.
..

HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: /amOnline/app/AppMain.page
Content-Length: 0
Date: Mon, 24 Jun 2019 02:53:27 GMT
Set-Cookie: JSESSIONID=898FFF2A3BE84AF807D06E6FBED6B74D; Path=/amOnline; HttpOnly



GET /amOnline/app/AppMain.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=AE1E776BF33CD2F26A4429E80DCAFFAA
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 02:53:27 GMT
x-ua-compatible: IE=edge,chrome=1

<!DOCTYPE html>
<html lang="zh-cn">
<head>
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
    <title>重点排污单位自动监控与基础数据库系统（企业端）</title>
    <link rel="stylesheet" href="/amOnline/static/layui/css/layui.css"  media="all">
    <style>
        .layui-body{
            left:0px;
        }
        .layui-side{
            width:0px;
        }
        .layui-layout-admin .layui-body{
            bottom:0px;
        }
    </style>

</head>
<body class="layui-layout-body">
<div class="layui-layout layui-layout-admin">
    <div class="layui-header layui-bg-blue">
        <div class="layui-logo">重点排污单位自动监控与基础数据库系统(企业端)</div>
        <!-- 头部区域（可配合layui已有的水平导航） -->
        <ul class="layui-nav layui-layout-right    layui-bg-blue">
            <li class="layui-nav-item layui-this"><a href="#"
onclick="loadIframe('app/psinfo/psInfo!view.page')">基本信息维护</a></li>
            <li class="layui-nav-item"  id="historyLine"><a href="#"
onclick="loadIframe('app/onlinemon/onlineAction!history.page')">数据监控</a></li>

            <li class="layui-nav-item">
```

```
                <a href="javascript:;">现场端管理</a>
                <dl class="layui-nav-child" id="xcdzhgl">
                    <dd><a href="#" onclick="loadIframe('app/monitorspot/spotAction!list.page')">
设备验收</a></dd>
                                <dd><a href="#"
onclick="loadIframe('app/monitorspot/stopAction!list.page')">停运管理</a></dd>
                                <!--<dd><a href="#"
onclick="loadIframe('app/viewmonitor/monitorDataAction!list.page')">信息填报</a></dd>   -->
                </dl>
            </li>
            <li class="layui-nav-item" id='reviseLi'><a href="#"
onclick="loadIframe('app/revisedmanage/revisedAction!list.page')">数据标记</a></li>
          <!--  <li class="layui-nav-item" ><a href="#"
onclick="loadIframe('app/revisedmanage/revisedAction!list.page')">数据标记</a></li>
            <li class="layui-nav-item" ><a href="#"
onclick="loadIframe('http://m.envsc.cn/WXIndexPSForQYD.aspx?
key=wPLFgACAKGA&pscode=140000000223&... -->
            <li class="layui-nav-item">
                <a href="javascript:;">
                    <img src="/amOnline/static/layui/images/ooopic_1509436490.png" class="layui-
nav-img">
                    黄智欢
                </a>
                <dl class="layui-nav-child">
                    <dd><a  href="#" onclick="loadIframe('app/account/accountAction!list.page')">
账户管理</a></dd>
                    <dd><a  href="#" onclick="loadIframe('app/loginfo/loginfoAction!list.page')">
操作日志</a></dd>
                    <dd><a onclick="logoutSys()" href="javascript:void(0);"  >退出系统</a></dd>
                </dl>
            </li>


        </ul>
    </div>


    <div class="layui-body">
        <iframe id="frame_lgpblpww"   src="/amOnline/app/psinfo/psInfo!view.page"
                style='width:100%; margin-right:-15px!important;margin-bottom:-14px!important;
overflow-y:scroll; overflow-x:hidden;'     >  </iframe>
    </div>



</div>
<script src="/amOnline/static/layui/layui.js" charset="utf-8"></script>
<!-- 注意：如果你直接复制所有代码到本地，上述js路径需要改成你本地的 -->
<script>


    layui.use('element', function(){
        var element = layui.element; //导航的hover效果、二级菜单等功能，需要依赖element模块

        //监听导航点击
        element.on('nav(demo)', function(elem){
            layer.msg(elem.text());
        });
    });

    function changeFrameHeight(){
        var ifm= document.getElementById("frame_lgpblpww");
        ifm.height=
...
...
...
```

问题 1 / 11

TOC

Authentication Bypass Using HTTP Verb Tampering

严重性:	中
CVSS 分数:	6.4
URL:	http://172.20.7.168:8083/amonline/app/applogin.page
实体:	AppLogin.page (Page)
风险:	可能会升级用户特权并通过 Web 应用程序获取管理许可权 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因:	Web 应用程序编程或配置不安全
固定值:	Configure your server to allow only required HTTP methods

差异: **方法** 从以下位置进行控制: `GET` 至: `BOGUS`
cookie 已从请求除去: `E5C9D3AC69648D3DEA7BBD6FB7A8FAE2`

推理: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the verb tampering was able to bypass the site authentication

测试请求和响应:

```
BOGUS /amOnline/app/AppLogin.page HTTP/1.1
Cookie: hasshown=1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/j_spring_security_logout
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 02:55:23 GMT
Set-Cookie: JSESSIONID=BEB7609C1D1269273AA02954E1036BA1; Path=/amOnline; HttpOnly
x-ua-compatible: IE=edge,chrome=1
cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
pragma: no-cache
expires: 0

<!DOCTYPE HTML>
<html style="height:100%">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<title>重点排污单位自动监控与基础数据库系统（企业端）</title>
<link rel="shortcut icon" href="/amOnline/static/images/favicon.ico"
mce_href="/amOnline/static/images/favicon.ico" type="image/x-icon"/>
```

```
<link rel="icon" href="/amOnline/static/images/favicon.ico"/>
<meta http-equiv="Content-Type" content="text/html;charset=utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta http-equiv="Cache-Control" content="no-store, no-cache, must-revalidate, post-check=0, pre-
check=0" />
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Expires" content="0" />
<link href="/amOnline/static/script/themes/default/ui.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/themes/default/login.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/script/themes/icon.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/themes/default/app.css" type="text/css" rel="stylesheet"/>
<script src="/amOnline/static/script/jquery2.js" type="text/javascript"></script>
<script src="/amOnline/static/script/jquery-migrate-1.2.1.js" type="text/javascript"></script>
<script src="/amOnline/static/script/jquery.ui.js" type="text/javascript"></script>
<script src="/amOnline/static/script/locale/ui-lang-zh_CN.js" type="text/javascript"></script>
<script src="/amOnline/static/script/core.js" type="text/javascript"></script>
<script type="text/javascript">
var context = '/amOnline';
var authorizeType = '1';
var enableCaptcha = 'false';
var loginTicket = '2c9487286b79d3e4016b8768d8fd1306';
</script>

<script src="/amOnline/static/script/common.js" type="text/javascript"></script>
<script src="/amOnline/static/script/AppLogin.js?v=20171023" type="text/javascript"></script>

<!-- 在线客服  -->
<script src="/amOnline/static/am/vendor/zxkf/kefu.js"></script>
<link href="/amOnline/static/am/vendor/zxkf/zxkf.css" rel="stylesheet" />

<!-- 扫码登陆 -->
<script src="/amOnline/static/script/jquery.qrcode.min.js" type="text/javascript"></script>
<script src="/amOnline/static/script/qr.code.login.js" type="text/javascript"></script>

<style type="text/css">
.floatTool {
 width: 110px;
 height: 138px;
 position: absolute;
 right: 0px;
 top: 50%;
 margin-top: -69px;
 vertical-align: middle;
 text-align: center;
}

.messager-text{
    width:200px;
}
.qr_login_sm_fs{height:100px;width: 288px;margin:0px auto;text-align: center; }
.login_type_fs{float:left; width:33%;}
a.a-login-sm {text-decoration: none; color:#5b5b5b; cursor: pointer;font-size: 16px;}
a.a-login-sm:hover {color:#FF8800 ; text-decoration:none; }
</style>
</head>

<body class="login_bg">
<div style="position:absolute;width:100%;height:100%; text-align: center;">
   <img src="/amOnline/static/themes/default/images/l_m_title_info.png" style="margin-
top:270px;"/>
</div>




 <!--在线客服Begin-->
<div id="floatTools" class="rides-cs">
 <div class="floatL">
         <a style="display: block" id="aFloatTools_Show" class="btnOpen" title="       查看在线客
服" onClick="javascript:$('#divFloatToolsView').animate({width: 'show', opacity: 'show'},
'normal',function(){ $('#divFloatToolsView').show();kf_setCookie('RightFloatShown', 0, '', '/',
'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:none');$('#aFloatTools_Hide').attr('style','disp.
.. href="javascript:void(0);">
                展开</a>
         <a style="display: none" id="aFloatTools_Hide" class="btnCtn" title="       关闭在线客服"
onClick="javascript:$('#divFloatToolsView').animate({width: 'hide', opacity: 'hide'},
'normal',function(){ $('#divFloatToolsView').hide();kf_setCookie('RightFloatShown', 1, '', '/',
```

```
'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:block');$('#aFloatTools_Hide').attr('style','dis.
.. href="javascript:void(0);">
                    收缩</a> </div>
 <div id="divFloatToolsView" class="floatR" style="display: none">
                    <p><img src="/amOnline/static/8.jpg" width="100px" height="100px"/></p>
                    <p><span style="text-align: left; color: rgb(255, 255, 255); font-size:
18px; font-weight: bold;">技术支持<br><span style="font-size: 14px;">7*10小时</span><br><span
style="font-size: 14px;">(08:30-18:30)</span></span></p>
...
...
...
```

原始响应

≈

测试响应

问题 2 / 11

TOC

Authentication Bypass Using HTTP Verb Tampering

严重性：	中
CVSS 分数：	6.4
URL：	http://172.20.7.168:8083/amonline/app/psinfoadmin/psinfo!listpsinfo.page
实体：	psInfo!listPsInfo.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	Configure your server to allow only required HTTP methods

差异： **方法** 从以下位置进行控制： `GET` 至： `BOGUS`

推理： The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the verb tampering was able to bypass the site authentication

测试请求和响应：

```
BOGUS /amOnline/app/psinfoadmin/psInfo!listPsInfo.page?psid= HTTP/1.1
X-Requested-With: XMLHttpRequest
```

```
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:00:44 GMT
Set-Cookie: JSESSIONID=ADF9992DA3BBCC57B0CCCE9656047605; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 3 / 11

TOC

Authentication Bypass Using HTTP Verb Tampering

严重性:	中
CVSS 分数:	6.4
URL:	http://172.20.7.168:8083/amonline/app/abnormityadmin/abnormityaction!jsonlist.page
实体:	abnormityAction!jsonList.page (Page)
风险:	可能会升级用户特权并通过 Web 应用程序获取管理许可权 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因:	Web 应用程序编程或配置不安全
固定值:	Configure your server to allow only required HTTP methods

差异: **方法** 从以下位置进行控制: `GET` 至: `BOGUS`

推理: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the verb tampering was able to bypass the site authentication

测试请求和响应:

```
BOGUS /amOnline/app/abnormityadmin/abnormityAction!jsonList.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:00:44 GMT
```

```
Set-Cookie: JSESSIONID=E7E60653BF8D705C623587E32B147739; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 4 / 11

TOC

Authentication Bypass Using HTTP Verb Tampering

严重性:	中
CVSS 分数:	6.4
URL:	http://172.20.7.168:8083/amonline/app/psinfo/admin/psinfo!listpsinfo.page
实体:	psInfo!listPsInfo.page (Page)
风险:	可能会升级用户特权并通过 Web 应用程序获取管理许可权 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因:	Web 应用程序编程或配置不安全
固定值:	Configure your server to allow only required HTTP methods

差异: **方法** 从以下位置进行控制: `GET` 至: `BOGUS`

推理: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the verb tampering was able to bypass the site authentication

测试请求和响应:

```
BOGUS /amOnline/app/psinfo/admin/psInfo!listPsInfo.page?psid= HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:00:44 GMT
Set-Cookie: JSESSIONID=776B36B759FD76D169B26F88B5675D05; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 5 / 11

TOC

Authentication Bypass Using HTTP Verb Tampering

严重性:	中
CVSS 分数:	6.4
URL:	http://172.20.7.168:8083/amonline/app/monitorspotadmin/stopaction!findstopinfos.page
实体:	stopAction!findStopInfos.page (Page)
风险:	可能会升级用户特权并通过 Web 应用程序获取管理许可权 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因:	Web 应用程序编程或配置不安全
固定值:	Configure your server to allow only required HTTP methods

差异: **方法** 从以下位置进行控制: GET 至: BOGUS

推理: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the verb tampering was able to bypass the site authentication

测试请求和响应:

```
BOGUS /amOnline/app/monitorspotadmin/stopAction!findStopInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:00:44 GMT
Set-Cookie: JSESSIONID=D40BAFB8FC6A25D479E3172D9D1C9BD5; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 6 / 11

TOC

Authentication Bypass Using HTTP Verb Tampering

严重性：	中
CVSS 分数：	6.4
URL：	http://172.20.7.168:8083/amonline/app/abnormity/admin/abnormityaction!jsonlist.page
实体：	abnormityAction!jsonList.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	Configure your server to allow only required HTTP methods

差异： **方法** 从以下位置进行控制： `GET` 至： `BOGUS`

推理： The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the verb tampering was able to bypass the site authentication

测试请求和响应：

```
BOGUS /amOnline/app/abnormity/admin/abnormityAction!jsonList.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:00:45 GMT
Set-Cookie: JSESSIONID=2A553F0C48C21AE3856B9E12679E1C5E; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       您没有登录或会话已过期,请重新登录"
}
```

Authentication Bypass Using HTTP Verb Tampering

严重性：	中
CVSS 分数：	6.4
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/admin/stopaction!findstopinfos.page
实体：	stopAction!findStopInfos.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	Configure your server to allow only required HTTP methods

差异： **方法** 从以下位置进行控制： `GET` 至： `BOGUS`

推理： The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the verb tampering was able to bypass the site authentication

测试请求和响应：

```
BOGUS /amOnline/app/monitorspot/admin/stopAction!findStopInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:00:44 GMT
Set-Cookie: JSESSIONID=CC5E9D18F5D8CFE38E000E54A909BC55; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

Authentication Bypass Using HTTP Verb Tampering

严重性：	中
CVSS 分数：	6.4
URL：	http://172.20.7.168:8083/amonline/app/onlinemonadmin/onlineaction!getpollutantswithpsid.page
实体：	onlineAction!getPollutantsWithPsID.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	Configure your server to allow only required HTTP methods

差异： **方法** 从以下位置进行控制： `GET` 至： `BOGUS`

推理： The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the verb tampering was able to bypass the site authentication

测试请求和响应：

```
BOGUS /amOnline/app/onlinemonadmin/onlineAction!getPollutantsWithPsID.page?psID=510101055565
HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:00:44 GMT
Set-Cookie: JSESSIONID=4723728B2D537608FD00B0764632D019; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       您没有登录或会话已过期,请重新登录"
}
```

Authentication Bypass Using HTTP Verb Tampering

严重性：	中
CVSS 分数：	6.4
URL：	http://172.20.7.168:8083/amonline/app/onlinemon/admin/onlineaction!getpollutantswithpsid.page
实体：	onlineAction!getPollutantsWithPsID.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	Configure your server to allow only required HTTP methods

差异： **方法** 从以下位置进行控制： `GET` 至： `BOGUS`

推理： The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the verb tampering was able to bypass the site authentication

测试请求和响应：

```
BOGUS /amOnline/app/onlinemon/admin/onlineAction!getPollutantsWithPsID.page?psID=510101055565
HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:00:44 GMT
Set-Cookie: JSESSIONID=B33B55BEE21CD445D2B2AEC6240DB5F8; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       您没有登录或会话已过期,请重新登录"
}
```

Authentication Bypass Using HTTP Verb Tampering

严重性：	中
CVSS 分数：	6.4
URL：	http://172.20.7.168:8083/amonline/app/monitorspotadmin/spotaction!findacceptinfos.page
实体：	spotAction!findAcceptInfos.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	Configure your server to allow only required HTTP methods

差异： **方法** 从以下位置进行控制： `GET` 至： `BOGUS`

推理： The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the verb tampering was able to bypass the site authentication

测试请求和响应：

```
BOGUS /amOnline/app/monitorspotadmin/spotAction!findAcceptInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:00:44 GMT
Set-Cookie: JSESSIONID=6A805D561AE32CFC1B911B9D0B51CB4E; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 11 / 11

TOC

Authentication Bypass Using HTTP Verb Tampering

严重性：	中
CVSS 分数：	6.4
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/admin/spotaction!findacceptinfos.page
实体：	spotAction!findAcceptInfos.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	Configure your server to allow only required HTTP methods

差异： **方法** 从以下位置进行控制： `GET` 至： `BOGUS`

推理： The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the verb tampering was able to bypass the site authentication

测试请求和响应：

```
BOGUS /amOnline/app/monitorspot/admin/spotAction!findAcceptInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:00:44 GMT
Set-Cookie: JSESSIONID=EFC5872013ADA0D5D97C5D3BF89C4C71; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

中 会话标识未更新 1

TOC

问题 1 / 1

TOC

会话标识未更新

严重性：	中
CVSS 分数：	6.4
URL：	http://172.20.7.168:8083/amonline/app/j_spring_security_check
实体：	j_spring_security_check (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	Web 应用程序编程或配置不安全
固定值：	登录之后更改会话标识符值

差异：

推理： 测试结果似乎指示存在脆弱性，因为“原始请求”（左侧）和“响应”（右侧）中的会话标识相同。这些标志应该已在响应中更新。

测试请求和响应：

```
POST /amOnline/app/j_spring_security_check HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: hasshown=1; JSESSIONID=4801DD573D4D329FBF176E117991946F
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppLogin.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Content-Length: 123

j_logintype=front_user&j_lt=2c9487286b79d3e4016b8767113e12eb&j_slt=&loginType=front&j_username=1.
..

HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: /amOnline/app/AppMain.page
Content-Length: 0
Date: Mon, 24 Jun 2019 02:53:27 GMT
Set-Cookie: JSESSIONID=898FFF2A3BE84AF807D06E6FBED6B74D; Path=/amOnline; HttpOnly



GET /amOnline/app/AppMain.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=AE1E776BF33CD2F26A4429E80DCAFFAA
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 02:53:27 GMT
x-ua-compatible: IE=edge,chrome=1

<!DOCTYPE html>
<html lang="zh-cn">
<head>
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
    <title>重点排污单位自动监控与基础数据库系统（企业端）</title>
    <link rel="stylesheet" href="/amOnline/static/layui/css/layui.css"  media="all">
    <style>
        .layui-body{
            left:0px;
```

```
        }
        .layui-side{
            width:0px;
        }
        .layui-layout-admin .layui-body{
            bottom:0px;
        }
    </style>

</head>
<body class="layui-layout-body">
<div class="layui-layout layui-layout-admin">
    <div class="layui-header layui-bg-blue">
        <div class="layui-logo">重点排污单位自动监控与基础数据库系统(企业端)</div>
        <!-- 头部区域（可配合layui已有的水平导航） -->
        <ul class="layui-nav layui-layout-right    layui-bg-blue">
            <li class="layui-nav-item layui-this"><a href="#"
onclick="loadIframe('app/psinfo/psInfo!view.page')">基本信息维护</a></li>
            <li class="layui-nav-item"  id="historyLine"><a href="#"
onclick="loadIframe('app/onlinemon/onlineAction!history.page')">数据监控</a></li>

            <li class="layui-nav-item">
                <a href="javascript:;">现场端管理</a>
                <dl class="layui-nav-child" id="xcdzhgl">
                    <dd><a href="#" onclick="loadIframe('app/monitorspot/spotAction!list.page')">
设备验收</a></dd>
                                <dd><a href="#"
onclick="loadIframe('app/monitorspot/stopAction!list.page')">停运管理</a></dd>
                                <!--<dd><a href="#"
onclick="loadIframe('app/viewmonitor/monitorDataAction!list.page')">信息填报</a></dd>   -->
                </dl>
            </li>
            <li class="layui-nav-item" id='reviseLi'><a href="#"
onclick="loadIframe('app/revisedmanage/revisedAction!list.page')">数据标记</a></li>
          <!--  <li class="layui-nav-item" ><a href="#"
onclick="loadIframe('app/revisedmanage/revisedAction!list.page')">数据标记</a></li>
            <li class="layui-nav-item" ><a href="#"
onclick="loadIframe('http://m.envsc.cn/WXIndexPSForQYD.aspx?
key=wPLFgACAKGA&pscode=140000000223&... -->
            <li class="layui-nav-item">
                <a href="javascript:;">
                    <img src="/amOnline/static/layui/images/ooopic_1509436490.png" class="layui-
nav-img">
                    黄智欢
                </a>
                <dl class="layui-nav-child">
                    <dd><a  href="#" onclick="loadIframe('app/account/accountAction!list.page')">
账户管理</a></dd>
                    <dd><a  href="#" onclick="loadIframe('app/loginfo/loginfoAction!list.page')">
操作日志</a></dd>
                    <dd><a onclick="logoutSys()" href="javascript:void(0);"  >退出系统</a></dd>
                </dl>
            </li>


        </ul>
    </div>


    <div class="layui-body">
        <iframe id="frame_lgpblpww"   src="/amOnline/app/psinfo/psInfo!view.page"
                style='width:100%; margin-right:-15px!important;margin-bottom:-14px!important;
overflow-y:scroll; overflow-x:hidden;'     >  </iframe>
    </div>



</div>
<script src="/amOnline/static/layui/layui.js" charset="utf-8"></script>
<!-- 注意：如果你直接复制所有代码到本地，上述js路径需要改成你本地的 -->
<script>


    layui.use('element', function(){
        var element = layui.element; //导航的hover效果、二级菜单等功能，需要依赖element模块

        //监听导航点击
        element.on('nav(demo)', function(elem){
```

```
            layer.msg(elem.text());
        });
    });

    function changeFrameHeight(){
        var ifm= document.getElementById("frame_lgpblpww");
        ifm.height=
...
...
...
```

低 Missing "Content-Security-Policy" header 17 TOC

问题 1 / 17 TOC

Missing "Content-Security-Policy" header

严重性:	低
CVSS 分数:	5.0
URL:	http://172.20.7.168:8083/amonline/app/applogin.page
实体:	AppLogin.page (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因:	Web 应用程序编程或配置不安全
固定值:	Config your server to use the "Content-Security-Policy" header

差异:

推理: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

测试请求和响应:

```
GET /amOnline/app/AppLogin.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E5C9D3AC69648D3DEA7BBD6FB7A8FAE2
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/j_spring_security_logout
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 02:55:23 GMT
x-ua-compatible: IE=edge,chrome=1
cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
pragma: no-cache
expires: 0

<!DOCTYPE HTML>
<html style="height:100%">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<title>重点排污单位自动监控与基础数据库系统（企业端）</title>
<link rel="shortcut icon" href="/amOnline/static/images/favicon.ico"
mce_href="/amOnline/static/images/favicon.ico" type="image/x-icon"/>
<link rel="icon" href="/amOnline/static/images/favicon.ico"/>
<meta http-equiv="Content-Type" content="text/html;charset=utf-8" />
```

```
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta http-equiv="Cache-Control" content="no-store, no-cache, must-revalidate, post-check=0, pre-
check=0" />
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Expires" content="0" />
<link href="/amOnline/static/script/themes/default/ui.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/themes/default/login.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/script/themes/icon.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/themes/default/app.css" type="text/css" rel="stylesheet"/>
<script src="/amOnline/static/script/jquery2.js" type="text/javascript"></script>
<script src="/amOnline/static/script/jquery-migrate-1.2.1.js" type="text/javascript"></script>
<script src="/amOnline/static/script/jquery.ui.js" type="text/javascript"></script>
<script src="/amOnline/static/script/locale/ui-lang-zh_CN.js" type="text/javascript"></script>
<script src="/amOnline/static/script/core.js" type="text/javascript"></script>
<script type="text/javascript">
var context = '/amOnline';
var authorizeType = '1';
var enableCaptcha = 'false';
var loginTicket = '2c9487286b79d3e4016b8768d90d1308';
</script>

<script src="/amOnline/static/script/common.js" type="text/javascript"></script>
<script src="/amOnline/static/script/AppLogin.js?v=20171023" type="text/javascript"></script>

<!-- 在线客服  -->
<script src="/amOnline/static/am/vendor/zxkf/kefu.js"></script>
<link href="/amOnline/static/am/vendor/zxkf/zxkf.css" rel="stylesheet" />

<!-- 扫码登陆 -->
<script src="/amOnline/static/script/jquery.qrcode.min.js" type="text/javascript"></script>
<script src="/amOnline/static/script/qr.code.login.js" type="text/javascript"></script>

<style type="text/css">
.floatTool {
 width: 110px;
 height: 138px;
 position: absolute;
 right: 0px;
 top: 50%;
 margin-top: -69px;
 vertical-align: middle;
 text-align: center;
}

.messager-text{
    width:200px;
}
.qr_login_sm_fs{height:100px;width: 288px;margin:0px auto;text-align: center; }
.login_type_fs{float:left; width:33%;}
a.a-login-sm {text-decoration: none; color:#5b5b5b; cursor: pointer;font-size: 16px;}
a.a-login-sm:hover {color:#FF8800 ; text-decoration:none; }
</style>
</head>

<body class="login_bg">
<div style="position:absolute;width:100%;height:100%; text-align: center;">
   <img src="/amOnline/static/themes/default/images/l_m_title_info.png" style="margin-
top:270px;"/>
</div>




 <!--在线客服Begin-->
<div id="floatTools" class="rides-cs">
 <div class="floatL">
         <a style="display: block" id="aFloatTools_Show" class="btnOpen" title="       查看在线客
服" onClick="javascript:$('#divFloatToolsView').animate({width: 'show', opacity: 'show'},
'normal',function(){ $('#divFloatToolsView').show();kf_setCookie('RightFloatShown', 0, '', '/',
'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:none');$('#aFloatTools_Hide').attr('style','disp.
.. href="javascript:void(0);">
                展开</a>
         <a style="display: none" id="aFloatTools_Hide" class="btnCtn" title="       关闭在线客服"
onClick="javascript:$('#divFloatToolsView').animate({width: 'hide', opacity: 'hide'},
'normal',function(){ $('#divFloatToolsView').hide();kf_setCookie('RightFloatShown', 1, '', '/',
'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:block');$('#aFloatTools_Hide').attr('style','dis.
```

```
.. href="javascript:void(0);">
                收缩</a> </div>
 <div id="divFloatToolsView" class="floatR" style="display: none">
                 <p><img src="/amOnline/static/8.jpg" width="100px" height="100px"/></p>
                 <p><span style="text-align: left; color: rgb(255, 255, 255); font-size:
18px; font-weight: bold;">技术支持<br><span style="font-size: 14px;">7*10小时</span><br><span
style="font-size: 14px;">(08:30-18:30)</span></span></p>
 </div>
</div>



 <form name
...
...
...
```

问题 2 / 17

TOC

Missing "Content-Security-Policy" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/abnormity/abnormityaction!jsonlist.page
实体：	abnormityAction!jsonList.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "Content-Security-Policy" header

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去： `2019-04-24`
参数 已从请求除去： `2019-06-24`

推理： AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

测试请求和响应：

```
POST /amOnline/app/abnormity/abnormityAction!jsonList.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
Content-Length: 97

search_alarmType=2&search_disposeType=1&pageNo=1&pageSize=15&showPageInfo=true&showPageList=false

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
```

```
Content-Length: 117
Date: Mon, 24 Jun 2019 03:54:05 GMT
Set-Cookie: JSESSIONID=ED83624FCE56CCDEB75A1D98B89F1EC6; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       用户名或密码错误"
}
```

问题 3 / 17

TOC

Missing "Content-Security-Policy" header

严重性:	低
CVSS 分数:	5.0
URL:	http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!getpollutantswithpsid.page
实体:	onlineAction!getPollutantsWithPsID.page (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因:	Web 应用程序编程或配置不安全
固定值:	Config your server to use the "Content-Security-Policy" header

差异: **cookie** 已从请求除去: `57A6A5AE8E37C43B017578F75A282932`

推理: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

测试请求和响应:

```
POST /amOnline/app/onlinemon/onlineAction!getPollutantsWithPsID.page?psID=510101055565 HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 117
Date: Mon, 24 Jun 2019 03:54:06 GMT
Set-Cookie: JSESSIONID=BFF1E5B40097D58D17AAEB6B5B20154C; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       用户名或密码错误"
}
```

问题 4 / 17

TOC

Missing "Content-Security-Policy" header

严重性:	低
CVSS 分数:	5.0
URL:	http://172.20.7.168:8083/amonline/app/j_spring_security_check
实体:	j_spring_security_check (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因:	Web 应用程序编程或配置不安全
固定值:	Config your server to use the "Content-Security-Policy" header

差异: **cookie** 已从请求除去: `57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去: `front_user`

推理: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

测试请求和响应:

```
POST /amOnline/app/j_spring_security_check HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/AppLogin.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
Content-Length: 39

j_username=13981937605&j_password=hfjcd

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=ISO-8859-1
Content-Length: 61
Date: Mon, 24 Jun 2019 04:00:44 GMT
Set-Cookie: JSESSIONID=F98D9C545215197C3325704EA9397F3E; Path=/amOnline; HttpOnly

{
 "result": "success",
 "targetUrl": "/amOnline/app/AppMain.page"
}
```

问题 5 / 17

TOC

Missing "Content-Security-Policy" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/psinfo/psinfo!listpsinfo.page
实体：	psInfo!listPsInfo.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "Content-Security-Policy" header

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去： `1561348464198`

推理： AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

测试请求和响应：

```
GET /amOnline/app/psinfo/psInfo!listPsInfo.page?psid= HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:54:05 GMT
Set-Cookie: JSESSIONID=26F47329B07DB23948BE5A37A1A48376; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       您没有登录或会话已过期,请重新登录"
}
```

问题 6 / 17

TOC

Missing "Content-Security-Policy" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/stopaction!findstopinfos.page
实体：	stopAction!findStopInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "Content-Security-Policy" header

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去： `2019-04-24`
参数 已从请求除去： `2019-06-24`

推理： AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

测试请求和响应：

```
POST /amOnline/app/monitorspot/stopAction!findStopInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
Content-Length: 57

pageNo=1&pageSize=20&showPageInfo=true&showPageList=false

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 117
Date: Mon, 24 Jun 2019 03:54:05 GMT
Set-Cookie: JSESSIONID=4BC83DD9F483D2A66CB800CDC21A269C; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       用户名或密码错误"
}
```

Missing "Content-Security-Policy" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/psinfo/admin/psinfo!listpsinfo.page
实体：	psInfo!listPsInfo.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "Content-Security-Policy" header

差异：

推理： AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

测试请求和响应：

```
GET /amOnline/app/psinfo/admin/psInfo!listPsInfo.page?psid= HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=88A3F6A907A453E6328F5295A865C34C; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       您没有登录或会话已过期,请重新登录"
}
```

问题 8 / 17

TOC

Missing "Content-Security-Policy" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!findacceptinfos.page
实体：	spotAction!findAcceptInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "Content-Security-Policy" header

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`

推理： AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

测试请求和响应：

```
POST /amOnline/app/monitorspot/spotAction!findAcceptInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
Content-Length: 58

search_acceptStatus=-99&search_pageNo=1&search_pageSize=20

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 117
Date: Mon, 24 Jun 2019 03:54:06 GMT
Set-Cookie: JSESSIONID=508294A61D07A9254784DE8C47DE421F; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       用户名或密码错误"
}
```

Missing "Content-Security-Policy" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/abnormityadmin/abnormityaction!jsonlist.page
实体：	abnormityAction!jsonList.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "Content-Security-Policy" header

差异：

推理： AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

测试请求和响应：

```
GET /amOnline/app/abnormityadmin/abnormityAction!jsonList.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=1CE9604FF5F9D66D2D8C490D1BE95DAC; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

Missing "Content-Security-Policy" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/abnormity/admin/abnormityaction!jsonlist.page
实体：	abnormityAction!jsonList.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "Content-Security-Policy" header

差异：

推理： AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

测试请求和响应：

```
GET /amOnline/app/abnormity/admin/abnormityAction!jsonList.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=0308DD52713329209493123C8AAC241F; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 11 / 17

TOC

Missing "Content-Security-Policy" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/admin/stopaction!findstopinfos.page
实体：	stopAction!findStopInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "Content-Security-Policy" header

差异：

推理： AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

测试请求和响应：

```
GET /amOnline/app/monitorspot/admin/stopAction!findStopInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=37E02AF99A57C266CC6093DE4DC28CD4; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

Missing "Content-Security-Policy" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/onlinemon/admin/onlineaction!getpollutantswithpsid.page
实体：	onlineAction!getPollutantsWithPsID.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "Content-Security-Policy" header

差异：

推理： AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

测试请求和响应：

```
GET /amOnline/app/onlinemon/admin/onlineAction!getPollutantsWithPsID.page?psID=510101055565
HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=E60331CB919C8831DF239AD76B6D8915; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 13 / 17

TOC

Missing "Content-Security-Policy" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspotadmin/spotaction!findacceptinfos.page
实体：	spotAction!findAcceptInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "Content-Security-Policy" header

差异：

推理： AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

测试请求和响应：

```
GET /amOnline/app/monitorspotadmin/spotAction!findAcceptInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=BB27D777C28C01B1FC07B8221BBA20FB; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

Missing "Content-Security-Policy" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/admin/spotaction!findacceptinfos.page
实体：	spotAction!findAcceptInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "Content-Security-Policy" header

差异：

推理： AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

测试请求和响应：

```
GET /amOnline/app/monitorspot/admin/spotAction!findAcceptInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=0E1D4C4C0B8EDB0165F5C5E64FACD5D6; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

Missing "Content-Security-Policy" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/psinfoadmin/psinfo!listpsinfo.page
实体：	psInfo!listPsInfo.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "Content-Security-Policy" header

差异：

推理： AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

测试请求和响应：

```
GET /amOnline/app/psinfoadmin/psInfo!listPsInfo.page?psid= HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=64A2C6D2765D3B6FE363B2BCFCD907D4; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       您没有登录或会话已过期,请重新登录"
}
```

Missing "Content-Security-Policy" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/onlinemonadmin/onlineaction!getpollutantswithpsid.page
实体：	onlineAction!getPollutantsWithPsID.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "Content-Security-Policy" header

差异：

推理： AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

测试请求和响应：

```
GET /amOnline/app/onlinemonadmin/onlineAction!getPollutantsWithPsID.page?psID=510101055565
HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=9AFC021927648D86F4807266101E642A; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 17 / 17

TOC

Missing "Content-Security-Policy" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspotadmin/stopaction!findstopinfos.page
实体：	stopAction!findStopInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "Content-Security-Policy" header

差异：

推理： AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

测试请求和响应：

```
GET /amOnline/app/monitorspotadmin/stopAction!findStopInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=714B3233E562CDF4EA67FF6FAF6B38B7; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

低 Missing "X-Content-Type-Options" header 17 TOC

问题 1 / 17 TOC

Missing "X-Content-Type-Options" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/applogin.page
实体：	AppLogin.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-Content-Type-Options" header

差异：

推理： AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

测试请求和响应：

```
GET /amOnline/app/AppLogin.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E5C9D3AC69648D3DEA7BBD6FB7A8FAE2
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/j_spring_security_logout
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 02:55:23 GMT
x-ua-compatible: IE=edge,chrome=1
cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
pragma: no-cache
expires: 0

<!DOCTYPE HTML>
<html style="height:100%">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<title>重点排污单位自动监控与基础数据库系统（企业端）</title>
<link rel="shortcut icon" href="/amOnline/static/images/favicon.ico"
mce_href="/amOnline/static/images/favicon.ico" type="image/x-icon"/>
<link rel="icon" href="/amOnline/static/images/favicon.ico"/>
<meta http-equiv="Content-Type" content="text/html;charset=utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta http-equiv="Cache-Control" content="no-store, no-cache, must-revalidate, post-check=0, pre-
check=0" />
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Expires" content="0" />
<link href="/amOnline/static/script/themes/default/ui.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/themes/default/login.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/script/themes/icon.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/themes/default/app.css" type="text/css" rel="stylesheet"/>
<script src="/amOnline/static/script/jquery2.js" type="text/javascript"></script>
<script src="/amOnline/static/script/jquery-migrate-1.2.1.js" type="text/javascript"></script>
<script src="/amOnline/static/script/jquery.ui.js" type="text/javascript"></script>
<script src="/amOnline/static/script/locale/ui-lang-zh_CN.js" type="text/javascript"></script>
<script src="/amOnline/static/script/core.js" type="text/javascript"></script>
<script type="text/javascript">
var context = '/amOnline';
var authorizeType = '1';
var enableCaptcha = 'false';
var loginTicket = '2c9487286b79d3e4016b8768d90d1308';
</script>
```

```
<script src="/amOnline/static/script/common.js" type="text/javascript"></script>
<script src="/amOnline/static/script/AppLogin.js?v=20171023" type="text/javascript"></script>

<!-- 在线客服  -->
<script src="/amOnline/static/am/vendor/zxkf/kefu.js"></script>
<link href="/amOnline/static/am/vendor/zxkf/zxkf.css" rel="stylesheet" />

<!-- 扫码登陆 -->
<script src="/amOnline/static/script/jquery.qrcode.min.js" type="text/javascript"></script>
<script src="/amOnline/static/script/qr.code.login.js" type="text/javascript"></script>

<style type="text/css">
.floatTool {
 width: 110px;
 height: 138px;
 position: absolute;
 right: 0px;
 top: 50%;
 margin-top: -69px;
 vertical-align: middle;
 text-align: center;
}

.messager-text{
    width:200px;
}
.qr_login_sm_fs{height:100px;width: 288px;margin:0px auto;text-align: center; }
.login_type_fs{float:left; width:33%;}
a.a-login-sm {text-decoration: none; color:#5b5b5b; cursor: pointer;font-size: 16px;}
a.a-login-sm:hover {color:#FF8800 ; text-decoration:none; }
</style>
</head>

<body class="login_bg">
<div style="position:absolute;width:100%;height:100%; text-align: center;">
   <img src="/amOnline/static/themes/default/images/l_m_title_info.png" style="margin-
top:270px;"/>
</div>




 <!--在线客服Begin-->
<div id="floatTools" class="rides-cs">
 <div class="floatL">
         <a style="display: block" id="aFloatTools_Show" class="btnOpen" title="       查看在线客
服" onClick="javascript:$('#divFloatToolsView').animate({width: 'show', opacity: 'show'},
'normal',function(){ $('#divFloatToolsView').show();kf_setCookie('RightFloatShown', 0, '', '/',
'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:none');$('#aFloatTools_Hide').attr('style','disp.
.. href="javascript:void(0);">
                展开</a>
         <a style="display: none" id="aFloatTools_Hide" class="btnCtn" title="       关闭在线客服"
onClick="javascript:$('#divFloatToolsView').animate({width: 'hide', opacity: 'hide'},
'normal',function(){ $('#divFloatToolsView').hide();kf_setCookie('RightFloatShown', 1, '', '/',
'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:block');$('#aFloatTools_Hide').attr('style','dis.
.. href="javascript:void(0);">
                收缩</a> </div>
 <div id="divFloatToolsView" class="floatR" style="display: none">
                 <p><img src="/amOnline/static/8.jpg" width="100px" height="100px"/></p>
                 <p><span style="text-align: left; color: rgb(255, 255, 255); font-size:
18px; font-weight: bold;">技术支持<br><span style="font-size: 14px;">7*10小时</span><br><span
style="font-size: 14px;">(08:30-18:30)</span></span></p>
 </div>
</div>




 <form name
...
...
...
```

问题 2 / 17

TOC

Missing "X-Content-Type-Options" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!findacceptinfos.page
实体：	spotAction!findAcceptInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-Content-Type-Options" header

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`

推理： AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

测试请求和响应：

```
POST /amOnline/app/monitorspot/spotAction!findAcceptInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
Content-Length: 58

search_acceptStatus=-99&search_pageNo=1&search_pageSize=20

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 117
Date: Mon, 24 Jun 2019 03:54:06 GMT
Set-Cookie: JSESSIONID=508294A61D07A9254784DE8C47DE421F; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       用户名或密码错误"
}
```

问题 3 / 17

TOC

Missing "X-Content-Type-Options" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/abnormity/abnormityaction!jsonlist.page
实体：	abnormityAction!jsonList.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-Content-Type-Options" header

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去： `2019-04-24`
参数 已从请求除去： `2019-06-24`

推理： AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

测试请求和响应：

```
POST /amOnline/app/abnormity/abnormityAction!jsonList.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
Content-Length: 97

search_alarmType=2&search_disposeType=1&pageNo=1&pageSize=15&showPageInfo=true&showPageList=false

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 117
Date: Mon, 24 Jun 2019 03:54:05 GMT
Set-Cookie: JSESSIONID=ED83624FCE56CCDEB75A1D98B89F1EC6; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       用户名或密码错误"
}
```

问题 4 / 17

TOC

Missing "X-Content-Type-Options" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/j_spring_security_check
实体：	j_spring_security_check (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-Content-Type-Options" header

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去： `front_user`

推理： AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

测试请求和响应：

```
POST /amOnline/app/j_spring_security_check HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/AppLogin.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
Content-Length: 39

j_username=13981937605&j_password=hfjcd

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=ISO-8859-1
Content-Length: 61
Date: Mon, 24 Jun 2019 04:00:44 GMT
Set-Cookie: JSESSIONID=F98D9C545215197C3325704EA9397F3E; Path=/amOnline; HttpOnly

{
 "result": "success",
 "targetUrl": "/amOnline/app/AppMain.page"
}
```

问题 5 / 17

TOC

Missing "X-Content-Type-Options" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/psinfo/psinfo!listpsinfo.page
实体：	psInfo!listPsInfo.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-Content-Type-Options" header

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去： `1561348464198`

推理： AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

测试请求和响应：

```
GET /amOnline/app/psinfo/psInfo!listPsInfo.page?psid= HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:54:05 GMT
Set-Cookie: JSESSIONID=26F47329B07DB23948BE5A37A1A48376; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       您没有登录或会话已过期,请重新登录"
}
```

Missing "X-Content-Type-Options" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!getpollutantswithpsid.page
实体：	onlineAction!getPollutantsWithPsID.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-Content-Type-Options" header

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`

推理： AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

测试请求和响应：

```
POST /amOnline/app/onlinemon/onlineAction!getPollutantsWithPsID.page?psID=510101055565 HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 117
Date: Mon, 24 Jun 2019 03:54:06 GMT
Set-Cookie: JSESSIONID=BFF1E5B40097D58D17AAEB6B5B20154C; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       用户名或密码错误"
}
```

Missing "X-Content-Type-Options" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/stopaction!findstopinfos.page
实体：	stopAction!findStopInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-Content-Type-Options" header

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去： `2019-04-24`
参数 已从请求除去： `2019-06-24`

推理： AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

测试请求和响应：

```
POST /amOnline/app/monitorspot/stopAction!findStopInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
Content-Length: 57

pageNo=1&pageSize=20&showPageInfo=true&showPageList=false

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 117
Date: Mon, 24 Jun 2019 03:54:05 GMT
Set-Cookie: JSESSIONID=4BC83DD9F483D2A66CB800CDC21A269C; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       用户名或密码错误"
}
```

Missing "X-Content-Type-Options" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/psinfo/admin/psinfo!listpsinfo.page
实体：	psInfo!listPsInfo.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-Content-Type-Options" header

差异：

推理： AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

测试请求和响应：

```
GET /amOnline/app/psinfo/admin/psInfo!listPsInfo.page?psid= HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=88A3F6A907A453E6328F5295A865C34C; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 9 / 17

TOC

Missing "X-Content-Type-Options" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/abnormityadmin/abnormityaction!jsonlist.page
实体：	abnormityAction!jsonList.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-Content-Type-Options" header

差异：

推理： AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

测试请求和响应：

```
GET /amOnline/app/abnormityadmin/abnormityAction!jsonList.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=1CE9604FF5F9D66D2D8C490D1BE95DAC; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

Missing "X-Content-Type-Options" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/onlinemon/admin/onlineaction!getpollutantswithpsid.page
实体：	onlineAction!getPollutantsWithPsID.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-Content-Type-Options" header

差异：

推理： AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

测试请求和响应：

```
GET /amOnline/app/onlinemon/admin/onlineAction!getPollutantsWithPsID.page?psID=510101055565
HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=E60331CB919C8831DF239AD76B6D8915; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 11 / 17

TOC

Missing "X-Content-Type-Options" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/admin/stopaction!findstopinfos.page
实体：	stopAction!findStopInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-Content-Type-Options" header

差异：

推理： AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

测试请求和响应：

```
GET /amOnline/app/monitorspot/admin/stopAction!findStopInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=37E02AF99A57C266CC6093DE4DC28CD4; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

Missing "X-Content-Type-Options" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/abnormity/admin/abnormityaction!jsonlist.page
实体：	abnormityAction!jsonList.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-Content-Type-Options" header

差异：

推理： AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

测试请求和响应：

```
GET /amOnline/app/abnormity/admin/abnormityAction!jsonList.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=0308DD52713329209493123C8AAC241F; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

Missing "X-Content-Type-Options" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspotadmin/spotaction!findacceptinfos.page
实体：	spotAction!findAcceptInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-Content-Type-Options" header

差异：

推理： AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

测试请求和响应：

```
GET /amOnline/app/monitorspotadmin/spotAction!findAcceptInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=BB27D777C28C01B1FC07B8221BBA20FB; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

Missing "X-Content-Type-Options" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/admin/spotaction!findacceptinfos.page
实体：	spotAction!findAcceptInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-Content-Type-Options" header

差异：

推理： AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

测试请求和响应：

```
GET /amOnline/app/monitorspot/admin/spotAction!findAcceptInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=0E1D4C4C0B8EDB0165F5C5E64FACD5D6; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

Missing "X-Content-Type-Options" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/psinfoadmin/psinfo!listpsinfo.page
实体：	psInfo!listPsInfo.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-Content-Type-Options" header

差异：

推理： AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

测试请求和响应：

```
GET /amOnline/app/psinfoadmin/psInfo!listPsInfo.page?psid= HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=64A2C6D2765D3B6FE363B2BCFCD907D4; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

Missing "X-Content-Type-Options" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/onlinemonadmin/onlineaction!getpollutantswithpsid.page
实体：	onlineAction!getPollutantsWithPsID.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-Content-Type-Options" header

差异：

推理： AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

测试请求和响应：

```
GET /amOnline/app/onlinemonadmin/onlineAction!getPollutantsWithPsID.page?psID=510101055565
HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=9AFC021927648D86F4807266101E642A; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 17 / 17

TOC

Missing "X-Content-Type-Options" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspotadmin/stopaction!findstopinfos.page
实体：	stopAction!findStopInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-Content-Type-Options" header

差异：

推理： AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

测试请求和响应：

```
GET /amOnline/app/monitorspotadmin/stopAction!findStopInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=714B3233E562CDF4EA67FF6FAF6B38B7; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

低 Missing "X-XSS-Protection" header 17

TOC

问题 1 / 17

TOC

Missing "X-XSS-Protection" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/applogin.page
实体：	AppLogin.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-XSS-Protection" header

差异：

推理： AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

测试请求和响应：

```
GET /amOnline/app/AppLogin.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E5C9D3AC69648D3DEA7BBD6FB7A8FAE2
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/j_spring_security_logout
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 02:55:23 GMT
x-ua-compatible: IE=edge,chrome=1
cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
pragma: no-cache
expires: 0

<!DOCTYPE HTML>
<html style="height:100%">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<title>重点排污单位自动监控与基础数据库系统（企业端）</title>
<link rel="shortcut icon" href="/amOnline/static/images/favicon.ico"
mce_href="/amOnline/static/images/favicon.ico" type="image/x-icon"/>
<link rel="icon" href="/amOnline/static/images/favicon.ico"/>
<meta http-equiv="Content-Type" content="text/html;charset=utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta http-equiv="Cache-Control" content="no-store, no-cache, must-revalidate, post-check=0, pre-
check=0" />
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Expires" content="0" />
<link href="/amOnline/static/script/themes/default/ui.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/themes/default/login.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/script/themes/icon.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/themes/default/app.css" type="text/css" rel="stylesheet"/>
<script src="/amOnline/static/script/jquery2.js" type="text/javascript"></script>
<script src="/amOnline/static/script/jquery-migrate-1.2.1.js" type="text/javascript"></script>
<script src="/amOnline/static/script/jquery.ui.js" type="text/javascript"></script>
<script src="/amOnline/static/script/locale/ui-lang-zh_CN.js" type="text/javascript"></script>
<script src="/amOnline/static/script/core.js" type="text/javascript"></script>
<script type="text/javascript">
var context = '/amOnline';
var authorizeType = '1';
var enableCaptcha = 'false';
var loginTicket = '2c9487286b79d3e4016b8768d90d1308';
</script>
```

```
<script src="/amOnline/static/script/common.js" type="text/javascript"></script>
<script src="/amOnline/static/script/AppLogin.js?v=20171023" type="text/javascript"></script>

<!-- 在线客服  -->
<script src="/amOnline/static/am/vendor/zxkf/kefu.js"></script>
<link href="/amOnline/static/am/vendor/zxkf/zxkf.css" rel="stylesheet" />

<!-- 扫码登陆 -->
<script src="/amOnline/static/script/jquery.qrcode.min.js" type="text/javascript"></script>
<script src="/amOnline/static/script/qr.code.login.js" type="text/javascript"></script>

<style type="text/css">
.floatTool {
 width: 110px;
 height: 138px;
 position: absolute;
 right: 0px;
 top: 50%;
 margin-top: -69px;
 vertical-align: middle;
 text-align: center;
}

.messager-text{
    width:200px;
}
.qr_login_sm_fs{height:100px;width: 288px;margin:0px auto;text-align: center; }
.login_type_fs{float:left; width:33%;}
a.a-login-sm {text-decoration: none; color:#5b5b5b; cursor: pointer;font-size: 16px;}
a.a-login-sm:hover {color:#FF8800 ; text-decoration:none; }
</style>
</head>

<body class="login_bg">
<div style="position:absolute;width:100%;height:100%; text-align: center;">
   <img src="/amOnline/static/themes/default/images/l_m_title_info.png" style="margin-
top:270px;"/>
</div>




 <!--在线客服Begin-->
<div id="floatTools" class="rides-cs">
 <div class="floatL">
         <a style="display: block" id="aFloatTools_Show" class="btnOpen" title="       查看在线客
服" onClick="javascript:$('#divFloatToolsView').animate({width: 'show', opacity: 'show'},
'normal',function(){ $('#divFloatToolsView').show();kf_setCookie('RightFloatShown', 0, '', '/',
'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:none');$('#aFloatTools_Hide').attr('style','disp.
.. href="javascript:void(0);">
                展开</a>
         <a style="display: none" id="aFloatTools_Hide" class="btnCtn" title="       关闭在线客服"
onClick="javascript:$('#divFloatToolsView').animate({width: 'hide', opacity: 'hide'},
'normal',function(){ $('#divFloatToolsView').hide();kf_setCookie('RightFloatShown', 1, '', '/',
'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:block');$('#aFloatTools_Hide').attr('style','dis.
.. href="javascript:void(0);">
                收缩</a> </div>
 <div id="divFloatToolsView" class="floatR" style="display: none">
                 <p><img src="/amOnline/static/8.jpg" width="100px" height="100px"/></p>
                 <p><span style="text-align: left; color: rgb(255, 255, 255); font-size:
18px; font-weight: bold;">技术支持<br><span style="font-size: 14px;">7*10小时</span><br><span
style="font-size: 14px;">(08:30-18:30)</span></span></p>
 </div>
</div>




 <form name
...
...
...
```

问题 2 / 17

TOC

Missing "X-XSS-Protection" header

严重性:	低
CVSS 分数:	5.0
URL:	http://172.20.7.168:8083/amonline/app/abnormity/abnormityaction!jsonlist.page
实体:	abnormityAction!jsonList.page (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因:	Web 应用程序编程或配置不安全
固定值:	Config your server to use the "X-XSS-Protection" header

差异: **cookie** 已从请求除去: `57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去: `2019-04-24`
参数 已从请求除去: `2019-06-24`

推理: AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

测试请求和响应:

```
POST /amOnline/app/abnormity/abnormityAction!jsonList.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
Content-Length: 97

search_alarmType=2&search_disposeType=1&pageNo=1&pageSize=15&showPageInfo=true&showPageList=false

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 117
Date: Mon, 24 Jun 2019 03:54:05 GMT
Set-Cookie: JSESSIONID=ED83624FCE56CCDEB75A1D98B89F1EC6; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       用户名或密码错误"
}
```

问题 3 / 17

TOC

Missing "X-XSS-Protection" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/j_spring_security_check
实体：	j_spring_security_check (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-XSS-Protection" header

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去： `front_user`

推理： AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

测试请求和响应：

```
POST /amOnline/app/j_spring_security_check HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/AppLogin.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
Content-Length: 39

j_username=13981937605&j_password=hfjcd

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=ISO-8859-1
Content-Length: 61
Date: Mon, 24 Jun 2019 04:00:44 GMT
Set-Cookie: JSESSIONID=F98D9C545215197C3325704EA9397F3E; Path=/amOnline; HttpOnly

{
 "result": "success",
 "targetUrl": "/amOnline/app/AppMain.page"
}
```

问题 4 / 17

TOC

Missing "X-XSS-Protection" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!findacceptinfos.page
实体：	spotAction!findAcceptInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-XSS-Protection" header

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`

推理： AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

测试请求和响应：

```
POST /amOnline/app/monitorspot/spotAction!findAcceptInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
Content-Length: 58

search_acceptStatus=-99&search_pageNo=1&search_pageSize=20

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 117
Date: Mon, 24 Jun 2019 03:54:06 GMT
Set-Cookie: JSESSIONID=508294A61D07A9254784DE8C47DE421F; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       用户名或密码错误"
}
```

Missing "X-XSS-Protection" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/psinfo/psinfo!listpsinfo.page
实体：	psInfo!listPsInfo.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-XSS-Protection" header

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去： `1561348464198`

推理： AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

测试请求和响应：

```
GET /amOnline/app/psinfo/psInfo!listPsInfo.page?psid= HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:54:05 GMT
Set-Cookie: JSESSIONID=26F47329B07DB23948BE5A37A1A48376; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       您没有登录或会话已过期,请重新登录"
}
```

问题 6 / 17

TOC

Missing "X-XSS-Protection" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/stopaction!findstopinfos.page
实体：	stopAction!findStopInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-XSS-Protection" header

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去： `2019-04-24`
参数 已从请求除去： `2019-06-24`

推理： AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

测试请求和响应：

```
POST /amOnline/app/monitorspot/stopAction!findStopInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
Content-Length: 57

pageNo=1&pageSize=20&showPageInfo=true&showPageList=false

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 117
Date: Mon, 24 Jun 2019 03:54:05 GMT
Set-Cookie: JSESSIONID=4BC83DD9F483D2A66CB800CDC21A269C; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       用户名或密码错误"
}
```

Missing "X-XSS-Protection" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!getpollutantswithpsid.page
实体：	onlineAction!getPollutantsWithPsID.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-XSS-Protection" header

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`

推理： AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

测试请求和响应：

```
POST /amOnline/app/onlinemon/onlineAction!getPollutantsWithPsID.page?psID=510101055565 HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
Content-Length: 0


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 117
Date: Mon, 24 Jun 2019 03:54:06 GMT
Set-Cookie: JSESSIONID=BFF1E5B40097D58D17AAEB6B5B20154C; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       用户名或密码错误"
}
```

Missing "X-XSS-Protection" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/psinfo/admin/psinfo!listpsinfo.page
实体：	psInfo!listPsInfo.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-XSS-Protection" header

差异：

推理： AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

测试请求和响应：

```
GET /amOnline/app/psinfo/admin/psInfo!listPsInfo.page?psid= HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=88A3F6A907A453E6328F5295A865C34C; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 9 / 17

TOC

Missing "X-XSS-Protection" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/abnormityadmin/abnormityaction!jsonlist.page
实体：	abnormityAction!jsonList.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-XSS-Protection" header

差异：

推理： AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

测试请求和响应：

```
GET /amOnline/app/abnormityadmin/abnormityAction!jsonList.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=1CE9604FF5F9D66D2D8C490D1BE95DAC; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

Missing "X-XSS-Protection" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/admin/stopaction!findstopinfos.page
实体：	stopAction!findStopInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-XSS-Protection" header

差异：

推理： AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

测试请求和响应：

```
GET /amOnline/app/monitorspot/admin/stopAction!findStopInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=37E02AF99A57C266CC6093DE4DC28CD4; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

Missing "X-XSS-Protection" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/abnormity/admin/abnormityaction!jsonlist.page
实体：	abnormityAction!jsonList.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-XSS-Protection" header

差异：

推理： AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

测试请求和响应：

```
GET /amOnline/app/abnormity/admin/abnormityAction!jsonList.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=0308DD52713329209493123C8AAC241F; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

Missing "X-XSS-Protection" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/onlinemon/admin/onlineaction!getpollutantswithpsid.page
实体：	onlineAction!getPollutantsWithPsID.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-XSS-Protection" header

差异：

推理： AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

测试请求和响应：

```
GET /amOnline/app/onlinemon/admin/onlineAction!getPollutantsWithPsID.page?psID=510101055565
HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=E60331CB919C8831DF239AD76B6D8915; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 13 / 17

TOC

Missing "X-XSS-Protection" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspotadmin/spotaction!findacceptinfos.page
实体：	spotAction!findAcceptInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-XSS-Protection" header

差异：

推理： AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

测试请求和响应：

```
GET /amOnline/app/monitorspotadmin/spotAction!findAcceptInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=BB27D777C28C01B1FC07B8221BBA20FB; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

Missing "X-XSS-Protection" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/admin/spotaction!findacceptinfos.page
实体：	spotAction!findAcceptInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-XSS-Protection" header

差异：

推理： AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

测试请求和响应：

```
GET /amOnline/app/monitorspot/admin/spotAction!findAcceptInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=0E1D4C4C0B8EDB0165F5C5E64FACD5D6; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

Missing "X-XSS-Protection" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/psinfoadmin/psinfo!listpsinfo.page
实体：	psInfo!listPsInfo.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-XSS-Protection" header

差异：

推理： AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

测试请求和响应：

```
GET /amOnline/app/psinfoadmin/psInfo!listPsInfo.page?psid= HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=64A2C6D2765D3B6FE363B2BCFCD907D4; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

Missing "X-XSS-Protection" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/onlinemonadmin/onlineaction!getpollutantswithpsid.page
实体：	onlineAction!getPollutantsWithPsID.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-XSS-Protection" header

差异：

推理： AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

测试请求和响应：

```
GET /amOnline/app/onlinemonadmin/onlineAction!getPollutantsWithPsID.page?psID=510101055565
HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=9AFC021927648D86F4807266101E642A; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 17 / 17

TOC

Missing "X-XSS-Protection" header

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspotadmin/stopaction!findstopinfos.page
实体：	stopAction!findStopInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	Config your server to use the "X-XSS-Protection" header

差异：

推理： AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

测试请求和响应：

```
GET /amOnline/app/monitorspotadmin/stopAction!findStopInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=714B3233E562CDF4EA67FF6FAF6B38B7; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

低 查询中接受的主体参数 2

TOC

问题 1 / 2

TOC

查询中接受的主体参数

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/j_spring_security_check
实体：	j_spring_security_check (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	请勿接受在查询字符串中发送的主体参数

差异： **方法** 从以下位置进行控制： POST 至： GET

推理： The test result seems to indicate a vulnerability because the Test Response is similar to the Original Response, indicating that the application processed body parameters that were submitted in the query

测试请求和响应：

```
GET /amOnline/app/j_spring_security_check?
j_logintype=front_user&j_lt=2c9487286b79d3e4016b8767113e12... HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: hasshown=1; JSESSIONID=E5C9D3AC69648D3DEA7BBD6FB7A8FAE2
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppLogin.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: /amOnline/app/AppLogin.page?loginError=auth_failed
Content-Length: 0
Date: Mon, 24 Jun 2019 02:55:52 GMT
Set-Cookie: JSESSIONID=A792152824F703E634A97AE75D0F3796; Path=/amOnline; HttpOnly



GET /amOnline/app/AppLogin.page?loginError=auth_failed HTTP/1.1
Cookie: hasshown=1; JSESSIONID=A792152824F703E634A97AE75D0F3796
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/j_spring_security_check?
j_logintype=front_user&j_lt=2c9487...
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 02:55:52 GMT
x-ua-compatible: IE=edge,chrome=1
cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
pragma: no-cache
expires: 0

<!DOCTYPE HTML>
<html style="height:100%">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<title>重点排污单位自动监控与基础数据库系统（企业端）</title>
<link rel="shortcut icon" href="/amOnline/static/images/favicon.ico"
```

```
mce_href="/amOnline/static/images/favicon.ico" type="image/x-icon"/>
<link rel="icon" href="/amOnline/static/images/favicon.ico"/>
<meta http-equiv="Content-Type" content="text/html;charset=utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta http-equiv="Cache-Control" content="no-store, no-cache, must-revalidate, post-check=0, pre-
check=0" />
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Expires" content="0" />
<link href="/amOnline/static/script/themes/default/ui.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/themes/default/login.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/script/themes/icon.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/themes/default/app.css" type="text/css" rel="stylesheet"/>
<script src="/amOnline/static/script/jquery2.js" type="text/javascript"></script>
<script src="/amOnline/static/script/jquery-migrate-1.2.1.js" type="text/javascript"></script>
<script src="/amOnline/static/script/jquery.ui.js" type="text/javascript"></script>
<script src="/amOnline/static/script/locale/ui-lang-zh_CN.js" type="text/javascript"></script>
<script src="/amOnline/static/script/core.js" type="text/javascript"></script>
<script type="text/javascript">
var context = '/amOnline';
var authorizeType = '1';
var enableCaptcha = 'false';
var loginTicket = '2c9487286b79d3e4016b87694ac1133e';
</script>

<script src="/amOnline/static/script/common.js" type="text/javascript"></script>
<script src="/amOnline/static/script/AppLogin.js?v=20171023" type="text/javascript"></script>

<!-- 在线客服  -->
<script src="/amOnline/static/am/vendor/zxkf/kefu.js"></script>
<link href="/amOnline/static/am/vendor/zxkf/zxkf.css" rel="stylesheet" />

<!-- 扫码登陆 -->
<script src="/amOnline/static/script/jquery.qrcode.min.js" type="text/javascript"></script>
<script src="/amOnline/static/script/qr.code.login.js" type="text/javascript"></script>

<style type="text/css">
.floatTool {
 width: 110px;
 height: 138px;
 position: absolute;
 right: 0px;
 top: 50%;
 margin-top: -69px;
 vertical-align: middle;
 text-align: center;
}

.messager-text{
    width:200px;
}
.qr_login_sm_fs{height:100px;width: 288px;margin:0px auto;text-align: center; }
.login_type_fs{float:left; width:33%;}
a.a-login-sm {text-decoration: none; color:#5b5b5b; cursor: pointer;font-size: 16px;}
a.a-login-sm:hover {color:#FF8800 ; text-decoration:none; }
</style>
</head>

<body class="login_bg">
<div style="position:absolute;width:100%;height:100%; text-align: center;">
   <img src="/amOnline/static/themes/default/images/l_m_title_info.png" style="margin-
top:270px;"/>
</div>




 <!--在线客服Begin-->
<div id="floatTools" class="rides-cs">
 <div class="floatL">
         <a style="display: block" id="aFloatTools_Show" class="btnOpen" title="       查看在线客
服" onClick="javascript:$('#divFloatToolsView').animate({width: 'show', opacity: 'show'},
'normal',function(){ $('#divFloatToolsView').show();kf_setCookie('RightFloatShown', 0, '', '/',
'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:none');$('#aFloatTools_Hide').attr('style','disp.
.. href="javascript:void(0);">
                展开</a>
         <a style="disp
...
```

```
...
...
```

问题 2 / 2

TOC

查询中接受的主体参数

严重性:	低
CVSS 分数:	5.0
URL:	http://172.20.7.168:8083/amonline/app/applogin.page
实体:	AppLogin.page (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因:	Web 应用程序编程或配置不安全
固定值:	请勿接受在查询字符串中发送的主体参数

差异: **方法** 从以下位置进行控制: `POST` 至: `GET`

推理: The test result seems to indicate a vulnerability because the Test Response is similar to the Original Response, indicating that the application processed body parameters that were submitted in the query

测试请求和响应:

```
GET /amOnline/app/AppLogin.page?
loginError=auth_failed&loginType=front&j_lt=2c9487286b79d3e4016b8767... HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: hasshown=1; JSESSIONID=E5C9D3AC69648D3DEA7BBD6FB7A8FAE2
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppLogin.page?loginError=auth_failed
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 02:55:53 GMT
Set-Cookie: JSESSIONID=A5EA00F2791F73230C99B24A3AF33C5C; Path=/amOnline; HttpOnly
x-ua-compatible: IE=edge,chrome=1
cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
pragma: no-cache
expires: 0

<!DOCTYPE HTML>
<html style="height:100%">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<title>重点排污单位自动监控与基础数据库系统（企业端）</title>
<link rel="shortcut icon" href="/amOnline/static/images/favicon.ico"
mce_href="/amOnline/static/images/favicon.ico" type="image/x-icon"/>
<link rel="icon" href="/amOnline/static/images/favicon.ico"/>
<meta http-equiv="Content-Type" content="text/html;charset=utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta http-equiv="Cache-Control" content="no-store, no-cache, must-revalidate, post-check=0, pre-
check=0" />
```

```
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Expires" content="0" />
<link href="/amOnline/static/script/themes/default/ui.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/themes/default/login.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/script/themes/icon.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/themes/default/app.css" type="text/css" rel="stylesheet"/>
<script src="/amOnline/static/script/jquery2.js" type="text/javascript"></script>
<script src="/amOnline/static/script/jquery-migrate-1.2.1.js" type="text/javascript"></script>
<script src="/amOnline/static/script/jquery.ui.js" type="text/javascript"></script>
<script src="/amOnline/static/script/locale/ui-lang-zh_CN.js" type="text/javascript"></script>
<script src="/amOnline/static/script/core.js" type="text/javascript"></script>
<script type="text/javascript">
var context = '/amOnline';
var authorizeType = '1';
var enableCaptcha = 'false';
var loginTicket = '2c9487286b79d3e4016b87694e7a139c';
</script>

<script src="/amOnline/static/script/common.js" type="text/javascript"></script>
<script src="/amOnline/static/script/AppLogin.js?v=20171023" type="text/javascript"></script>

<!-- 在线客服  -->
<script src="/amOnline/static/am/vendor/zxkf/kefu.js"></script>
<link href="/amOnline/static/am/vendor/zxkf/zxkf.css" rel="stylesheet" />

<!-- 扫码登陆 -->
<script src="/amOnline/static/script/jquery.qrcode.min.js" type="text/javascript"></script>
<script src="/amOnline/static/script/qr.code.login.js" type="text/javascript"></script>

<style type="text/css">
.floatTool {
 width: 110px;
 height: 138px;
 position: absolute;
 right: 0px;
 top: 50%;
 margin-top: -69px;
 vertical-align: middle;
 text-align: center;
}

.messager-text{
    width:200px;
}
.qr_login_sm_fs{height:100px;width: 288px;margin:0px auto;text-align: center; }
.login_type_fs{float:left; width:33%;}
a.a-login-sm {text-decoration: none; color:#5b5b5b; cursor: pointer;font-size: 16px;}
a.a-login-sm:hover {color:#FF8800 ; text-decoration:none; }
</style>
</head>

<body class="login_bg">
<div style="position:absolute;width:100%;height:100%; text-align: center;">
   <img src="/amOnline/static/themes/default/images/l_m_title_info.png" style="margin-
top:270px;"/>
</div>




 <!--在线客服Begin-->
<div id="floatTools" class="rides-cs">
 <div class="floatL">
         <a style="display: block" id="aFloatTools_Show" class="btnOpen" title="       查看在线客
服" onClick="javascript:$('#divFloatToolsView').animate({width: 'show', opacity: 'show'},
'normal',function(){ $('#divFloatToolsView').show();kf_setCookie('RightFloatShown', 0, '', '/',
'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:none');$('#aFloatTools_Hide').attr('style','disp.
.. href="javascript:void(0);">
                 展开</a>
         <a style="display: none" id="aFloatTools_Hide" class="btnCtn" title="       关闭在线客服"
onClick="javascript:$('#divFloatToolsView').animate({width: 'hide', opacity: 'hide'},
'normal',function(){ $('#divFloatToolsView').hide();kf_setCookie('RightFloatShown', 1, '', '/',
'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:block');$('#aFloatTools_Hide').attr('style','dis.
.. href="javascript:void(0);">
                 收缩</a> </div>
 <div id="divFloatToolsView" class="floatR" style="display: none">
```

```
                <p><img src="/amOnline/static/8.jpg" width="100px" height="100px"/></p>
                <p><span style="text-align: left; color:
...
...
...
```

原始响应

≈

测试响应

低 归档文件下载 5 TOC

问题 1 / 5 TOC

归档文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/psinfo/psinfo!listpsinfo.page
实体：	psInfo!listPsInfo.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **cookie** 已从请求除去：`57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去：`1561348464198`
路径 从以下位置进行控制：`/amOnline/app/psinfo/psInfo!listPsInfo.page` 至：`/amOnline/app/psinfo/psInfo!listPsInfo.page.arc`

推理： 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。
测试请求和响应：

```
GET /amOnline/app/psinfo/psInfo!listPsInfo.page.arc?psid= HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:54:15 GMT
Set-Cookie: JSESSIONID=F17D52D778832875D4B72F8679B7B8A9; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 2 / 5

TOC

归档文件下载

严重性:	低
CVSS 分数:	5.0
URL:	http://172.20.7.168:8083/amonline/app/abnormity/abnormityaction!jsonlist.page
实体:	abnormityAction!jsonList.page (Page)
风险:	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因:	在生产环境中留下临时文件
固定值:	除去虚拟目录中的旧版本文件

差异: **cookie** 已从请求除去: `57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去: `2019-04-24`
参数 已从请求除去: `2019-06-24`
方法 从以下位置进行控制: `POST` 至: `GET`
主体 从以下位置进行控制:
`search_alarmType=2&search_disposeType=1&pageNo=1&pageSize=15&showPageInfo=true&showPageList=false`
至:
标题 已从请求除去: `application/x-www-form-urlencoded; charset=UTF-8`
路径 从以下位置进行控制: `/amOnline/app/abnormity/abnormityAction!jsonList.page` 至:
`/amOnline/app/abnormity/abnormityAction!jsonList.page.arc`

推理: 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。
测试请求和响应:

```
GET /amOnline/app/abnormity/abnormityAction!jsonList.page.arc HTTP/1.1
```

```
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:54:14 GMT
Set-Cookie: JSESSIONID=38B6394CD98CD7C6A35B6071985212F1; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 3 / 5

TOC

归档文件下载

严重性:	低
CVSS 分数:	5.0
URL:	http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!getpollutantswithpsid.page
实体:	onlineAction!getPollutantsWithPsID.page (Page)
风险:	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因:	在生产环境中留下临时文件
固定值:	除去虚拟目录中的旧版本文件

差异: **cookie** 已从请求除去: `57A6A5AE8E37C43B017578F75A282932`
方法 从以下位置进行控制: `POST` 至: `GET`
路径 从以下位置进行控制: `/amOnline/app/onlinemon/onlineAction!getPollutantsWithPsID.page`
至: `/amOnline/app/onlinemon/onlineAction!getPollutantsWithPsID.page.ARC`

推理: 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。

测试请求和响应:

```
GET /amOnline/app/onlinemon/onlineAction!getPollutantsWithPsID.page.ARC?psID=510101055565
HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:54:16 GMT
Set-Cookie: JSESSIONID=5CD15B54E4243AD6DA2D8A4E6677EC56; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 4 / 5

TOC

归档文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!findacceptinfos.page
实体：	spotAction!findAcceptInfos.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`
方法 从以下位置进行控制： `POST` 至： `GET`
主体 从以下位置进行控制： `search_acceptStatus=-99&search_pageNo=1&search_pageSize=20` 至：
标题 已从请求除去： `application/x-www-form-urlencoded; charset=UTF-8`
路径 从以下位置进行控制： `/amOnline/app/monitorspot/spotAction!findAcceptInfos.page` 至：
`/amOnline/app/monitorspot/spotAction!findAcceptInfos.page.arc`

推理： 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。
测试请求和响应：

```
GET /amOnline/app/monitorspot/spotAction!findAcceptInfos.page.arc HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:54:18 GMT
Set-Cookie: JSESSIONID=3129D2C15E1A37DEF5CA20B90BF8A653; Path=/amOnline; HttpOnly

{
```

```
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 5 / 5

TOC

归档文件下载

严重性:	低
CVSS 分数:	5.0
URL:	http://172.20.7.168:8083/amonline/app/monitorspot/stopaction!findstopinfos.page
实体:	stopAction!findStopInfos.page (Page)
风险:	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因:	在生产环境中留下临时文件
固定值:	除去虚拟目录中的旧版本文件

差异: **cookie** 已从请求除去: `57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去: `2019-04-24`
参数 已从请求除去: `2019-06-24`
方法 从以下位置进行控制: `POST` 至: `GET`
主体 从以下位置进行控制: `pageNo=1&pageSize=20&showPageInfo=true&showPageList=false` 至:
标题 已从请求除去: `application/x-www-form-urlencoded; charset=UTF-8`
路径 从以下位置进行控制: `/amOnline/app/monitorspot/stopAction!findStopInfos.page` 至: `/amOnline/app/monitorspot/stopAction!findStopInfos.page.arc`

推理: 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。
测试请求和响应:

```
GET /amOnline/app/monitorspot/stopAction!findStopInfos.page.arc HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:54:19 GMT
Set-Cookie: JSESSIONID=61F52EE7EF3F0EDFCB6A8961E27445C5; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

低 检测到文件替代版本 13 TOC

问题 1 / 13 TOC

检测到文件替代版本	
严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/psinfo/psinfo!view.page
实体：	psInfo!view.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制： `/amOnline/app/psinfo/psInfo!view.page` 至： `/amOnline/app/psinfo/.psInfo!view.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/psinfo/.psInfo!view.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

问题 2 / 13

TOC

检测到文件替代版本

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!history.page
实体：	onlineAction!history.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/onlinemon/onlineAction!history.page` 至：`/amOnline/app/onlinemon/.onlineAction!history.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/onlinemon/.onlineAction!history.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

问题 3 / 13

TOC

检测到文件替代版本	
严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!list.page
实体：	spotAction!list.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/monitorspot/spotAction!list.page` 至：`/amOnline/app/monitorspot/Old%20spotAction!list.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/monitorspot/Old%20spotAction!list.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

问题 4 / 13

TOC

检测到文件替代版本

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/stopaction!list.page
实体：	stopAction!list.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/monitorspot/stopAction!list.page` 至：`/amOnline/app/monitorspot/_stopAction!list.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/monitorspot/_stopAction!list.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

检测到文件替代版本

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/revisedmanage/revisedaction!list.page
实体：	revisedAction!list.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/revisedmanage/revisedAction!list.page` 至：`/amOnline/app/revisedmanage/.revisedAction!list.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/revisedmanage/.revisedAction!list.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

检测到文件替代版本

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/account/accountaction!list.page
实体：	accountAction!list.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/account/accountAction!list.page` 至：`/amOnline/app/account/.accountAction!list.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/account/.accountAction!list.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

检测到文件替代版本

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/loginfo/loginfoaction!list.page
实体：	loginfoAction!list.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/loginfo/loginfoAction!list.page` 至：`/amOnline/app/loginfo/Old%20loginfoAction!list.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/loginfo/Old%20loginfoAction!list.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

检测到文件替代版本

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/applogin.page
实体：	AppLogin.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制： `/amOnline/app/AppLogin.page` 至： `/amOnline/app/_AppLogin.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/_AppLogin.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=DD5A70E857941E31A168272200273FE6
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

检测到文件替代版本

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/psinfo/psinfo!listpsinfo.page
实体：	psInfo!listPsInfo.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **cookie** 已从请求除去：`57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去：`1561348464198`
路径 从以下位置进行控制：`/amOnline/app/psinfo/psInfo!listPsInfo.page` 至：
`/amOnline/app/psinfo/.psInfo!listPsInfo.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/psinfo/.psInfo!listPsInfo.page?psid= HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:54:16 GMT
Set-Cookie: JSESSIONID=290EE5A894D8E7326DF31202E4979C3C; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "       您没有登录或会话已过期,请重新登录"
}
```

检测到文件替代版本

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/abnormity/abnormityaction!jsonlist.page
实体：	abnormityAction!jsonList.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **cookie** 已从请求除去：`57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去：`2019-04-24`
参数 已从请求除去：`2019-06-24`
方法 从以下位置进行控制：`POST` 至：`GET`
主体 从以下位置进行控制：
`search_alarmType=2&search_disposeType=1&pageNo=1&pageSize=15&showPageInfo=true&showPageList=false`
至：
标题 已从请求除去：`application/x-www-form-urlencoded; charset=UTF-8`
路径 从以下位置进行控制：`/amOnline/app/abnormity/abnormityAction!jsonList.page` 至：
`/amOnline/app/abnormity/_abnormityAction!jsonList.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/abnormity/_abnormityAction!jsonList.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:54:15 GMT
Set-Cookie: JSESSIONID=58DCFDDD4FAC3E3452D7EE16E0E362A2; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

检测到文件替代版本

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!getpollutantswithpsid.page
实体：	onlineAction!getPollutantsWithPsID.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`
方法 从以下位置进行控制： `POST` 至： `GET`
路径 从以下位置进行控制： `/amOnline/app/onlinemon/onlineAction!getPollutantsWithPsID.page`
至： `/amOnline/app/onlinemon/_onlineAction!getPollutantsWithPsID.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/onlinemon/_onlineAction!getPollutantsWithPsID.page?psID=510101055565 HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:54:16 GMT
Set-Cookie: JSESSIONID=414FDACDEA9165C8ABA6EA9453E116F7; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

检测到文件替代版本

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!findacceptinfos.page
实体：	spotAction!findAcceptInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **cookie** 已从请求除去：`57A6A5AE8E37C43B017578F75A282932`
方法 从以下位置进行控制：`POST` 至：`GET`
主体 从以下位置进行控制：`search_acceptStatus=-99&search_pageNo=1&search_pageSize=20` 至：
标题 已从请求除去：`application/x-www-form-urlencoded; charset=UTF-8`
路径 从以下位置进行控制：`/amOnline/app/monitorspot/spotAction!findAcceptInfos.page` 至：
`/amOnline/app/monitorspot/_spotAction!findAcceptInfos.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/monitorspot/_spotAction!findAcceptInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:54:19 GMT
Set-Cookie: JSESSIONID=337D0C18CCB685B2B3D4073B217BFE49; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

检测到文件替代版本

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/stopaction!findstopinfos.page
实体：	stopAction!findStopInfos.page (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **cookie** 已从请求除去：`57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去：`2019-04-24`
参数 已从请求除去：`2019-06-24`
方法 从以下位置进行控制：`POST` 至：`GET`
主体 从以下位置进行控制：`pageNo=1&pageSize=20&showPageInfo=true&showPageList=false` 至：
标题 已从请求除去：`application/x-www-form-urlencoded; charset=UTF-8`
路径 从以下位置进行控制：`/amOnline/app/monitorspot/stopAction!findStopInfos.page` 至：
`/amOnline/app/monitorspot/_stopAction!findStopInfos.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/monitorspot/_stopAction!findStopInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:54:19 GMT
Set-Cookie: JSESSIONID=2DFDEBB1C0E9A402A9B5E80D7BDE9FD6; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

低 临时文件下载 23 TOC

问题 1 / 23

TOC

临时文件下载	
严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/psinfo/psinfo!view.page
实体：	psInfo!view.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/psinfo/psInfo!view.page` 至：`/amOnline/app/psinfo/Copy%20of%20psInfo!view.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/psinfo/Copy%20of%20psInfo!view.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

问题 2 / 23

TOC

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/appmain.page
实体：	AppMain.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/AppMain.page` 至：`/amOnline/app/Copy%20of%20AppMain.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/Copy%20of%20AppMain.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=DD5A70E857941E31A168272200273FE6
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

问题 3 / 23

TOC

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!history.page
实体：	onlineAction!history.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/onlinemon/onlineAction!history.page` 至：`/amOnline/app/onlinemon/Copy%20of%20onlineAction!history.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/onlinemon/Copy%20of%20onlineAction!history.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

问题 4 / 23

TOC

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!list.page
实体：	spotAction!list.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/monitorspot/spotAction!list.page` 至：`/amOnline/app/monitorspot/Copy%20of%20spotAction!list.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/monitorspot/Copy%20of%20spotAction!list.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

问题 5 / 23

TOC

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/stopaction!list.page
实体：	stopAction!list.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/monitorspot/stopAction!list.page` 至：`/amOnline/app/monitorspot/Copy%20of%20stopAction!list.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/monitorspot/Copy%20of%20stopAction!list.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/revisedmanage/revisedaction!list.page
实体：	revisedAction!list.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/revisedmanage/revisedAction!list.page` 至：`/amOnline/app/revisedmanage/Copy%20of%20revisedAction!list.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/revisedmanage/Copy%20of%20revisedAction!list.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/account/accountaction!list.page
实体：	accountAction!list.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/account/accountAction!list.page` 至：`/amOnline/app/account/Copy%20of%20accountAction!list.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/account/Copy%20of%20accountAction!list.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/loginfo/loginfoaction!list.page
实体：	loginfoAction!list.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/loginfo/loginfoAction!list.page` 至：`/amOnline/app/loginfo/Copy%20of%20loginfoAction!list.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/loginfo/Copy%20of%20loginfoAction!list.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/abnormity/abnormityaction!jsonlist.page
实体：	abnormityAction!jsonList.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **cookie** 已从请求除去：`57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去：`2019-04-24`
参数 已从请求除去：`2019-06-24`
方法 从以下位置进行控制：`POST` 至：`GET`
主体 从以下位置进行控制：
`search_alarmType=2&search_disposeType=1&pageNo=1&pageSize=15&showPageInfo=true&showPageList=false`
至：
标题 已从请求除去：`application/x-www-form-urlencoded; charset=UTF-8`
路径 从以下位置进行控制：`/amOnline/app/abnormity/abnormityAction!jsonList.page` 至：
`/amOnline/app/abnormity/abnormityAction!jsonList.sav`

推理： 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。
测试请求和响应：

```
GET /amOnline/app/abnormity/abnormityAction!jsonList.sav HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:54:14 GMT
Set-Cookie: JSESSIONID=CCEA2021EE811FACAAAE6EBDE2509DF9; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/psinfo/psinfo!listpsinfo.page
实体：	psInfo!listPsInfo.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **cookie** 已从请求除去：`57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去：`1561348464198`
路径 从以下位置进行控制：`/amOnline/app/psinfo/psInfo!listPsInfo.page` 至：`/amOnline/app/psinfo/psInfo!listPsInfo.old`

推理： 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。
测试请求和响应：

```
GET /amOnline/app/psinfo/psInfo!listPsInfo.old?psid= HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:54:15 GMT
Set-Cookie: JSESSIONID=F5F84B780417059F9ACF8BCDDDBCEDEA; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 11 / 23

TOC

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!getpollutantswithpsid.page
实体：	onlineAction!getPollutantsWithPsID.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`
方法 从以下位置进行控制： `POST` 至： `GET`
路径 从以下位置进行控制： `/amOnline/app/onlinemon/onlineAction!getPollutantsWithPsID.page`
至： `/amOnline/app/onlinemon/onlineAction!getPollutantsWithPsID.old`

推理： 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。
测试请求和响应：

```
GET /amOnline/app/onlinemon/onlineAction!getPollutantsWithPsID.old?psID=510101055565 HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:54:16 GMT
Set-Cookie: JSESSIONID=5F31446BA03A20249CE15FC5E8F159A3; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 12 / 23

TOC

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!findacceptinfos.page
实体：	spotAction!findAcceptInfos.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **cookie** 已从请求除去：`57A6A5AE8E37C43B017578F75A282932`
方法 从以下位置进行控制：`POST` 至：`GET`
主体 从以下位置进行控制：`search_acceptStatus=-99&search_pageNo=1&search_pageSize=20` 至：
标题 已从请求除去：`application/x-www-form-urlencoded; charset=UTF-8`
路径 从以下位置进行控制：`/amOnline/app/monitorspot/spotAction!findAcceptInfos.page` 至：`/amOnline/app/monitorspot/spotAction!findAcceptInfos.old`

推理： 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。
测试请求和响应：

```
GET /amOnline/app/monitorspot/spotAction!findAcceptInfos.old HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:54:18 GMT
Set-Cookie: JSESSIONID=7195EE4450298BDFE362B433E768433D; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 13 / 23

TOC

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/onlinemon/admin/onlineaction!getpollutantswithpsid.page
实体：	onlineAction!getPollutantsWithPsID.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：
`/amOnline/app/onlinemon/admin/onlineAction!getPollutantsWithPsID.page` 至：
`/amOnline/app/onlinemon/admin/Copy%20of%20onlineAction!getPollutantsWithPsID.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/onlinemon/admin/Copy%20of%20onlineAction!getPollutantsWithPsID.page?
psID=510101055565 HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:01:05 GMT
Set-Cookie: JSESSIONID=C647F3A873CF1F1FED62D166D155F8E6; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 14 / 23

TOC

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/stopaction!findstopinfos.page
实体：	stopAction!findStopInfos.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **cookie** 已从请求除去：`57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去：`2019-04-24`
参数 已从请求除去：`2019-06-24`
方法 从以下位置进行控制：`POST` 至：`GET`
主体 从以下位置进行控制：`pageNo=1&pageSize=20&showPageInfo=true&showPageList=false` 至：
标题 已从请求除去：`application/x-www-form-urlencoded; charset=UTF-8`
路径 从以下位置进行控制：`/amOnline/app/monitorspot/stopAction!findStopInfos.page` 至：
`/amOnline/app/monitorspot/stopAction!findStopInfos.old`

推理： 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。
测试请求和响应：

```
GET /amOnline/app/monitorspot/stopAction!findStopInfos.old HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:54:19 GMT
Set-Cookie: JSESSIONID=17C127EA9906DA26E5C777199F025E4A; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 15 / 23

TOC

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspotadmin/spotaction!findacceptinfos.page
实体：	spotAction!findAcceptInfos.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/monitorspotadmin/spotAction!findAcceptInfos.page`
至：`/amOnline/app/monitorspotadmin/Copy%20of%20spotAction!findAcceptInfos.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/monitorspotadmin/Copy%20of%20spotAction!findAcceptInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:01:06 GMT
Set-Cookie: JSESSIONID=4CC25200D0392225EEA134DA30E3F677; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 16 / 23

TOC

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/abnormity/admin/abnormityaction!jsonlist.page
实体：	abnormityAction!jsonList.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/abnormity/admin/abnormityAction!jsonList.page` 至：`/amOnline/app/abnormity/admin/Copy%20of%20abnormityAction!jsonList.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/abnormity/admin/Copy%20of%20abnormityAction!jsonList.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:01:00 GMT
Set-Cookie: JSESSIONID=3E76B3E252C343B523B2C985F4F436BB; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 17 / 23

TOC

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/admin/stopaction!findstopinfos.page
实体：	stopAction!findStopInfos.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/monitorspot/admin/stopAction!findStopInfos.page`
至：`/amOnline/app/monitorspot/admin/Copy%20of%20stopAction!findStopInfos.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/monitorspot/admin/Copy%20of%20stopAction!findStopInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:01:09 GMT
Set-Cookie: JSESSIONID=7BB3BF6BE379964E73AF17387D00EA75; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/admin/spotaction!findacceptinfos.page
实体：	spotAction!findAcceptInfos.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/monitorspot/admin/spotAction!findAcceptInfos.page`
至：`/amOnline/app/monitorspot/admin/Copy%20of%20spotAction!findAcceptInfos.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/monitorspot/admin/Copy%20of%20spotAction!findAcceptInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:01:08 GMT
Set-Cookie: JSESSIONID=DBBF120B0759E9E4F0AA43B43416B490; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspotadmin/stopaction!findstopinfos.page
实体：	stopAction!findStopInfos.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/monitorspotadmin/stopAction!findStopInfos.page`
至：`/amOnline/app/monitorspotadmin/Copy%20of%20stopAction!findStopInfos.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/monitorspotadmin/Copy%20of%20stopAction!findStopInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:01:08 GMT
Set-Cookie: JSESSIONID=FF336C97EE9D66F66F187650E28107DA; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/psinfoadmin/psinfo!listpsinfo.page
实体：	psInfo!listPsInfo.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/psinfoadmin/psInfo!listPsInfo.page` 至：`/amOnline/app/psinfoadmin/Copy%20of%20psInfo!listPsInfo.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/psinfoadmin/Copy%20of%20psInfo!listPsInfo.page?psid= HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:01:03 GMT
Set-Cookie: JSESSIONID=D108678749C75FA3C2FAC8576E75C68A; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 21 / 23

TOC

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/onlinemonadmin/onlineaction!getpollutantswithpsid.page
实体：	onlineAction!getPollutantsWithPsID.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：
`/amOnline/app/onlinemonadmin/onlineAction!getPollutantsWithPsID.page` 至：
`/amOnline/app/onlinemonadmin/Copy%20of%20onlineAction!getPollutantsWithPsID.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/onlinemonadmin/Copy%20of%20onlineAction!getPollutantsWithPsID.page?
psID=510101055565 HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:01:03 GMT
Set-Cookie: JSESSIONID=D1A60EE5E6B554B96E0BCC6C33BDBFB3; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 22 / 23

TOC

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/abnormityadmin/abnormityaction!jsonlist.page
实体：	abnormityAction!jsonList.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/abnormityadmin/abnormityAction!jsonList.page` 至：`/amOnline/app/abnormityadmin/Copy%20of%20abnormityAction!jsonList.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/abnormityadmin/Copy%20of%20abnormityAction!jsonList.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:01:00 GMT
Set-Cookie: JSESSIONID=CA11BF381B78A2EC0466F029E6AC9261; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/psinfo/admin/psinfo!listpsinfo.page
实体：	psInfo!listPsInfo.page (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

差异： **路径** 从以下位置进行控制：`/amOnline/app/psinfo/admin/psInfo!listPsInfo.page` 至：`/amOnline/app/psinfo/admin/Copy%20of%20psInfo!listPsInfo.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/psinfo/admin/Copy%20of%20psInfo!listPsInfo.page?psid= HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 04:01:03 GMT
Set-Cookie: JSESSIONID=5698F38966AEFE013170C368F5373711; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

低 直接访问管理页面 12

TOC

问题 1 / 12

TOC

直接访问管理页面

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/psinfo/psinfo!view.page
实体：	psInfo!view.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	将适当的授权应用到管理脚本

差异： **路径** 从以下位置进行控制：`/amOnline/app/psinfo/psInfo!view.page` 至：`/amOnline/app/psinfoadmin/psInfo!view.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/psinfoadmin/psInfo!view.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

问题 2 / 12

TOC

直接访问管理页面

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!history.page
实体：	onlineAction!history.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	将适当的授权应用到管理脚本

差异： **路径** 从以下位置进行控制：`/amOnline/app/onlinemon/onlineAction!history.page` 至：`/amOnline/app/onlinemonadmin/onlineAction!history.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/onlinemonadmin/onlineAction!history.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

直接访问管理页面

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!list.page
实体：	spotAction!list.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	将适当的授权应用到管理脚本

差异： **路径** 从以下位置进行控制：`/amOnline/app/monitorspot/spotAction!list.page` 至：`/amOnline/app/monitorspotadmin/spotAction!list.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/monitorspotadmin/spotAction!list.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

直接访问管理页面

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/stopaction!list.page
实体：	stopAction!list.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	将适当的授权应用到管理脚本

差异： **路径** 从以下位置进行控制：`/amOnline/app/monitorspot/stopAction!list.page` 至：`/amOnline/app/monitorspotadmin/stopAction!list.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/monitorspotadmin/stopAction!list.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

直接访问管理页面

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/revisedmanage/revisedaction!list.page
实体：	revisedAction!list.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	将适当的授权应用到管理脚本

差异： **路径** 从以下位置进行控制：`/amOnline/app/revisedmanage/revisedAction!list.page` 至：`/amOnline/app/revisedmanageadmin/revisedAction!list.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/revisedmanageadmin/revisedAction!list.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

直接访问管理页面

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/account/accountaction!list.page
实体：	accountAction!list.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	将适当的授权应用到管理脚本

差异： **路径** 从以下位置进行控制：`/amOnline/app/account/accountAction!list.page` 至：`/amOnline/app/accountadmin/accountAction!list.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/accountadmin/accountAction!list.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

直接访问管理页面

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/loginfo/loginfoaction!list.page
实体：	loginfoAction!list.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	将适当的授权应用到管理脚本

差异： **路径** 从以下位置进行控制：`/amOnline/app/loginfo/loginfoAction!list.page` 至：`/amOnline/app/loginfoadmin/loginfoAction!list.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
GET /amOnline/app/loginfoadmin/loginfoAction!list.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=E07562F6D54977989F74AA54CCC033DF
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 03:10:37 GMT

<html>
<head>
    <title>404</title>
    <link href="/amOnline/static/themes/exception.css" type="text/css" rel="stylesheet"/>
</head>

<body class="errorPageBg">
<div class="msgTitle">系统错误</div>
<div class="msgDetail">
<p>错误码：404</p>
<p>错误信息：您访问的功能已经被移除或不存在!</p>
</div>
</body>
</html>
```

直接访问管理页面

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/abnormity/abnormityaction!jsonlist.page
实体：	abnormityAction!jsonList.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	将适当的授权应用到管理脚本

差异： **cookie** 已从请求除去：`57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去：`2019-04-24`
参数 已从请求除去：`2019-06-24`
方法 从以下位置进行控制：`POST` 至：`GET`
主体 从以下位置进行控制：
`search_alarmType=2&search_disposeType=1&pageNo=1&pageSize=15&showPageInfo=true&showPageList=false`
至：
标题 已从请求除去：`application/x-www-form-urlencoded; charset=UTF-8`
路径 从以下位置进行控制：`/amOnline/app/abnormity/abnormityAction!jsonList.page` 至：
`/amOnline/app/abnormityadmin/abnormityAction!jsonList.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
--begin_highlight_tag---end_highlight_tag--GET /amOnline/app/--end_mark_tag--
abnormityadmin/abnormityAction!jsonList.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=1CE9604FF5F9D66D2D8C490D1BE95DAC; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

直接访问管理页面

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/psinfo/psinfo!listpsinfo.page
实体：	psInfo!listPsInfo.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	将适当的授权应用到管理脚本

差异： **cookie** 已从请求除去：`57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去：`1561348464198`
路径 从以下位置进行控制：`/amOnline/app/psinfo/psInfo!listPsInfo.page` 至：`/amOnline/app/psinfoadmin/psInfo!listPsInfo.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
--begin_highlight_tag---end_highlight_tag--GET /amO--end_mark_tag--
nline/app/psinfoadmin/psInfo!listPsInfo.page?psid= HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=64A2C6D2765D3B6FE363B2BCFCD907D4; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

直接访问管理页面

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!getpollutantswithpsid.page
实体：	onlineAction!getPollutantsWithPsID.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	将适当的授权应用到管理脚本

差异： **cookie** 已从请求除去： `57A6A5AE8E37C43B017578F75A282932`
方法 从以下位置进行控制： `POST` 至： `GET`
路径 从以下位置进行控制： `/amOnline/app/onlinemon/onlineAction!getPollutantsWithPsID.page`
至： `/amOnline/app/onlinemonadmin/onlineAction!getPollutantsWithPsID.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
--begin_highlight_tag---end_highlight_tag--GET /amOnline/app/onlinemona--end_mark_tag--
dmin/onlineAction!getPollutantsWithPsID.page?psID=510101055565 HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache
Cookie: hasshown=1


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=9AFC021927648D86F4807266101E642A; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

直接访问管理页面

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!findacceptinfos.page
实体：	spotAction!findAcceptInfos.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	将适当的授权应用到管理脚本

差异： **cookie** 已从请求除去：`57A6A5AE8E37C43B017578F75A282932`
方法 从以下位置进行控制：`POST` 至：`GET`
主体 从以下位置进行控制：`search_acceptStatus=-99&search_pageNo=1&search_pageSize=20` 至：
标题 已从请求除去：`application/x-www-form-urlencoded; charset=UTF-8`
路径 从以下位置进行控制：`/amOnline/app/monitorspot/spotAction!findAcceptInfos.page` 至：
`/amOnline/app/monitorspotadmin/spotAction!findAcceptInfos.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
--begin_highlight_tag---end_highlight_tag--GET /amOnline/app/moni--end_mark_tag--
torspotadmin/spotAction!findAcceptInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=BB27D777C28C01B1FC07B8221BBA20FB; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

问题 12 / 12

TOC

直接访问管理页面

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/monitorspot/stopaction!findstopinfos.page
实体：	stopAction!findStopInfos.page (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	将适当的授权应用到管理脚本

差异： **cookie** 已从请求除去：`57A6A5AE8E37C43B017578F75A282932`
参数 已从请求除去：`2019-04-24`
参数 已从请求除去：`2019-06-24`
方法 从以下位置进行控制：`POST` 至：`GET`
主体 从以下位置进行控制：`pageNo=1&pageSize=20&showPageInfo=true&showPageList=false` 至：
标题 已从请求除去：`application/x-www-form-urlencoded; charset=UTF-8`
路径 从以下位置进行控制：`/amOnline/app/monitorspot/stopAction!findStopInfos.page` 至：`/amOnline/app/monitorspotadmin/stopAction!findStopInfos.page`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应：

```
--begin_highlight_tag---end_highlight_tag--GET /amOnline/app/mo--end_mark_tag--
nitorspotadmin/stopAction!findStopInfos.page HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Cookie: hasshown=1
X-Requested-With: XMLHttpRequest
Referer: http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 172.20.7.168:8083
Connection: Keep-Alive
Pragma: no-cache


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 142
Date: Mon, 24 Jun 2019 03:59:36 GMT
Set-Cookie: JSESSIONID=714B3233E562CDF4EA67FF6FAF6B38B7; Path=/amOnline; HttpOnly

{
 "result": "failed",
 "targetUrl": "/amOnline/app/AppLogin.page?loginError=auth_failed",
 "msg": "        您没有登录或会话已过期,请重新登录"
}
```

低 自动填写未对密码字段禁用的 HTML 属性 1 TOC

问题 1 / 1

TOC

自动填写未对密码字段禁用的 HTML 属性

严重性：	低
CVSS 分数：	5.0
URL：	http://172.20.7.168:8083/amonline/app/applogin.page
实体：	AppLogin.page (Page)
风险：	可能会绕开 Web 应用程序的认证机制
原因：	Web 应用程序编程或配置不安全
固定值：	将“autocomplete”属性正确设置为“off”

差异：

推理： AppScan 发现密码字段没有强制禁用自动填写功能。

测试请求和响应：

```
GET /amOnline/app/AppLogin.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=AE1E776BF33CD2F26A4429E80DCAFFAA
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/j_spring_security_logout
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 02:53:31 GMT
x-ua-compatible: IE=edge,chrome=1
cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
pragma: no-cache
expires: 0

<!DOCTYPE HTML>
<html style="height:100%">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<title>重点排污单位自动监控与基础数据库系统（企业端）</title>
<link rel="shortcut icon" href="/amOnline/static/images/favicon.ico"
mce_href="/amOnline/static/images/favicon.ico" type="image/x-icon"/>
<link rel="icon" href="/amOnline/static/images/favicon.ico"/>
<meta http-equiv="Content-Type" content="text/html;charset=utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta http-equiv="Cache-Control" content="no-store, no-cache, must-revalidate, post-check=0, pre-
check=0" />
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Expires" content="0" />
<link href="/amOnline/static/script/themes/default/ui.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/themes/default/login.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/script/themes/icon.css" type="text/css" rel="stylesheet"/>
<link href="/amOnline/static/themes/default/app.css" type="text/css" rel="stylesheet"/>
<script src="/amOnline/static/script/jquery2.js" type="text/javascript"></script>
<script src="/amOnline/static/script/jquery-migrate-1.2.1.js" type="text/javascript"></script>
<script src="/amOnline/static/script/jquery.ui.js" type="text/javascript"></script>
<script src="/amOnline/static/script/locale/ui-lang-zh_CN.js" type="text/javascript"></script>
<script src="/amOnline/static/script/core.js" type="text/javascript"></script>
<script type="text/javascript">
var context = '/amOnline';
var authorizeType = '1';
```

```
var enableCaptcha = 'false';
var loginTicket = '2c9487286b79d3e4016b8767223612f4';
</script>

<script src="/amOnline/static/script/common.js" type="text/javascript"></script>
<script src="/amOnline/static/script/AppLogin.js?v=20171023" type="text/javascript"></script>

<!-- 在线客服  -->
<script src="/amOnline/static/am/vendor/zxkf/kefu.js"></script>
<link href="/amOnline/static/am/vendor/zxkf/zxkf.css" rel="stylesheet" />

<!-- 扫码登陆 -->
<script src="/amOnline/static/script/jquery.qrcode.min.js" type="text/javascript"></script>
<script src="/amOnline/static/script/qr.code.login.js" type="text/javascript"></script>

<style type="text/css">
.floatTool {
 width: 110px;
 height: 138px;
 position: absolute;
 right: 0px;
 top: 50%;
 margin-top: -69px;
 vertical-align: middle;
 text-align: center;
}

.messager-text{
    width:200px;
}
.qr_login_sm_fs{height:100px;width: 288px;margin:0px auto;text-align: center; }
.login_type_fs{float:left; width:33%;}
a.a-login-sm {text-decoration: none; color:#5b5b5b; cursor: pointer;font-size: 16px;}
a.a-login-sm:hover {color:#FF8800 ; text-decoration:none; }
</style>
</head>

<body class="login_bg">
<div style="position:absolute;width:100%;height:100%; text-align: center;">
   <img src="/amOnline/static/themes/default/images/l_m_title_info.png" style="margin-
top:270px;"/>
</div>




 <!--在线客服Begin-->
<div id="floatTools" class="rides-cs">
 <div class="floatL">
         <a style="display: block" id="aFloatTools_Show" class="btnOpen" title="       查看在线客
服" onClick="javascript:$('#divFloatToolsView').animate({width: 'show', opacity: 'show'},
'normal',function(){ $('#divFloatToolsView').show();kf_setCookie('RightFloatShown', 0, '', '/',
'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:none');$('#aFloatTools_Hide').attr('style','disp.
.. href="javascript:void(0);">
                展开</a>
         <a style="display: none" id="aFloatTools_Hide" class="btnCtn" title="       关闭在线客服"
onClick="javascript:$('#divFloatToolsView').animate({width: 'hide', opacity: 'hide'},
'normal',function(){ $('#divFloatToolsView').hide();kf_setCookie('RightFloatShown', 1, '', '/',
'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:block');$('#aFloatTools_Hide').attr('style','dis.
.. href="javascript:void(0);">
                收缩</a> </div>
 <div id="divFloatToolsView" class="floatR" style="display: none">
                 <p><img src="/amOnline/static/8.jpg" width="100px" height="100px"/></p>
                 <p><span style="text-align: left; color: rgb(255, 255, 255); font-size:
18px; font-weight: bold;">技术支持<br><span style="font-size: 14px;">7*10小时</span><br><span
style="font-size: 14px;">(08:30-18:30)</span></span></p>
 </div>
</div>




 <form name
...
...
...
```

参 HTML 注释敏感信息泄露 2 TOC

问题 1 / 2 TOC

HTML 注释敏感信息泄露

严重性：	参考信息
CVSS 分数：	0.0
URL：	http://172.20.7.168:8083/amonline/app/appmain.page
实体：	<dd>信息填报</dd> (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /amOnline/app/AppMain.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=AE1E776BF33CD2F26A4429E80DCAFFAA
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 02:53:27 GMT
x-ua-compatible: IE=edge,chrome=1

<!DOCTYPE html>
<html lang="zh-cn">
<head>
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
    <title>重点排污单位自动监控与基础数据库系统（企业端）</title>
    <link rel="stylesheet" href="/amOnline/static/layui/css/layui.css"  media="all">
    <style>
        .layui-body{
            left:0px;
        }
        .layui-side{
            width:0px;
        }
```

```
        .layui-layout-admin .layui-body{
            bottom:0px;
        }
    </style>

</head>
<body class="layui-layout-body">
<div class="layui-layout layui-layout-admin">
    <div class="layui-header layui-bg-blue">
        <div class="layui-logo">重点排污单位自动监控与基础数据库系统(企业端)</div>
        <!-- 头部区域（可配合layui已有的水平导航） -->
        <ul class="layui-nav layui-layout-right    layui-bg-blue">
            <li class="layui-nav-item layui-this"><a href="#"
onclick="loadIframe('app/psinfo/psInfo!view.page')">基本信息维护</a></li>
            <li class="layui-nav-item"  id="historyLine"><a href="#"
onclick="loadIframe('app/onlinemon/onlineAction!history.page')">数据监控</a></li>

            <li class="layui-nav-item">
                <a href="javascript:;">现场端管理</a>
                <dl class="layui-nav-child" id="xcdzhgl">
                    <dd><a href="#" onclick="loadIframe('app/monitorspot/spotAction!list.page')">
设备验收</a></dd>
                                <dd><a href="#"
onclick="loadIframe('app/monitorspot/stopAction!list.page')">停运管理</a></dd>
                                <!--<dd><a href="#"
onclick="loadIframe('app/viewmonitor/monitorDataAction!list.page')">信息填报</a></dd>   -->
                </dl>
            </li>
            <li class="layui-nav-item" id='reviseLi'><a href="#"
onclick="loadIframe('app/revisedmanage/revisedAction!list.page')">数据标记</a></li>
           <!--  <li class="layui-nav-item" ><a href="#"
onclick="loadIframe('app/revisedmanage/revisedAction!list.page')">数据标记</a></li>
            <li class="layui-nav-item" ><a href="#"
onclick="loadIframe('http://m.envsc.cn/WXIndexPSForQYD.aspx?
key=wPLFgACAKGA&pscode=140000000223&... -->
            <li class="layui-nav-item">
                <a href="javascript:;">
                    <img src="/amOnline/static/layui/images/ooopic_1509436490.png" class="layui-
nav-img">
                    黄智欢
                </a>
                <dl class="layui-nav-child">
                    <dd><a  href="#" onclick="loadIframe('app/account/accountAction!list.page')">
账户管理</a></dd>
                    <dd><a  href="#" onclick="loadIframe('app/loginfo/loginfoAction!list.page')">
操作日志</a></dd>
                    <dd><a onclick="logoutSys()" href="javascript:void(0);"  >退出系统</a></dd>
                </dl>
            </li>


        </ul>
    </div>


    <div class="layui-body">
        <iframe id="frame_lgpblpww"   src="/amOnline/app/psinfo/psInfo!view.page"
                style='width:100%; margin-right:-15px!important;margin-bottom:-14px!important;
overflow-y:scroll; overflow-x:hidden;'     >  </iframe>
    </div>



</div>
<script src="/amOnline/static/layui/layui.js" charset="utf-8"></script>
<!-- 注意：如果你直接复制所有代码到本地，上述js路径需要改成你本地的 -->
<script>


    layui.use('element', function(){
        var element = layui.element; //导航的hover效果、二级菜单等功能，需要依赖element模块

        //监听导航点击
        element.on('nav(demo)', function(elem){
            layer.msg(elem.text());
        });
    });
```

```
    function changeFrameHeight(){
        var ifm= document.getElementById("frame_lgpblpww");
        ifm.height=document.documentElement.clientHeight-64;
    }
    changeFrameHeight()
    //changeFrameHeight();
    window.onresize=function(){
        changeFrameHeight();
    }
    //退出系统
    function logoutSys(ifrSrc){
         window.location.href='/amOnline/app/j_spring_security_logout';
    }

   function loadIframe(ifrSrc){
    var ifm= document.getElementById("frame_lgpblpww");
    ifm.src='/amOnline/'+ifrSrc;
   }

   var regionCode='510101000';
   if(regionCode!=''&&regionCode.substr(0, 2)=='64'){
       document.getElementById("xcdzhgl").innerHTML = "";
       var html="";
       html+="<dd><a href=\"#\" onclick=\"loadIframe('app/monitorspot/spotAction!list.page')\">设
备验收</a></dd>";

       html+="<dd><a href=\"#\" onclick=\"loadIframe('app/viewmo
...
...
...
```

问题 2 / 2

TOC

HTML 注释敏感信息泄露

严重性：	参考信息
CVSS 分数：	0.0
URL：	http://172.20.7.168:8083/amonline/app/appmain.page
实体：	<li class="layui-nav-item" ><a href="#" onclick="loadIframe('app/revisedmanage/revisedAction!list.pa... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /amOnline/app/AppMain.page HTTP/1.1
Cookie: hasshown=1; JSESSIONID=AE1E776BF33CD2F26A4429E80DCAFFAA
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppMain.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 02:53:27 GMT
x-ua-compatible: IE=edge,chrome=1

<!DOCTYPE html>
<html lang="zh-cn">
<head>
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
    <title>重点排污单位自动监控与基础数据库系统（企业端）</title>
    <link rel="stylesheet" href="/amOnline/static/layui/css/layui.css"  media="all">
    <style>
        .layui-body{
            left:0px;
        }
        .layui-side{
            width:0px;
        }
        .layui-layout-admin .layui-body{
            bottom:0px;
        }
    </style>

</head>
<body class="layui-layout-body">
<div class="layui-layout layui-layout-admin">
    <div class="layui-header layui-bg-blue">
        <div class="layui-logo">重点排污单位自动监控与基础数据库系统(企业端)</div>
        <!-- 头部区域（可配合layui已有的水平导航） -->
        <ul class="layui-nav layui-layout-right    layui-bg-blue">
            <li class="layui-nav-item layui-this"><a href="#"
onclick="loadIframe('app/psinfo/psInfo!view.page')">基本信息维护</a></li>
            <li class="layui-nav-item"  id="historyLine"><a href="#"
onclick="loadIframe('app/onlinemon/onlineAction!history.page')">数据监控</a></li>

            <li class="layui-nav-item">
                <a href="javascript:;">现场端管理</a>
                <dl class="layui-nav-child" id="xcdzhgl">
                    <dd><a href="#" onclick="loadIframe('app/monitorspot/spotAction!list.page')">
设备验收</a></dd>
                                <dd><a href="#"
onclick="loadIframe('app/monitorspot/stopAction!list.page')">停运管理</a></dd>
                                <!--<dd><a href="#"
onclick="loadIframe('app/viewmonitor/monitorDataAction!list.page')">信息填报</a></dd>   -->
                </dl>
            </li>
            <li class="layui-nav-item" id='reviseLi'><a href="#"
onclick="loadIframe('app/revisedmanage/revisedAction!list.page')">数据标记</a></li>
          <!--  <li class="layui-nav-item" ><a href="#"
onclick="loadIframe('app/revisedmanage/revisedAction!list.page')">数据标记</a></li>
            <li class="layui-nav-item" ><a href="#"
onclick="loadIframe('http://m.envsc.cn/WXIndexPSForQYD.aspx?
key=wPLFgACAKGA&pscode=140000000223&... -->
            <li class="layui-nav-item">
                <a href="javascript:;">
                    <img src="/amOnline/static/layui/images/ooopic_1509436490.png" class="layui-
nav-img">
                    黄智欢
                </a>
                <dl class="layui-nav-child">
                    <dd><a  href="#" onclick="loadIframe('app/account/accountAction!list.page')">
账户管理</a></dd>
                    <dd><a  href="#" onclick="loadIframe('app/loginfo/loginfoAction!list.page')">
操作日志</a></dd>
                    <dd><a onclick="logoutSys()" href="javascript:void(0);"  >退出系统</a></dd>
                </dl>
            </li>


        </ul>
    </div>


    <div class="layui-body">
```

```
        <iframe id="frame_lgpblpww"   src="/amOnline/app/psinfo/psInfo!view.page"
                style='width:100%; margin-right:-15px!important;margin-bottom:-14px!important;
overflow-y:scroll; overflow-x:hidden;'     >  </iframe>
    </div>



</div>
<script src="/amOnline/static/layui/layui.js" charset="utf-8"></script>
<!-- 注意：如果你直接复制所有代码到本地，上述js路径需要改成你本地的 -->
<script>


    layui.use('element', function(){
        var element = layui.element; //导航的hover效果、二级菜单等功能，需要依赖element模块

        //监听导航点击
        element.on('nav(demo)', function(elem){
            layer.msg(elem.text());
        });
    });

    function changeFrameHeight(){
        var ifm= document.getElementById("frame_lgpblpww");
        ifm.height=document.documentElement.clientHeight-64;
    }
    changeFrameHeight()
    //changeFrameHeight();
    window.onresize=function(){
        changeFrameHeight();
    }
    //退出系统
    function logoutSys(ifrSrc){
         window.location.href='/amOnline/app/j_spring_security_logout';
    }

   function loadIframe(ifrSrc){
    var ifm= document.getElementById("frame_lgpblpww");
    ifm.src='/amOnline/'+ifrSrc;
   }

   var regionCode='510101000';
   if(regionCode!=''&&regionCode.substr(0, 2)=='64'){
       document.getElementById("xcdzhgl").innerHTML = "";
       var html="";
       html+="<dd><a href=\"#\" onclick=\"loadIframe('app/monitorspot/spotAction!list.page')\">设
备验收</a></dd>";

       html+="<dd><a href=\"#\" onclick=\"loadIframe('app/viewmo
...
...
...
```

参 应用程序错误 1 TOC

问题 1 / 1 TOC

应用程序错误

严重性：	参考信息
CVSS 分数：	0.0
URL：	http://172.20.7.168:8083/amonline/app/j_spring_security_check
实体：	j_password (Parameter)
风险：	可能会收集敏感的调试信息
原因：	未对入局参数值执行适当的边界检查 未执行验证以确保用户输入与预期的数据类型匹配
固定值：	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

差异： **参数** 从以下位置进行控制：`j_password` 至：`__ORIG_VAL__.`

推理： 应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

测试请求和响应：

```
POST /amOnline/app/j_spring_security_check HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: hasshown=1; JSESSIONID=1025D3126A59156CC2D6FC1CABC30E63
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.20.7.168:8083/amOnline/app/AppLogin.page
Host: 172.20.7.168:8083
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Content-Length: 124

j_logintype=front_user&j_lt=2c9487286b79d3e4016b8767113e12eb&j_slt=&loginType=front&j_username=1.
..

HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 6192
Vary: Accept-Encoding
Date: Mon, 24 Jun 2019 02:56:44 GMT
Connection: close
Set-Cookie: JSESSIONID=891838FE797C1182D18C6B9DD26DCDAC; Path=/amOnline; HttpOnly

<!doctype html><html lang="en"><head><title>HTTP Status 500 - Internal Server Error</title><style
type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-
color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color :
black;}A.name {color : black;}.line {height: 1px; background-color: #525D76; border: none;}
</style></head><body><h1>HTTP Status 500 - Internal Server Error</h1><hr class="line" /><p>
<b>Type</b> Exception Report</p><p><b>Description</b> The server encountered an unexpected
condition that prevented it from fulfilling the request.</p><p><b>Exception</b></p>
<pre>java.lang.NullPointerException
 com.jointsky.jointframe.security.filter.ConfigableUserAuthenticationProcessingFilter.logi
nUserP...
 com.jointsky.jointframe.security.filter.ConfigableUserAuthenticationProcessingFilter.atte
mptAut...
 org.springframework.security.web.authentication.AbstractAuthenticationProcessingFilter.do
Filter...
 org.springframework.security.web.FilterChainProxy$VirtualFilterChain.doFilter(FilterChain
Proxy....
 org.springframework.security.web.context.SecurityContextPersistenceFilter.doFilter(Securi
tyCont...
 org.springframework.security.web.FilterChainProxy$VirtualFilterChain.doFilter(FilterChain
Proxy....
 com.jointsky.jointframe.security.filter.ConcurrentSessionFilter.doFilter(ConcurrentSessio
nFilte...
 org.springframework.security.web.FilterChainProxy$VirtualFilterChain.doFilter(FilterChain
```

```
Proxy....
 com.jointsky.jointframe.security.filter.MDCFilter.doFilter(MDCFilter.java:60)
 org.springframework.security.web.FilterChainProxy$VirtualFilterChain.doFilter(FilterChain
Proxy....
 com.jointsky.jointframe.security.filter.CharacterEncodingFilter.doFilter(CharacterEncodin
gFilte...
 org.springframework.security.web.FilterChainProxy$VirtualFilterChain.doFilter(FilterChain
Proxy....
 com.jointsky.jointframe.security.filter.OsgiOpenSessionInViewFilter.doFilterInternal(Osgi
OpenSe...
 org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:10
7)
 org.springframework.security.web.FilterChainProxy$VirtualFilterChain.doFilter(FilterChain
Proxy....
 org.springframework.web.filter.RequestContextFilter.doFilterInternal(RequestContextFilter
.java:...
 org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:10
7)
 org.springframework.security.web.FilterChainProxy$VirtualFilterChain.doFilter(FilterChain
Proxy....
 org.springframework.security.web.FilterChainProxy.doFilterInternal(FilterChainProxy.java:
192)
 org.springframework.security.web.FilterChainProxy.doFilter(FilterChainProxy.java:160)
 sun.reflect.GeneratedMethodAccessor185.invoke(Unknown Source)
 sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
 java.lang.reflect.Method.invoke(Method.java:606)
 org.springframework.aop.support.AopUtils.invokeJoinpointUsingReflection(AopUtils.java:317
)
 org.springframework.osgi.service.importer.support.internal.aop.ServiceInvoker.doInvoke(Se
rviceI...
 org.springframework.osgi.service.importer.support.internal.aop.ServiceInvoker.invoke(Serv
iceInv...
 org.springframework.aop.framework.ReflectiveMethodInvocation.proceed(ReflectiveMethodInvo
cation...
 org.springframework.aop.support.DelegatingIntroductionInterceptor.doProceed(DelegatingInt
roduct...
 org.springframework.aop.support.DelegatingIntroductionInterceptor.invoke(DelegatingIntrod
uction...
 org.springframework.aop.framework.ReflectiveMethodInvocation.proceed(ReflectiveMethodInvo
cation...
 org.springframework.osgi.service.util.internal.aop.ServiceTCCLInterceptor.invokeUnprivile
ged(Se...
 org.springframework.osgi.service.util.internal.aop.ServiceTCCLInterceptor.invoke(ServiceT
CCLInt...
 org.springframework.aop.framework.Reflect
...
...
...
```

修订建议

高 查看危险字符注入的可能解决方案 TOC

该任务修复的问题类型

- 使用 SQL 注入的认证旁路

一般

有多种减轻威胁的技巧：
[1] 策略：库或框架
使用不允许此弱点出现的经过审核的库或框架，或提供更容易避免此弱点的构造。
[2] 策略：参数化
如果可用，使用自动实施数据和代码之间的分离的结构化机制。这些机制也许能够自动提供相关引用、编码和验证，而不是依赖于开发者在生成输出的每一处提供此能力。

[3] 策略：环境固化
使用完成必要任务所需的最低特权来运行代码。
[4] 策略：输出编码
如果在有风险的情况下仍需要使用动态生成的查询字符串或命令，请对参数正确地加引号并将这些参数中的任何特殊字符转义。

[5] 策略：输入验证假定所有输入都是恶意的。使用“接受已知善意”输入验证策略：严格遵守规范的可接受输入的白名单。拒绝任何没有严格遵守规范的输入，或者将其转换为遵守规范的内容。不要完全依赖于针对恶意或格式错误的输入的黑名单。但是，黑名单可帮助检测潜在攻击，或者确定哪些输入格式不正确，以致应当将其彻底拒绝。

.Net

以下是保护 Web 应用程序免遭 SQL 注入攻击的两种可行方法：

[1] 使用存储过程，而不用动态构建的 SQL 查询字符串。 将参数传递给 SQL Server 存储过程的方式，可防止使用单引号和连字符。

以下是如何在 ASP.NET 中使用存储过程的简单示例：

```
' Visual Basic example
Dim DS As DataSet
Dim MyConnection As SqlConnection
Dim MyCommand As SqlDataAdapter
```

```
Dim SelectCommand As String = "select * from users where username = @username"
...
MyCommand.SelectCommand.Parameters.Add(New SqlParameter("@username", SqlDbType.NVarChar, 20))
MyCommand.SelectCommand.Parameters("@username").Value = UserNameField.Value


// C# example
String selectCmd = "select * from Authors where state = @username";
SqlConnection myConnection = new SqlConnection("server=...");
SqlDataAdapter myCommand = new SqlDataAdapter(selectCmd, myConnection);

myCommand.SelectCommand.Parameters.Add(new SqlParameter("@username", SqlDbType.NVarChar, 20));
myCommand.SelectCommand.Parameters["@username"].Value = UserNameField.Value;
```

[2] 您可以使用验证控件，将输入验证添加到“Web 表单”页面。 验证控件提供适用于所有常见类型的标准验证的易用机制 — 例如，测试验证日期是否有效，或验证值是否在范围内 — 以及进行定制编写验证的方法。此外，验证控件还使您能够完整定制向用户显示错误信息的方式。验证控件可搭配“Web 表单”页面的类文件中处理的任何控件使用，其中包括 HTML 和 Web 服务器控件。
为了确保用户输入仅包含有效值，您可以使用以下其中一种验证控件：
a. “RangeValidator”：检查用户条目（值）是否在指定的上下界限之间。 您可以检查配对数字、字母字符和日期内的范围。
b. “RegularExpressionValidator”：检查条目是否与正则表达式定义的模式相匹配。 此类型的验证使您能够检查可预见的字符序列，如社会保险号码、电子邮件地址、电话号码、邮政编码等中的字符序列。
重要注意事项：验证控件不会阻止用户输入或更改页面处理流程；它们只会设置错误状态，并产生错误消息。程序员的职责是，在执行进一步的应用程序特定操作前，测试代码中控件的状态。
有两种方法可检查用户输入的有效性：
1. 测试常规错误状态：
在您的代码中，测试页面的 IsValid 属性。该属性会将页面上所有验证控件的 IsValid 属性值汇总（使用逻辑 AND）。如果将其中一个验证控件设置为无效，那么页面属性将会返回 false。
2. 测试个别控件的错误状态：
在页面的“验证器”集合中循环，该集合包含对所有验证控件的引用。然后，您就可以检查每个验证控件的 IsValid 属性。

J2EE

** 预编译语句：

以下是保护应用程序免遭 SQL 注入（即恶意篡改 SQL 参数）的三种可行方法。 使用以下方法，而非动态构建 SQL 语句：

[1] PreparedStatement，通过预编译并且存储在 PreparedStatement 对象池中。 PreparedStatement 定义 setter 方法，以注册与受支持的 JDBC SQL 数据类型兼容的输入参数。 例如，setString 应该用于 VARCHAR 或 LONGVARCHAR 类型的输入参数（请参阅 Java API，以获取进一步的详细信息）。 通过这种方法来设置输入参数，可防止攻击者通过注入错误字符（如单引号）来操纵 SQL 语句。

如何在 J2EE 中使用 PreparedStatement 的示例：

```
// J2EE PreparedStatemenet Example
// Get a connection to the database
Connection myConnection;
if (isDataSourceEnabled()) {
    // using the DataSource to get a managed connection
    Context ctx = new InitialContext();
    myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
} else {
    try {
        // using the DriverManager to get a JDBC connection
        Class.forName(jdbcDriverClassPath);
        myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
    } catch (ClassNotFoundException e) {
```

```
            ...
        }
    }
    ...
    try {
        PreparedStatement myStatement = myConnection.prepareStatement("select * from users where username =
?");
        myStatement.setString(1, userNameField);
        ResultSet rs = myStatement.executeQuery();
        ...
        rs.close();
    } catch (SQLException sqlException) {
        ...
    } finally {
        myStatement.close();
        myConnection.close();
    }
```

[2] CallableStatement，扩展 PreparedStatement 以执行数据库 SQL 存储过程。 该类继承 PreparedStatement 的输入 setter 方法（请参阅上面的 [1]）。

以下示例假定已创建该数据库存储过程：

```
CREATE PROCEDURE select_user (@username varchar(20))
AS SELECT * FROM USERS WHERE USERNAME = @username;
```

如何在 J2EE 中使用 CallableStatement 以执行以上存储过程的示例：

```
    // J2EE PreparedStatemenet Example
    // Get a connection to the database
    Connection myConnection;
    if (isDataSourceEnabled()) {
        // using the DataSource to get a managed connection
        Context ctx = new InitialContext();
        myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
    } else {
        try {
            // using the DriverManager to get a JDBC connection
            Class.forName(jdbcDriverClassPath);
            myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
        } catch (ClassNotFoundException e) {
            ...
        }
    }
    ...
    try {
        PreparedStatement myStatement = myConnection.prepareCall("{?= call select_user ?,?}");
        myStatement.setString(1, userNameField);
        myStatement.registerOutParameter(1, Types.VARCHAR);
        ResultSet rs = myStatement.executeQuery();
        ...
        rs.close();
    } catch (SQLException sqlException) {
        ...
    } finally {
        myStatement.close();
        myConnection.close();
    }
```

[3] 实体 Bean，代表持久存储机制中的 EJB 业务对象。 实体 Bean 有两种类型：bean 管理和容器管理。 当使用 bean 管理的持久性时，开发者负责撰写访问数据库的 SQL 代码（请参阅以上的 [1] 和 [2] 部分）。 当使用容器管理的持久性时，EJB 容器会自动生成 SQL 代码。 因此，容器要负责防止恶意尝试篡改生成的 SQL 代码。

如何在 J2EE 中使用实体 Bean 的示例：

```
// J2EE EJB Example
try {
    // lookup the User home interface
    UserHome userHome = (UserHome)context.lookup(User.class);
    // find the User remote interface
    User = userHome.findByPrimaryKey(new UserKey(userNameField));
    ...
} catch (Exception e) {
    ...
}
```

推荐使用的 JAVA 工具
不适用

参考资料
http://java.sun.com/j2se/1.4.1/docs/api/java/sql/PreparedStatement.html
http://java.sun.com/j2se/1.4.1/docs/api/java/sql/CallableStatement.html

** 输入数据验证：虽然为方便用户而在客户端层上提供数据验证，但仍必须使用 Servlet 在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 Javascript。
一份好的设计通常需要 Web 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：[1] 必需字段[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）[3] 字段长度[4] 字段范围[5] 字段选项[6] 字段模式[7] cookie 值[8] HTTP 响应好的做法是将以上例程作为“验证器”实用程序类中的静态方法实现。以下部分描述验证器类的一个示例。
[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。

如何验证必需字段的示例：

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
            isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。使用 Java 基本包装程序类，来检查是否可将字段值安全地转换为所需的基本数据类型。
验证数字字段（int 类型）的方式的示例：

```
// Java example to validate that a field is an int number
public Class Validator {
    ...
```

```
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
        try {
            Integer.parseInt(value);
            isFieldValid = true;
        } catch (Exception e) {
            isFieldValid = false;
        }
        return isFieldValid;
    }
    ...
}
...
// check if the HTTP request parameter is of type int
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

好的做法是将所有 HTTP 请求参数转换为其各自的数据类型。例如，开发者应将请求参数的“integerValue”存储在请求属性中，并按以下示例所示来使用：

```
// Example to convert the HTTP request parameter to a primitive wrapper data type
// and store this value in a request attribute for further processing
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // convert fieldValue to an Integer
    Integer integerValue = Integer.getInteger(fieldValue);
    // store integerValue in a request attribute
    request.setAttribute("fieldName", integerValue);
}
...
// Use the request attribute for further processing
Integer integerValue = (Integer)request.getAttribute("fieldName");
...
```

应用程序应处理的主要 Java 数据类型：
- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。以下示例验证 userName 字段的长度是否在 8 至 20 个字符之间：

```
// Example to validate the field length
public Class Validator {
    ...
    public static boolean validateLength(String value, int minLength, int maxLength) {
        String validatedValue = value;
        if (!validateRequired(value)) {
            validatedValue = "";
        }
        return (validatedValue.length() >= minLength &&
                    validatedValue.length() <= maxLength);
    }
    ...
}
...
```

```
String userName = request.getParameter("userName");
if (Validator.validateRequired(userName)) {
    if (Validator.validateLength(userName, 8, 20)) {
        // userName is valid, continue further processing
        ...
    }
}
```

[4] 字段范围
始终确保输入参数是在由功能需求定义的范围内。
以下示例验证输入 numberOfChoices 是否在 10 至 20 之间：

```
// Example to validate the field range
public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
            // numberOfChoices is valid, continue processing request
            ...
        }
    }
}
```

[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 SELECT HTML 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。以下示例验证用户针对允许的选项列表进行的选择：

```
// Example to validate user selection against a list of options
public Class Validator {
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
            List list = Arrays.asList(options);
            if (list != null) {
                isValidValue = list.contains(value);
            }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
// Allowed options
String[] options = {"option1", "option2", "option3");
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}
```

[6] 字段模式
始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 userName 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：^[a-zA-Z0-9]*$

Java 1.3 或更早的版本不包含任何正则表达式包。建议将“Apache 正则表达式包”（请参阅以下“资源”）与 Java 1.3 一起使用，以解决该缺乏支持的问题。执行正则表达式验证的示例：

```
// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
             RE r = new RE(expression);
             match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alpha-numeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}
```

Java 1.4 引进了一种新的正则表达式包（java.util.regex）。以下是使用新的 Java 1.4 正则表达式包的 Validator.matchPattern 修订版：

```
// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regexe.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
            match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}
```

[7] cookie 值使用 javax.servlet.http.Cookie 对象来验证 cookie 值。适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。
验证必需 cookie 值的示例：

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
```

```
            if (cookies[i].getName().equals("user")) {
                // validate the cookie value
                if (Validator.validateRequired(cookies[i].getValue()) {
                    // valid cookie value, continue processing request
                    ...
                }
            }
        }
    }
```

[8] HTTP 响应
[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，请通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：< > " ' % ;) (& +

以下示例通过将敏感字符转换为其对应的字符实体来过滤指定字符串：

```
// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
            return null;
        }
        StringBuffer result = new StringBuffer(value.length());
        for (int i=0; i<value.length(); ++i) {
            switch (value.charAt(i)) {
            case '<':
                result.append("&lt;");
                break;
            case '>':
                result.append("&gt;");
                break;
            case '"':
                result.append("&quot;");
                break;
            case '\'':
                result.append("&#39;");
                break;
            case '%':
                result.append("&#37;");
                break;
            case ';':
                result.append("&#59;");
                break;
            case '(':
                result.append("&#40;");
                break;
            case ')':
                result.append("&#41;");
                break;
            case '&':
                result.append("&amp;");
                break;
            case '+':
                result.append("&#43;");
                break;
            default:
                result.append(value.charAt(i));
                break;
        }
        return result;
    }
    ...
}
...
// Filter the HTTP response using Validator.filter
PrintWriter out = response.getWriter();
// set output response
out.write(Validator.filter(response));
out.close();
```

Java Servlet API 2.3 引进了“过滤器”，它支持拦截和转换 HTTP 请求或响应。
以下示例使用 Validator.filter 来用“Servlet 过滤器”清理响应：

```
  // Example to filter all sensitive characters in the HTTP response using a Java Filter.
  // This example is for illustration purposes since it will filter all content in the response, including
HTML tags!
  public class SensitiveCharsFilter implements Filter {
      ...
      public void doFilter(ServletRequest request,
                      ServletResponse response,
                      FilterChain chain)
              throws IOException, ServletException {

          PrintWriter out = response.getWriter();
          ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response);
          chain.doFilter(request, wrapper);

          CharArrayWriter caw = new CharArrayWriter();
          caw.write(Validator.filter(wrapper.toString()));

          response.setContentType("text/html");
          response.setContentLength(caw.toString().length());
          out.write(caw.toString());
          out.close();
      }
      ...
      public class CharResponseWrapper extends HttpServletResponseWrapper {
          private CharArrayWriter output;

          public String toString() {
              return output.toString();
          }

          public CharResponseWrapper(HttpServletResponse response){
              super(response);
              output = new CharArrayWriter();
          }

          public PrintWriter getWriter(){
              return new PrintWriter(output);
          }
      }
  }

  }
```

[8-2] 保护 cookie
在 cookie 中存储敏感数据时，确保使用 Cookie.setSecure（布尔标志）在 HTTP 响应中设置 cookie 的安全标志，以指导浏览器使用安全协议（如 HTTPS 或 SSL）发送 cookie。
保护“用户”cookie 的示例：

```
  // Example to secure a cookie, i.e. instruct the browser to
  // send the cookie using a secure protocol
  Cookie cookie = new Cookie("user", "sensitive");
  cookie.setSecure(true);
  response.addCookie(cookie);
```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：
[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 实施所有以上数据验证需求，是强

大的框架。这些规则配置在定义表单字段的输入验证规则的 XML 文件中。在缺省情况下，Struts 支持在使用 Struts“bean:write”标记撰写的所有数据上，过滤 [8] HTTP 响应中输出的危险字符。可通过设置“filter=false”标志来禁用该过滤。
Struts 定义以下基本输入验证器，但也可定义定制的验证器：
required：如果字段包含空格以外的任何字符，便告成功。
mask：如果值与掩码属性给定的正则表达式相匹配，便告成功。
range：如果值在 min 和 max 属性给定的值的范围内（(value >= min) & (value <= max)），便告成功。
maxLength：如果字段长度小于或等于 max 属性，便告成功。
minLength：如果字段长度大于或等于 min 属性，便告成功。
byte、short、integer、long、float、double：如果可将值转换为对应的基本类型，便告成功。
date：如果值代表有效日期，便告成功。可能会提供日期模式。
creditCard：如果值可以是有效的信用卡号码，便告成功。
e-mail：如果值可以是有效的电子邮件地址，便告成功。
使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```
<form-validation>
    <global>
        ...
        <validator name="required"
            classname="org.apache.struts.validator.FieldChecks"
            method="validateRequired"
            msg="errors.required">
        </validator>
        <validator name="mask"
            classname="org.apache.struts.validator.FieldChecks"
            method="validateMask"
            msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
            <!-- userName is required and is alpha-numeric case insensitive -->
            <field property="userName" depends="required,mask">
                <!-- message resource key to display if validation fails -->
                <msg name="mask" key="login.userName.maskmsg"/>
                <arg0 key="login.userName.displayname"/>
                <var>
                    <var-name>mask</var-name>
                    <var-value>^[a-zA-Z0-9]*$</var-value>
                </var>
            </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

[2] JavaServer Faces 技术
“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件和输入验证的 Java API（JSR 127）。
JavaServer Faces API 实现以下基本验证器，但可定义定制的验证器： validate_doublerange：在组件上注册 DoubleRangeValidator
validate_length：在组件上注册 LengthValidator
validate_longrange：在组件上注册 LongRangeValidator
validate_required：在组件上注册 RequiredValidator
validate_stringrange：在组件上注册 StringRangeValidator
validator：在组件上注册定制的 Validator

JavaServer Faces API 定义以下 UIInput 和 UIOutput 处理器（标记）：
input_date：接受以 java.text.Date 实例格式化的 java.util.Date
output_date：显示以 java.text.Date 实例格式化的 java.util.Date
input_datetime：接受以 java.text.DateTime 实例格式化的 java.util.Date
output_datetime：显示以 java.text.DateTime 实例格式化的 java.util.Date
input_number：显示以 java.text.NumberFormat 格式化的数字数据类型（java.lang.Number 或基本类型）

output_number：显示以 java.text.NumberFormat 格式化的数字数据类型（java.lang.Number 或基本类型）
input_text：接受单行文本字符串。
output_text：显示单行文本字符串。
input_time：接受以 java.text.DateFormat 时间实例格式化的 java.util.Date
output_time：显示以 java.text.DateFormat 时间实例格式化的 java.util.Date
input_hidden：允许页面作者在页面中包括隐藏变量
input_secret：接受不含空格的单行文本，并在输入时，将其显示为一组星号
input_textarea：接受多行文本
output_errors：显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息
output_label：将嵌套的组件显示为指定输入字段的标签
output_message：显示本地化消息

使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

引用
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java 正则表达式包 —
http://jakarta.apache.org/regexp/
Jakarta 验证器 —
http://jakarta.apache.org/commons/validator/
JavaServer Faces 技术 —
http://java.sun.com/j2ee/javaserverfaces/
** 错误处理：
许多 J2EE Web 应用程序体系结构都遵循“模型视图控制器（MVC）”模式。在该模式中，Servlet 扮演“控制器”的角色。Servlet 将应用程序处理委派给 EJB 会话 Bean（模型）之类的 JavaBean。然后，Servlet 再将请求转发给 JSP（视图），以呈现处理结果。Servlet 应检查所有的输入、输出、返回码、错误代码和已知的异常，以确保实际处理按预期进行。
数据验证可保护应用程序免遭恶意数据篡改，而有效的错误处理策略则是防止应用程序意外泄露内部错误消息（如异常堆栈跟踪）所不可或缺的。好的错误处理策略会处理以下项：
[1] 定义错误
[2] 报告错误
[3] 呈现错误
[4] 错误映射
[1] 定义错误
应避免在应用程序层（如 Servlet）中硬编码错误消息。 相反地，应用程序应该使用映射到已知应用程序故障的错误密钥。好的做法是定义错误密钥，且该错误密钥映射到 HTML 表单字段或其他 Bean 属性的验证规则。例如，如果需要“user_name”字段，其内容为字母数字，并且必须在数据库中是唯一的，那么就应定义以下错误密钥：

(a) ERROR_USERNAME_REQUIRED：该错误密钥用于显示消息，以通知用户需要“user_name”字段；
(b) ERROR_USERNAME_ALPHANUMERIC：该错误密钥用于显示消息，以通知用户“user_name”字段应该是字母数字；
(c) ERROR_USERNAME_DUPLICATE：该错误密钥用于显示消息，以通知用户“user_name”值在数据库中重复；
(d) ERROR_USERNAME_INVALID：该错误密钥用于显示一般消息，以通知用户“user_name”值无效；
好的做法是定义用于存储和报告应用程序错误的以下框架 Java 类：
- ErrorKeys：定义所有错误密钥

```
// Example: ErrorKeys defining the following error keys:
//    - ERROR_USERNAME_REQUIRED
//    - ERROR_USERNAME_ALPHANUMERIC
//    - ERROR_USERNAME_DUPLICATE
//    - ERROR_USERNAME_INVALID
//    ...
public Class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- Error：封装个别错误

```
// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public Class Error implements Serializable {

    // Constructor given a specified error key
    public Error(String key) {
        this(key, null);
    }

    // Constructor given a specified error key and array of placeholder objects
    public Error(String key, Object[] values) {
        this.key = key;
        this.values = values;
    }

    // Returns the error key
    public String getKey() {
        return this.key;
    }

    // Returns the placeholder values
    public Object[] getValues() {
        return this.values;
    }

    private String key = null;
    private Object[] values = null;
}
```

- Errors：封装错误的集合

```
// Example: Errors encapsulates the Error objects being reported to the presentation layer.
// Errors are stored in a HashMap where the key is the bean property name and value is an
// ArrayList of Error objects.
public Class Errors implements Serializable {

    // Adds an Error object to the Collection of errors for the specified bean property.
```

```
        public void addError(String property, Error error) {
            ArrayList propertyErrors = (ArrayList)errors.get(property);
            if (propertyErrors == null) {
                propertyErrors = new ArrayList();
                errors.put(property, propertyErrors);
            }
            propertyErrors.put(error);
        }

        // Returns true if there are any errors
        public boolean hasErrors() {
            return (errors.size > 0);
        }

        // Returns the Errors for the specified property
        public ArrayList getErrors(String property) {
            return (ArrayList)errors.get(property);
        }

        private HashMap errors = new HashMap();
    }
```

以下是使用上述框架类来处理“user_name”字段验证错误的示例：

```
// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
else
{
    // (c) Duplicate check validation rule
    // We assume that there is an existing UserValidationEJB session bean that implements
    // a checkIfDuplicate() method to verify if the user already exists in the database.
    try {
        ...
        if (UserValidationEJB.checkIfDuplicate(userName)) {
            errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    } catch (RemoteException e) {
        // log the error
        logger.error("Could not validate user for specified userName: " + userName);
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE);
    }
}
// set the errors object in a request attribute called "errors"
request.setAttribute("errors", errors);
...
```

[2] 报告错误
有两种方法可报告 web 层应用程序错误：
(a) Servlet 错误机制
(b) JSP 错误机制

[2-a] Servlet 错误机制
Servlet 可通过以下方式报告错误：
- 转发给输入 JSP（已将错误存储在请求属性中），或
- 使用 HTTP 错误代码参数来调用 response.sendError，或
- 抛出异常

好的做法是处理所有已知应用程序错误（如 [1] 部分所述），将这些错误存储在请求属性中，然后转发给输入 JSP。输入 JSP 应显示错误消息，并提示用户重新输入数据。以下示例阐明转发给输入 JSP（userInput.jsp）的方式：

```
// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}
```

如果 Servlet 无法转发给已知的 JSP 页面，那么第二个选项是使用 response.sendError 方法，将 HttpServletResponse.SC_INTERNAL_SERVER_ERROR（状态码 500）作为参数，来报告错误。请参阅 javax.servlet.http.HttpServletResponse 的 Javadoc，以获取有关各种 HTTP 状态码的更多详细信息。返回 HTTP 错误的示例：

```
// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
                           messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}
```

作为最后的手段，Servlet 可以抛出异常，且该异常必须是以下其中一类的子类： - RuntimeException - ServletException - IOException
[2-b] JSP 错误机制
JSP 页面通过定义 errorPage 伪指令来提供机制，以处理运行时异常，如以下示例所示：

```
    <%@ page errorPage="/errors/userValidation.jsp" %>
```

未捕获的 JSP 异常被转发给指定的 errorPage，并且原始异常设置在名称为 javax.servlet.jsp.jspException 的请求参数中。错误页面必须包括 isErrorPage 伪指令，如下所示：

```
    <%@ page isErrorPage="true" %>
```

isErrorPage 伪指令导致“exception”变量初始化为所抛出的异常对象。
[3] 呈现错误
J2SE Internationalization API 提供使应用程序资源外部化以及将消息格式化的实用程序类，其中包括：
(a) 资源束
(b) 消息格式化
[3-a] 资源束
资源束通过将本地化数据从使用该数据的源代码中分离来支持国际化。每一资源束都会为特定的语言环境存储键/值对的映射。
java.util.PropertyResourceBundle 将内容存储在外部属性文件中，对其进行使用或扩展都很常见，如以下示例所示：

```
################################################
# ErrorMessages.properties
################################################
```

```
# required user name error message
error.username.required=User name field is required

# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

可定义多种资源，以支持不同的语言环境（因此名为资源束）。例如，可定义 ErrorMessages_fr.properties 以支持该束系列的法语成员。如果请求的语言环境的资源成员不存在，那么会使用缺省成员。在以上示例中，缺省资源是 ErrorMessages.properties。应用程序（JSP 或 Servlet）会根据用户的语言环境从适当的资源检索内容。
[3-b] 消息格式化
J2SE 标准类 java.util.MessageFormat 提供使用替换占位符来创建消息的常规方法。MessageFormat 对象包含嵌入了格式说明符的模式字符串，如下所示：

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

以下是使用 ResourceBundle 和 MessageFormat 来呈现错误消息的更加全面的示例：

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public Class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }

    // Returns the error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Locale locale) {
        return getErrorMessage(errorKey, null, locale);
    }

    // Returns a formatted error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
        // Get localized ErrorMessageResource
        ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
        // Get localized error message
        String errorMessage = errorMessageResource.getString(errorKey);
        if (args != null) {
            // Format the message using the specified placeholders args
            return MessageFormat.format(errorMessage, args);
        } else {
            return errorMessage;
        }
    }

    // default environment locale
    private Locale defaultLocale = Locale.getDefaultLocale();
}
...
// Get the user's locale
Locale userLocale = request.getLocale();
// Check if there were any validation errors
Errors errors = (Errors)request.getAttribute("errors");
if (errors != null && errors.hasErrors()) {
```

```
        // iterate through errors and output error messages corresponding to the "user_name" property
        ArrayList userNameErrors = errors.getErrors("user_name");
        ListIterator iterator = userNameErrors.iterator();
        while (iterator.hasNext()) {
            // Get the next error object
            Error error = (Error)iterator.next();
            String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
            output.write(errorMessage + "\r\n");
        }
    }
```

建议定义定制 JSP 标记（如 displayErrors），以迭代处理并呈现错误消息，如以上示例所示。
[4] 错误映射
通常情况下，“Servlet 容器”会返回与响应状态码或异常相对应的缺省错误页面。可以使用定制错误页面来指定状态码或异常与 Web 资源之间的映射。好的做法是开发不会泄露内部错误状态的静态错误页面（缺省情况下，大部分 Servlet 容器都会报告内部错误消息）。该映射配置在“Web 部署描述符（web.xml）”中，如以下示例所指定：

```
<!-- Mapping of HTTP error codes and application exceptions to error pages -->
<error-page>
  <exception-type>UserValidationException</exception-type>
  <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
  <error-code>500</exception-type>
  <location>/errors/internalError.html</error-page>
</error-page>
<error-page>
...
</error-page>
...
```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：
[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator是 Java 框架，定义如上所述的错误处理机制。验证规则配置在 XML 文件中，该文件定义了表单字段的输入验证规则以及对应的验证错误密钥。Struts 提供国际化支持以使用资源束和消息格式化来构建本地化应用程序。
使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```
<form-validation>
    <global>
        ...
        <validator name="required"
            classname="org.apache.struts.validator.FieldChecks"
            method="validateRequired"
            msg="errors.required">
        </validator>
        <validator name="mask"
            classname="org.apache.struts.validator.FieldChecks"
            method="validateMask"
            msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
            <!-- userName is required and is alpha-numeric case insensitive -->
            <field property="userName" depends="required,mask">
                <!-- message resource key to display if validation fails -->
                <msg name="mask" key="login.userName.maskmsg"/>
                <arg0 key="login.userName.displayname"/>
                <var>
                    <var-name>mask</var-name>
                    <var-value>^[a-zA-Z0-9]*$</var-value>
```

```
                </var>
            </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

Struts JSP 标记库定义了有条件地显示一组累计错误消息的“errors”标记，如以下示例所示：

```
<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<html:html>
<head>
<body>
    <html:form action="/logon.do">
    <table border="0" width="100%">
    <tr>
        <th align="right">
            <html:errors property="username"/>
            <bean:message key="prompt.username"/>
        </th>
        <td align="left">
            <html:text property="username" size="16"/>
        </td>
    </tr>
    <tr>
    <td align="right">
        <html:submit><bean:message key="button.submit"/></html:submit>
    </td>
    <td align="right">
        <html:reset><bean:message key="button.reset"/></html:reset>
    </td>
    </tr>
    </table>
    </html:form>
</body>
</html:html>
```

[2] JavaServer Faces 技术
“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件、验证输入和支持国际化的 Java API（JSR 127）。

JavaServer Faces API 定义“output_errors”UIOutput 处理器，该处理器显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息。
使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

引用
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java 正则表达式包 —
http://jakarta.apache.org/regexp/
Jakarta 验证器 —
http://jakarta.apache.org/commons/validator/
JavaServer Faces 技术 —
http://java.sun.com/j2ee/javaserverfaces/

PHP

** 过滤用户输入

将任何数据传给 SQL 查询之前，应始终先使用筛选技术来适当过滤。 这无论如何强调都不为过。 过滤用户输入可让许多注入缺陷在到达数据库之前便得到更正。

** 对用户输入加引号

不论任何数据类型，只要数据库允许，便用单引号括住所有用户数据，始终是好的观念。 MySQL 允许此格式化技术。

** 转义数据值

如果使用 MySQL 4.3.0 或更新的版本，您应该用 mysql_real_escape_string() 来转义所有字符串。 如果使用旧版的 MySQL，便应该使用 mysql_escape_string() 函数。 如果未使用 MySQL，您可以选择使用特定数据库的特定换码功能。 如果不知道换码功能，您可以选择使用较一般的换码功能，例如，addslashes()。

如果使用 PEAR DB 数据库抽象层，您可以使用 DB::quote() 方法或使用 ? 之类的查询占位符，它会自动转义替换占位符的值。

参考资料
http://ca3.php.net/mysql_real_escape_string
http://ca.php.net/mysql_escape_string
http://ca.php.net/addslashes
http://pear.php.net/package-info.php?package=DB

** 输入数据验证：虽然为方便用户而在客户端层上提供数据验证，但仍必须始终在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 Javascript。
一份好的设计通常需要 Web 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：[1] 必需字段[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）[3] 字段长度[4] 字段范围[5] 字段选项[6] 字段模式[7] cookie 值[8] HTTP 响应好的做法是实现一个或多个验证每个应用程序参数的函数。以下部分描述一些检查的示例。
[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。如何验证必需字段的示例：

```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
```

```
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。[4] 字段范围
始终确保输入参数是在由功能需求定义的范围内。
[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 SELECT HTML 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。[6] 字段模式
始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 userName 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：^[a-zA-Z0-9]+$

[7] cookie 值
适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。
[8] HTTP 响应[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，开发者应通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：< > " ' % ;) (& +

PHP 包含一些自动化清理实用程序函数，如 htmlentities()：

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

此外，为了避免“跨站点脚本编制”的 UTF-7 变体，您应该显式定义响应的 Content-Type 头，例如：

```
<?php

header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] 保护 cookie
在 cookie 中存储敏感数据且通过 SSL 来传输时，请确保先在 HTTP 响应中设置 cookie 的安全标志。这将会指示浏览器仅通过 SSL 连接来使用该 cookie。
为了保护 cookie，您可以使用以下代码示例：

```
<$php

    $value = "some_value";
    $time = time()+3600;
    $path = "/application/";
    $domain = ".example.com";
    $secure = 1;

    setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);
?>
```

此外，我们建议您使用 HttpOnly 标志。当 HttpOnly 标志设置为 TRUE 时，将只能通过 HTTP 协议来访问 cookie。这意味着无法用脚本语言（如 JavaScript）来访问 cookie。该设置可有效地帮助减少通过 XSS 攻击盗用身份的情况（虽然并非所有浏览器都支持该设置）。
在 PHP 5.2.0 中添加了 HttpOnly 标志。
引用[1] 使用 HTTP 专用 cookie 来减轻“跨站点脚本编制”的影响：
http://msdn2.microsoft.com/en-us/library/ms533046.aspx
[2] PHP 安全协会：
http://phpsec.org/
[3] PHP 和 Web 应用程序安全博客（Chris Shiflett）：
http://shiflett.org/

高 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。 TOC

该任务修复的问题类型

- 已解密的登录请求

一般

1. 确保所有登录请求都以加密方式发送到服务器。
2. 请确保敏感信息，例如：
   - 用户名
   - 密码
   - 社会保险号码
   - 信用卡号码
   - 驾照号码
   - 电子邮件地址
   - 电话号码
   - 邮政编码

一律以加密方式传给服务器。

中 Configure your server to allow only required HTTP methods TOC

该任务修复的问题类型

- Authentication Bypass Using HTTP Verb Tampering

一般

If you use HTTP Method based access control, configure your web server to allow only required HTTP methods.

Make sure that the configuration indeed limits the non-listed methods:

In Apache .htaccess file: avoid using the problematic "LIMIT" directive. Use "LimitExcept" directive instead.
In JAVA EE: avoid using the <http-method> elements in access control policy.
In ASP.NET Authorization: use <deny verbs="*" users="*" /> after allowing a white list of required verbs.

中 登录之后更改会话标识符值 TOC

该任务修复的问题类型

- 会话标识未更新

一般

阻止用户操控会话标识的能力。请勿接受在登录时由用户的浏览器提供的会话标识；始终生成新会话以供用户在成功认证后登录。在对新用户会话授权之前废除任何现有会话标识。对于不为会话标识 cookie 生成新值的平台（例如 ASP），请利用辅助 cookie。在该方法中，将用户浏览器上的辅助 cookie 设置为随机值，并将会话变量设置为相同值。如果会话变量和 cookie 值从不匹配，请废除会话，并强制用户再次登录。

低 Config your server to use the "Content-Security-Policy" header TOC

该任务修复的问题类型

- Missing "Content-Security-Policy" header

一般

Configure your server to send the "Content-Security-Policy" header.

For Apache, see:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
For IIS, see:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
For nginx, see:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

低 Config your server to use the "X-Content-Type-Options" header TOC

该任务修复的问题类型

- Missing "X-Content-Type-Options" header

一般

Configure your server to send the "X-Content-Type-Options" header with value "nosniff" on all outgoing requests.

For Apache, see:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
For IIS, see:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
For nginx, see:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

低 Config your server to use the "X-XSS-Protection" header TOC

该任务修复的问题类型

- Missing "X-XSS-Protection" header

一般

Configure your server to send the "X-XSS-Protection" header with value "1" (i.e. Enabled) on all outgoing requests.

For Apache, see:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
For IIS, see:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
For nginx, see:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

低 除去 HTML 注释中的敏感信息 TOC

该任务修复的问题类型

- HTML 注释敏感信息泄露

一般

[1] 请勿在 HTML 注释中遗留任何重要信息（如文件名或文件路径）。
[2] 从生产站点注释中除去以前（或未来）站点链接的跟踪信息。
[3] 避免在 HTML 注释中放置敏感信息。
[4] 确保 HTML 注释不包括源代码片段。
[5] 确保程序员没有遗留重要信息。

低 除去虚拟目录中的旧版本文件 TOC

该任务修复的问题类型

- 归档文件下载
- 检测到文件替代版本
- 临时文件下载

一般

归档文件下载

请勿将文件的归档版本存放在虚拟 Web 服务器根目录之下。相反地，请将归档文件存放在虚拟根之外。请确保，在虚拟根目录下，只有实际在使用的文件。

检测到文件替代版本

请勿将文件的备用版本存放在虚拟 Web 服务器的根目录下。相反地，当更新站点时，请将文件删除或移动到虚拟根目录以外的目录、在这个目录中编辑文件，然后再将文件移动（或拷贝）回虚拟根目录。请确保，在虚拟根目录下，只有实际在使用的文件。

临时文件下载

请勿将文件的备份/暂存版本归档在虚拟 Web 服务器根目录之下。 这通常在编辑器“就地”编辑这些文件之时发生。 相反地，当升级站点时，请将文件移动或复制到虚拟根目录以外的目录、在这个目录中编辑文件，然后再将文件移动（或复制）回虚拟根目录。 请确保，在虚拟根目录下，只有实际在使用的文件。

低 将“autocomplete”属性正确设置为“off” TOC

该任务修复的问题类型

- 自动填写未对密码字段禁用的 HTML 属性

一般

如果“input”元素的“password”字段中缺失“autocomplete”属性，请进行添加并将其设置为“off“。
如果“autocomplete”属性设置为“on”，请将其更改为“off”。
例如：易受攻击站点：

```
<form action="AppScan.html" method="get">
    Username: <input type="text" name="firstname" /><br />
    Password: <input type="password" name="lastname" />
    <input type="submit" value="Submit" />
<form>
```

非易受攻击站点：

```
<form action="AppScan.html" method="get">
    Username: <input type="text" name="firstname" /><br />
    Password: <input type="password" name="lastname" autocomplete="off"/>
    <input type="submit" value="Submit" />
<form>
```

低 将适当的授权应用到管理脚本 TOC

该任务修复的问题类型

- 直接访问管理页面

一般

不具备适当的授权，便禁止访问管理脚本，因为攻击者可能会因而获取特许权利。

低 请勿接受在查询字符串中发送的主体参数 TOC

该任务修复的问题类型

- 查询中接受的主体参数

一般
重新对应用程序编程以禁用对查询中列出的 POST 参数的处理

低 验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常 TOC

该任务修复的问题类型

- 应用程序错误

一般
[1] 检查入局请求，以了解所有预期的参数和值是否存在。 当参数缺失时，发出适当的错误消息，或使用缺省值。
[2] 应用程序应验证其输入是否由有效字符组成（解码后）。 例如，应拒绝包含空字节（编码为 %00）、单引号、引号等的输入值。
[3] 确保值符合预期范围和类型。 如果应用程序预期特定参数具有特定集合中的值，那么该应用程序应确保其接收的值确实属于该集合。 例如，如果应用程序预期值在 10..99 范围内，那么就该确保该值确实是数字，且在 10..99 范围内。
[4] 验证数据是否属于提供给客户端的集合。
[5] 请勿在生产环境中输出调试错误消息和异常。

.Net
要在 ASP.NET 中禁用调试，请编辑 web.config 文件，使其包含以下属性：
```
<compilation
    debug="false"
/>
```

要获取更多信息，请参阅“HOW TO: Disable Debugging for ASP.NET Applications”，位置如下：
http://support.microsoft.com/default.aspx?scid=kb;en-us;815157

您可以使用验证控件，将输入验证添加到“Web 表单”页面。验证控件提供适用于所有常见类型的标准验证的易用机制（例如，测试验证日期是否有效，或验证值是否在范围内），以及进行定制编写验证的方法。此外，验证控件还使您能够完整定制向用户显示错误信息的方式。验证控件可搭配“Web 表单”页面的类文件中处理的任何控件使用，其中包括 HTML 和 Web 服务器控件。
要确保所有的必需参数都存在于请求中，请使用 "RequiredFieldValidator" 验证控件。该控件确保用户不会跳过 web 表单中的任何条目。
要确保用户输入仅包含有效值，您可以使用以下验证控件中的一种：

[1] “RangeValidator”：检查用户条目（值）是否在指定的上下界限之间。您可以检查配对数字、字母字符和日期内的范围。
[2] “RegularExpressionValidator”：检查条目是否与正则表达式定义的模式相匹配。此类型的验证使您能够检查可预见的字符序列，如社会保险号码、电子邮件地址、电话号码、邮政编码等中的字符序列。
重要注意事项：验证控件不会阻止用户输入或更改页面处理流程；它们只会设置错误状态，并产生错误消息。程序员的职责是，在执行进一步的应用程序特定操作前，测试代码中控件的状态。
有两种方法可检查用户输入的有效性：
1. 测试常规错误状态：

在您的代码中，测试页面的 IsValid 属性。该属性会将页面上所有验证控件的 IsValid 属性值汇总（使用逻辑 AND）。如果将其中一个验证控件设置为无效，那么页面属性将会返回 false。
2. 测试个别控件的错误状态：

在页面的“验证器”集合中循环，该集合包含对所有验证控件的引用。然后，您就可以检查每个验证控件的 IsValid 属性。

J2EE

** 输入数据验证：虽然为方便用户而在客户端层上提供数据验证，但仍必须使用 Servlet 在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 Javascript。
一份好的设计通常需要 Web 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：
[1] 必需字段
[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）
[3] 字段长度
[4] 字段范围
[5] 字段选项
[6] 字段模式
[7] cookie 值
[8] HTTP 响应
好的做法是将以上例程作为“验证器”实用程序类中的静态方法实现。以下部分描述验证器类的一个示例。
[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。

如何验证必需字段的示例：

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
            isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。使用 Java 基本包装程序类，来检查是否可将字段值安全地转换为所需的基本数据类型。
验证数字字段（int 类型）的方式的示例：

```
// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
        try {
            Integer.parseInt(value);
            isFieldValid = true;
        } catch (Exception e) {
            isFieldValid = false;
        }
```

```
            return isFieldValid;
        }
        ...
    }
    ...
    // check if the HTTP request parameter is of type int
    String fieldValue = request.getParameter("fieldName");
    if (Validator.validateInt(fieldValue)) {
        // fieldValue is valid, continue processing request
        ...
    }
```

好的做法是将所有 HTTP 请求参数转换为其各自的数据类型。例如，将请求参数的“integerValue”存储在请求属性中，并按以下示例所示来使用：

```
    // Example to convert the HTTP request parameter to a primitive wrapper data type
    // and store this value in a request attribute for further processing
    String fieldValue = request.getParameter("fieldName");
    if (Validator.validateInt(fieldValue)) {
        // convert fieldValue to an Integer
        Integer integerValue = Integer.getInteger(fieldValue);
        // store integerValue in a request attribute
        request.setAttribute("fieldName", integerValue);
    }
    ...
    // Use the request attribute for further processing
    Integer integerValue = (Integer)request.getAttribute("fieldName");
    ...
```

应用程序应处理的主要 Java 数据类型：
- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。以下示例验证 userName 字段的长度是否在 8 至 20 个字符之间：

```
    // Example to validate the field length
    public Class Validator {
        ...
        public static boolean validateLength(String value, int minLength, int maxLength) {
            String validatedValue = value;
            if (!validateRequired(value)) {
                validatedValue = "";
            }
            return (validatedValue.length() >= minLength &&
                        validatedValue.length() <= maxLength);
        }
        ...
    }
    ...
    String userName = request.getParameter("userName");
    if (Validator.validateRequired(userName)) {
        if (Validator.validateLength(userName, 8, 20)) {
            // userName is valid, continue further processing
            ...
        }
    }
```

[4] 字段范围
始终确保输入参数是在由功能需求定义的范围内。
以下示例验证输入 numberOfChoices 是否在 10 至 20 之间：

```
// Example to validate the field range
public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
            // numberOfChoices is valid, continue processing request
            ...
        }
    }
}
```

[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 SELECT HTML 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。以下示例验证用户针对允许的选项列表进行的选择：

```
// Example to validate user selection against a list of options
public Class Validator {
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
            List list = Arrays.asList(options);
            if (list != null) {
                isValidValue = list.contains(value);
            }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
// Allowed options
String[] options = {"option1", "option2", "option3");
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}
```

[6] 字段模式
始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 userName 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：^[a-zA-Z0-9]*$

Java 1.3 或更早的版本不包含任何正则表达式包。建议将“Apache 正则表达式包”（请参阅以下“资源”）与 Java 1.3 一起使用，以解决该缺乏支持的问题。执行正则表达式验证的示例：

```
// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
             RE r = new RE(expression);
             match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alpha-numeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}
```

Java 1.4 引进了一种新的正则表达式包 (java.util.regex)。以下是使用新的 Java 1.4 正则表达式包的 Validator.matchPattern 修订版：

```
// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regexe.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
            match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}
```

[7] cookie 值使用 javax.servlet.http.Cookie 对象来验证 cookie 值。适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。
验证必需 cookie 值的示例：

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
            // validate the cookie value
            if (Validator.validateRequired(cookies[i].getValue()) {
                // valid cookie value, continue processing request
                ...
            }
        }
```

```
        }
    }
```

[8] HTTP 响应
[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，请通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：< > " ' % ;) (& +

以下示例通过将敏感字符转换为其对应的字符实体来过滤指定字符串：

```
// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
            return null;
        }
        StringBuffer result = new StringBuffer(value.length());
        for (int i=0; i<value.length(); ++i) {
            switch (value.charAt(i)) {
            case '<':
                result.append("&lt;");
                break;
            case '>':
                result.append("&gt;");
                break;
            case '"':
                result.append("&quot;");
                break;
            case '\'':
                result.append("&#39;");
                break;
            case '%':
                result.append("&#37;");
                break;
            case ';':
                result.append("&#59;");
                break;
            case '(':
                result.append("&#40;");
                break;
            case ')':
                result.append("&#41;");
                break;
            case '&':
                result.append("&amp;");
                break;
            case '+':
                result.append("&#43;");
                break;
            default:
                result.append(value.charAt(i));
                break;
            }
        }
        return result;
    }
    ...
}
...
// Filter the HTTP response using Validator.filter
PrintWriter out = response.getWriter();
// set output response
out.write(Validator.filter(response));
out.close();
```

Java Servlet API 2.3 引进了“过滤器”，它支持拦截和转换 HTTP 请求或响应。

以下示例使用 Validator.filter 来用“Servlet 过滤器”清理响应：

```
  // Example to filter all sensitive characters in the HTTP response using a Java Filter.
  // This example is for illustration purposes since it will filter all content in the response, including
HTML tags!
  public class SensitiveCharsFilter implements Filter {
      ...
      public void doFilter(ServletRequest request,
                      ServletResponse response,
                      FilterChain chain)
              throws IOException, ServletException {

          PrintWriter out = response.getWriter();
          ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response);
          chain.doFilter(request, wrapper);

          CharArrayWriter caw = new CharArrayWriter();
          caw.write(Validator.filter(wrapper.toString()));

          response.setContentType("text/html");
          response.setContentLength(caw.toString().length());
          out.write(caw.toString());
          out.close();
      }
      ...
      public class CharResponseWrapper extends HttpServletResponseWrapper {
          private CharArrayWriter output;

          public String toString() {
              return output.toString();
          }

          public CharResponseWrapper(HttpServletResponse response){
              super(response);
              output = new CharArrayWriter();
          }

          public PrintWriter getWriter(){
              return new PrintWriter(output);
          }
      }
  }

  }
```

[8-2] 保护 cookie
在 cookie 中存储敏感数据时，确保使用 Cookie.setSecure（布尔标志）在 HTTP 响应中设置 cookie 的安全标志，以指导浏览器使用安全协议（如 HTTPS 或 SSL）发送 cookie。
保护“用户”cookie 的示例：

```
  // Example to secure a cookie, i.e. instruct the browser to
  // send the cookie using a secure protocol
  Cookie cookie = new Cookie("user", "sensitive");
  cookie.setSecure(true);
  response.addCookie(cookie);
```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：
[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 实施所有以上数据验证需求，是强大的框架。这些规则配置在定义表单字段的输入验证规则的 XML 文件中。在缺省情况下，Struts 支持在使用 Struts“bean:write”标记撰写的所有数据上，过滤 [8] HTTP 响应中输出的危险字符。可通过设置“filter=false”标志来禁用该过滤。
Struts 定义以下基本输入验证器，但也可定义定制的验证器：
required：如果字段包含空格以外的任何字符，便告成功。

mask：如果值与掩码属性给定的正则表达式相匹配，便告成功。
range：如果值在 min 和 max 属性给定的值的范围内（(value >= min) & (value <= max)），便告成功。
maxLength：如果字段长度小于或等于 max 属性，便告成功。
minLength：如果字段长度大于或等于 min 属性，便告成功。
byte、short、integer、long、float、double：如果可将值转换为对应的基本类型，便告成功。
date：如果值代表有效日期，便告成功。可能会提供日期模式。
creditCard：如果值可以是有效的信用卡号码，便告成功。
e-mail：如果值可以是有效的电子邮件地址，便告成功。
使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```
<form-validation>
    <global>
        ...
        <validator name="required"
            classname="org.apache.struts.validator.FieldChecks"
            method="validateRequired"
            msg="errors.required">
        </validator>
        <validator name="mask"
            classname="org.apache.struts.validator.FieldChecks"
            method="validateMask"
            msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
            <!-- userName is required and is alpha-numeric case insensitive -->
            <field property="userName" depends="required,mask">
                <!-- message resource key to display if validation fails -->
                <msg name="mask" key="login.userName.maskmsg"/>
                <arg0 key="login.userName.displayname"/>
                <var>
                    <var-name>mask</var-name>
                    <var-value>^[a-zA-Z0-9]*$</var-value>
                </var>
            </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

[2] JavaServer Faces 技术
“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件和输入验证的 Java API (JSR 127)。
JavaServer Faces API 实现以下基本验证器，但可定义定制的验证器： validate_doublerange：在组件上注册 DoubleRangeValidator
validate_length：在组件上注册 LengthValidator
validate_longrange：在组件上注册 LongRangeValidator
validate_required：在组件上注册 RequiredValidator
validate_stringrange：在组件上注册 StringRangeValidator
validator：在组件上注册定制的 Validator

JavaServer Faces API 定义以下 UIInput 和 UIOutput 处理器（标记）：
input_date：接受以 java.text.Date 实例格式化的 java.util.Date
output_date：显示以 java.text.Date 实例格式化的 java.util.Date
input_datetime：接受以 java.text.DateTime 实例格式化的 java.util.Date
output_datetime：显示以 java.text.DateTime 实例格式化的 java.util.Date
input_number：显示以 java.text.NumberFormat 格式化的数字数据类型（java.lang.Number 或基本类型）
output_number：显示以 java.text.NumberFormat 格式化的数字数据类型（java.lang.Number 或基本类型）
input_text：接受单行文本字符串。
output_text：显示单行文本字符串。
input_time：接受以 java.text.DateFormat 时间实例格式化的 java.util.Date
output_time：显示以 java.text.DateFormat 时间实例格式化的 java.util.Date

input_hidden：允许页面作者在页面中包括隐藏变量
input_secret：接受不含空格的单行文本，并在输入时，将其显示为一组星号
input_textarea：接受多行文本
output_errors：显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息
output_label：将嵌套的组件显示为指定输入字段的标签
output_message：显示本地化消息

使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

引用
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java 正则表达式包 —
http://jakarta.apache.org/regexp/
Jakarta 验证器 —
http://jakarta.apache.org/commons/validator/
JavaServer Faces 技术 —
http://java.sun.com/j2ee/javaserverfaces/

** 错误处理：
许多 J2EE Web 应用程序体系结构都遵循“模型视图控制器（MVC）”模式。在该模式中，Servlet 扮演“控制器”的角色。Servlet 将应用程序处理委派给 EJB 会话 Bean（模型）之类的 JavaBean。然后，Servlet 再将请求转发给 JSP（视图），以呈现处理结果。Servlet 应检查所有的输入、输出、返回码、错误代码和已知的异常，以确保实际处理按预期进行。
数据验证可保护应用程序免遭恶意数据篡改，而有效的错误处理策略则是防止应用程序意外泄露内部错误消息（如异常堆栈跟踪）所不可或缺的。好的错误处理策略会处理以下项：
[1] 定义错误
[2] 报告错误
[3] 呈现错误
[4] 错误映射
[1] 定义错误
应避免在应用程序层（如 Servlet）中硬编码错误消息。 相反地，应用程序应该使用映射到已知应用程序故障的错误密钥。好的做法是定义错误密钥，且该错误密钥映射到 HTML 表单字段或其他 Bean 属性的验证规则。例如，如果需要“user_name”字段，其内容为字母数字，并且必须在数据库中是唯一的，那么就应定义以下错误密钥：
(a) ERROR_USERNAME_REQUIRED：该错误密钥用于显示消息，以通知用户需要“user_name”字段；
(b) ERROR_USERNAME_ALPHANUMERIC：该错误密钥用于显示消息，以通知用户“user_name”字段应该是字母数字；
(c) ERROR_USERNAME_DUPLICATE：该错误密钥用于显示消息，以通知用户“user_name”值在数据库中重复；

(d) ERROR_USERNAME_INVALID：该错误密钥用于显示一般消息，以通知用户“user_name”值无效；
好的做法是定义用于存储和报告应用程序错误的以下框架 Java 类：
- ErrorKeys：定义所有错误密钥

```
// Example: ErrorKeys defining the following error keys:
//    - ERROR_USERNAME_REQUIRED
//    - ERROR_USERNAME_ALPHANUMERIC
//    - ERROR_USERNAME_DUPLICATE
//    - ERROR_USERNAME_INVALID
//    ...
public Class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- Error：封装个别错误

```
// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public Class Error implements Serializable {

    // Constructor given a specified error key
    public Error(String key) {
        this(key, null);
    }

    // Constructor given a specified error key and array of placeholder objects
    public Error(String key, Object[] values) {
        this.key = key;
        this.values = values;
    }

    // Returns the error key
    public String getKey() {
        return this.key;
    }

    // Returns the placeholder values
    public Object[] getValues() {
        return this.values;
    }

    private String key = null;
    private Object[] values = null;
}
```

- Errors：封装错误的集合

```
// Example: Errors encapsulates the Error objects being reported to the presentation layer.
// Errors are stored in a HashMap where the key is the bean property name and value is an
// ArrayList of Error objects.
public Class Errors implements Serializable {

    // Adds an Error object to the Collection of errors for the specified bean property.
    public void addError(String property, Error error) {
        ArrayList propertyErrors = (ArrayList)errors.get(property);
        if (propertyErrors == null) {
            propertyErrors = new ArrayList();
            errors.put(property, propertyErrors);
```

```
            }
            propertyErrors.put(error);
        }

        // Returns true if there are any errors
        public boolean hasErrors() {
            return (errors.size > 0);
        }

        // Returns the Errors for the specified property
        public ArrayList getErrors(String property) {
            return (ArrayList)errors.get(property);
        }

        private HashMap errors = new HashMap();
    }
```

以下是使用上述框架类来处理“user_name”字段验证错误的示例：

```
// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
else
{
    // (c) Duplicate check validation rule
    // We assume that there is an existing UserValidationEJB session bean that implements
    // a checkIfDuplicate() method to verify if the user already exists in the database.
    try {
        ...
        if (UserValidationEJB.checkIfDuplicate(userName)) {
            errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    } catch (RemoteException e) {
        // log the error
        logger.error("Could not validate user for specified userName: " + userName);
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE);
    }
}
// set the errors object in a request attribute called "errors"
request.setAttribute("errors", errors);
...
```

[2] 报告错误
有两种方法可报告 web 层应用程序错误：
(a) Servlet 错误机制
(b) JSP 错误机制

[2-a] Servlet 错误机制
Servlet 可通过以下方式报告错误：
- 转发给输入 JSP（已将错误存储在请求属性中），或
- 使用 HTTP 错误代码参数来调用 response.sendError，或
- 抛出异常

好的做法是处理所有已知应用程序错误（如 [1] 部分所述），将这些错误存储在请求属性中，然后转发给输入 JSP。输入 JSP 应显示错误消息，并提示用户重新输入数据。以下示例阐明转发给输入 JSP（userInput.jsp）的方式：

```
// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}
```

如果 Servlet 无法转发给已知的 JSP 页面，那么第二个选项是使用 response.sendError 方法，将 HttpServletResponse.SC_INTERNAL_SERVER_ERROR（状态码 500）作为参数，来报告错误。请参阅 javax.servlet.http.HttpServletResponse 的 Javadoc，以获取有关各种 HTTP 状态码的更多详细信息。

返回 HTTP 错误的示例：

```
// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
                           messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}
```

作为最后的手段，Servlet 可以抛出异常，且该异常必须是以下其中一类的子类： - RuntimeException - ServletException - IOException
[2-b] JSP 错误机制
JSP 页面通过定义 errorPage 伪指令来提供机制，以处理运行时异常，如以下示例所示：

```
    <%@ page errorPage="/errors/userValidation.jsp" %>
```

未捕获的 JSP 异常被转发给指定的 errorPage，并且原始异常设置在名称为 javax.servlet.jsp.jspException 的请求参数中。错误页面必须包括 isErrorPage 伪指令，如下所示：

```
    <%@ page isErrorPage="true" %>
```

isErrorPage 伪指令导致“exception”变量初始化为所抛出的异常对象。
[3] 呈现错误
J2SE Internationalization API 提供使应用程序资源外部化以及将消息格式化的实用程序类，其中包括：
(a) 资源束
(b) 消息格式化
[3-a] 资源束
资源束通过将本地化数据从使用该数据的源代码中分离来支持国际化。资源束通过将本地化数据从使用该数据的源代码中分离来支持国际化。每一资源束都会为特定的语言环境存储键/值对的映射。
java.util.PropertyResourceBundle 将内容存储在外部属性文件中，对其进行使用或扩展都很常见，如以下示例所示：

```
##############################################
# ErrorMessages.properties
##############################################
# required user name error message
error.username.required=User name field is required
```

```
# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

可定义多种资源，以支持不同的语言环境（因此名为资源束）。例如，可定义 ErrorMessages_fr.properties 以支持该束系列的法语成员。如果请求的语言环境的资源成员不存在，那么会使用缺省成员。在以上示例中，缺省资源是 ErrorMessages.properties。应用程序（JSP 或 Servlet）会根据用户的语言环境从适当的资源检索内容。
[3-b] 消息格式化
J2SE 标准类 java.util.MessageFormat 提供使用替换占位符来创建消息的常规方法。MessageFormat 对象包含嵌入了格式说明符的模式字符串，如下所示：

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

以下是使用 ResourceBundle 和 MessageFormat 来呈现错误消息的更加全面的示例：

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public Class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }

    // Returns the error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Locale locale) {
        return getErrorMessage(errorKey, null, locale);
    }

    // Returns a formatted error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
        // Get localized ErrorMessageResource
        ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
        // Get localized error message
        String errorMessage = errorMessageResource.getString(errorKey);
        if (args != null) {
            // Format the message using the specified placeholders args
            return MessageFormat.format(errorMessage, args);
        } else {
            return errorMessage;
        }
    }

    // default environment locale
    private Locale defaultLocale = Locale.getDefaultLocale();
}
...
// Get the user's locale
Locale userLocale = request.getLocale();
// Check if there were any validation errors
Errors errors = (Errors)request.getAttribute("errors");
if (errors != null && errors.hasErrors()) {
    // iterate through errors and output error messages corresponding to the "user_name" property
    ArrayList userNameErrors = errors.getErrors("user_name");
    ListIterator iterator = userNameErrors.iterator();
```

```
        while (iterator.hasNext()) {
            // Get the next error object
            Error error = (Error)iterator.next();
            String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
            output.write(errorMessage + "\r\n");
        }
    }
```

建议定义定制 JSP 标记（如 displayErrors），以迭代处理并呈现错误消息，如以上示例所示。
[4] 错误映射
通常情况下，“Servlet 容器”会返回与响应状态码或异常相对应的缺省错误页面。可以使用定制错误页面来指定状态码或异常与 Web 资源之间的映射。好的做法是开发不会泄露内部错误状态的静态错误页面（缺省情况下，大部分 Servlet 容器都会报告内部错误消息）。该映射配置在“Web 部署描述符（web.xml）”中，如以下示例所指定：

```
<!-- Mapping of HTTP error codes and application exceptions to error pages -->
<error-page>
  <exception-type>UserValidationException</exception-type>
  <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
  <error-code>500</exception-type>
  <location>/errors/internalError.html</error-page>
</error-page>
<error-page>
...
</error-page>
...
```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：
[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator是 Java 框架，定义如上所述的错误处理机制。验证规则配置在 XML 文件中，该文件定义了表单字段的输入验证规则以及对应的验证错误密钥。Struts 提供国际化支持以使用资源束和消息格式化来构建本地化应用程序。
使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```
<form-validation>
    <global>
        ...
        <validator name="required"
            classname="org.apache.struts.validator.FieldChecks"
            method="validateRequired"
            msg="errors.required">
        </validator>
        <validator name="mask"
            classname="org.apache.struts.validator.FieldChecks"
            method="validateMask"
            msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
            <!-- userName is required and is alpha-numeric case insensitive -->
            <field property="userName" depends="required,mask">
                <!-- message resource key to display if validation fails -->
                <msg name="mask" key="login.userName.maskmsg"/>
                <arg0 key="login.userName.displayname"/>
                <var>
                    <var-name>mask</var-name>
                    <var-value>^[a-zA-Z0-9]*$</var-value>
                </var>
            </field>
        ...
```

```
        </form>
        ...
    </formset>
</form-validation>
```

Struts JSP 标记库定义了有条件地显示一组累计错误消息的“errors”标记，如以下示例所示：

```
<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<html:html>
<head>
<body>
    <html:form action="/logon.do">
    <table border="0" width="100%">
    <tr>
        <th align="right">
            <html:errors property="username"/>
            <bean:message key="prompt.username"/>
        </th>
        <td align="left">
            <html:text property="username" size="16"/>
        </td>
    </tr>
    <tr>
    <td align="right">
        <html:submit><bean:message key="button.submit"/></html:submit>
    </td>
    <td align="right">
        <html:reset><bean:message key="button.reset"/></html:reset>
    </td>
    </tr>
    </table>
    </html:form>
</body>
</html:html>
```

[2] JavaServer Faces 技术
“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件、验证输入和支持国际化的 Java API（JSR 127）。

JavaServer Faces API 定义“output_errors”UIOutput 处理器，该处理器显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息。
使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

引用
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java 正则表达式包 —
http://jakarta.apache.org/regexp/
Jakarta 验证器 —
http://jakarta.apache.org/commons/validator/
JavaServer Faces 技术 —
http://java.sun.com/j2ee/javaserverfaces/

PHP

** 输入数据验证：虽然为方便用户而在客户端层上提供数据验证，但仍必须始终在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 Javascript。
一份好的设计通常需要 Web 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：
[1] 必需字段
[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）
[3] 字段长度
[4] 字段范围
[5] 字段选项
[6] 字段模式
[7] cookie 值
[8] HTTP 响应
好的做法是实现一个或多个验证每个应用程序参数的函数。以下部分描述一些检查的示例。
[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。如何验证必需字段的示例：

```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。[4] 字段范围
始终确保输入参数是在由功能需求定义的范围内。
[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 SELECT HTML 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。[6] 字段模式
始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 userName 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：^[a-zA-Z0-9]+$

[7] cookie 值

适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。
[8] HTTP 响应
[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，开发者应通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：< > " ' % ;) (& +

PHP 包含一些自动化清理实用程序函数，如 htmlentities()：

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

此外，为了避免“跨站点脚本编制”的 UTF-7 变体，您应该显式定义响应的 Content-Type 头，例如：

```
<?php

header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] 保护 cookie
在 cookie 中存储敏感数据且通过 SSL 来传输时，请确保先在 HTTP 响应中设置 cookie 的安全标志。这将会指示浏览器仅通过 SSL 连接来使用该 cookie。
为了保护 cookie，您可以使用以下代码示例：

```
<$php

    $value = "some_value";
    $time = time()+3600;
    $path = "/application/";
    $domain = ".example.com";
    $secure = 1;

    setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);
?>
```

此外，我们建议您使用 HttpOnly 标志。当 HttpOnly 标志设置为 TRUE 时，将只能通过 HTTP 协议来访问 cookie。这意味着无法用脚本语言（如 JavaScript）来访问 cookie。该设置可有效地帮助减少通过 XSS 攻击盗用身份的情况（虽然并非所有浏览器都支持该设置）。
在 PHP 5.2.0 中添加了 HttpOnly 标志。
引用[1] 使用 HTTP 专用 cookie 来减轻“跨站点脚本编制”的影响：
http://msdn2.microsoft.com/en-us/library/ms533046.aspx
[2] PHP 安全协会：
http://phpsec.org/
[3] PHP 和 Web 应用程序安全博客 (Chris Shiflett)：
http://shiflett.org/

咨询

使用 SQL 注入的认证旁路

TOC

测试类型：
应用程序级别测试

威胁分类：
认证不充分

原因：
未对用户输入正确执行危险字符清理

安全性风险：
可能会绕开 Web 应用程序的认证机制

受影响产品：

CWE:
566

X-Force：
8783

引用：
“Web Application Disassembly with ODBC Error Messages”（作者：David Litchfield）
SQL Injection Training Module

技术描述：
该应用程序使用的保护机制依赖于是否存在输入或依赖于输入的值，但是不可信用户可通过绕过该保护机制的方式来修改输入。在根据用户输入的值进行安全性决策（例如认证和授权）时，攻击者可绕过软件的安全保护机制。假设相关查询是：

```
SELECT COUNT(*) FROM accounts WHERE username='$user' AND password='$pass'
```

其中 $user 和 $pass 是用户输入（从调用了构造查询的脚本的 HTTP 请求中进行收集 - 来自 GET 请求查询参数，或者来自 POST 请求主体参数）。在此查询的常规用法下，值为 $user=john、$password=secret123。形成的查询如下：

```
SELECT COUNT(*) FROM accounts WHERE username='john' AND password='secret123'
```

如果数据库中没有这样的用户/密码对，预期的查询结果为 0；否则（即数据库中有名为“john”的用户，其密码为“secret123”），结果 >0。这将用作应用程序的基本认证机制。但是，攻击者可以通过提交以下值来绕过此机制：$user=john，$password=' OR '1'='1。
生成的查询如下：

```
SELECT COUNT(*) FROM accounts WHERE username='john' AND password='' OR '1'='1'
```

这表示查询（在 SQL 数据库中）对于 'john' 用户将返回 TRUE，因为表达式 1=1 永远为 true。因此，查询将返回一个正数，因而用户（攻击者）无需知道密码也将被视为有效。

已解密的登录请求

TOC

测试类型：
应用程序级别测试

威胁分类：
传输层保护不足

原因：
诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递

安全性风险：
可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息

受影响产品：

CWE:
523

X-Force：
52471

引用：

金融隐私权：The Gramm-Leach Bliley Act
Health Insurance Portability and Accountability Act (HIPAA)
Sarbanes-Oxley Act
California SB1386

技术描述：

在应用程序测试过程中，检测到将未加密的登录请求发送到服务器。由于登录过程中所使用的部分输入字段（例如：用户名、密码、电子邮件地址、社会安全号等）是个人敏感信息，因此建议通过加密连接（例如 SSL）将其发送到服务器。
任何以明文传给服务器的信息都可能被窃，稍后可用来电子欺骗身份或伪装用户。
此外，若干隐私权法规指出，用户凭证之类的敏感信息一律以加密方式传给 Web 站点。

Authentication Bypass Using HTTP Verb Tampering

TOC

测试类型：

应用程序级别测试

威胁分类：

认证不充分

原因：

Web 应用程序编程或配置不安全

安全性风险：

- 可能会升级用户特权并通过 Web 应用程序获取管理许可权
- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

受影响产品：

引用：

Bypassing VBAAC with HTTP Verb Tampering
Http Verb Tempering - Bypassing Web Authentication and Authorization

技术描述：

Many web servers allow configuring access control using HTTP Methods (a.k.a Verbs), enabling access using one or more methods.
The problem is that many of those configuration implementations ALLOW access to methods that were not listed in the access control rule, resulting in access control breach.

Sample Exploit:
BOGUS /some_protected_resource.html HTTP/1.1
host: www.vulnerable_site.com

会话标识未更新

TOC

测试类型：

应用程序级别测试

威胁分类：

会话定置

原因：

Web 应用程序编程或配置不安全

安全性风险：

可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

受影响产品：

CWE:

304

X-Force：

52863

引用：

“Session Fixation Vulnerability in Web-based Applications”，作者：Mitja Kolsek - Acros Security
PHP Manual, Session Handling Functions, Sessions and security

技术描述：

在认证用户或者以其他方式建立新用户会话时，如果不使任何现有会话标识失效，攻击者就有机会窃取已认证的会话。通常在以下情况下会观察到这样的场景：
[1] Web 应用程序在没有首先废除现有会话的情况下认证用户，也就是说，继续使用已与用户关联的会话
[2] 攻击者能够强制对用户使用已知会话标识，这样一旦用户进行认证，攻击者就有权访问已认证的会话
[3] 应用程序或容器使用可预测的会话标识。
在会话固定漏洞的普通探索过程中，攻击者在 web 应用程序上创建新会话，并记录关联的会话标识。然后，攻击者致使受害者使用该会话标识针对服务器进行关联，并可能进行认证，这样攻击者就能够通过活动会话访问用户的帐户。AppScan 发现在登录过程之前和之后的会话标识未更新，这意味着有可能发生假冒用户的情况。远程攻击者预先知道了会话标识值，就能够假冒已登录的合法用户的身份。
攻击流程：
a) 攻击者使用受害者的浏览器来打开易受攻击的站点的登录表单。
b) 一旦打开表单，攻击者就写下会话标识值，然后等待。
c) 在受害者登录到易受攻击的站点时，其会话标识不会更新。
d) 然后攻击者可利用会话标识值来假冒受害的用户，并以该用户的身份操作。
会话标识值可通过利用“跨站点脚本编制”脆弱性（导致受害者的浏览器在联系易受攻击的站点时使用预定义的会话标识）来获取，或者通过发起“会话固定”攻击（将导致站点向受害者的浏览器提供预定义的会话标识）来获取。

Missing "Content-Security-Policy" header

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

Web 应用程序编程或配置不安全

安全性风险：

- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
- 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

受影响产品：

引用：

List of useful HTTP headers
An Introduction to Content Security Policy

技术描述：

The "Content-Security-Policy" header is designed to modify the way browsers render pages, and thus to protect from various cross-site injections, including Cross-Site Scripting. It is important to set the header value correctly, in a way that will not prevent proper operation of the web site. For example, if the header is set to prevent execution of inline JavaScript, the web site must not use inline JavaScript in it's pages.

Missing "X-Content-Type-Options" header

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

Web 应用程序编程或配置不安全

安全性风险：

- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
- 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

受影响产品：

引用：

List of useful HTTP headers
Reducing MIME type security risks

技术描述：

The "X-Content-Type-Options" header (with "nosniff" value) prevents IE and Chrome from ignoring the content-type of a response.
This action may prevent untrusted content (e.g. user uploaded content) from being executed on the user browser (after a malicious naming, for example).

Missing "X-XSS-Protection" header

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

Web 应用程序编程或配置不安全

安全性风险：

- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
- 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

受影响产品：

引用：

List of useful HTTP headers
IE XSS Filter

技术描述：

The "X-XSS-Protection" header forces the Cross-Site Scripting filter into Enable mode, even if disabled by the user. This filter is built into most recent web browsers (IE 8+, Chrome 4+), and is usually enabled by default. Although it is not designed as first and only defence against Cross-Site Scripting, it acts as an additional layer of protection.

查询中接受的主体参数

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

Web 应用程序编程或配置不安全

安全性风险：

- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
- 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

受影响产品：

引用：

超文本传输协议 (HTTP/1.1) 语义和内容：
GET
POST

技术描述：

GET 请求设计的目的在于查询服务器，而 POST 请求用于提交数据。但是，除了技术目的之外，攻击查询参数比攻击主体参数更容易，因为向原始站点发送链接或在博客或注释中发布链接更容易，而且得到的结果比另一种方法更好，为了攻击带有主体参数的请求，攻击者需要创建其中包含表单的页面，当受害者访问表单时就会提交表单。
说服受害者访问他不了解的页面比让受害者访问原始站点要难很多。因此，不建议支持可到达查询字符串的主体参数。

归档文件下载

TOC

测试类型：

基础结构测试

威胁分类：

可预测资源位置

原因：

在生产环境中留下临时文件

安全性风险：
可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

受影响产品：

X-Force：
52496

引用：
WASC 威胁分类：可预期的资源位置

技术描述：
Web 服务器通常会使“公共网关接口（CGI）”文件扩展名（如 .pl）与 Perl 之类的某个处理程序相关联。 当 URL 路径结尾是 .pl 时，路径所指定的文件名会发送给 Perl 执行；文件内容不会返回给浏览器。 不过，当归档脚本文件时，会创建一个 ARC 文件。Web 服务器通常没有处理这个文件扩展名的特定处理程序。如果攻击者请求这个文件，文件内容会直接发送到浏览器。

检测到文件替代版本

TOC

测试类型：
基础结构测试

威胁分类：
信息泄露

原因：
在生产环境中留下临时文件

安全性风险：
可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

受影响产品：

X-Force：
52504

技术描述：
开发者往往会将脚本文件的备用版本留在虚拟根目录中，例如，开头是“Copy of”、“_”、“.”、“~”和“Old”的文件。当请求这些文件时，它们会显示在浏览器中。这些文件可能包含现有脚本的备用版本或旧版本。
请务必从虚拟目录下除去这些文件，因为它们可能包含用于调试的敏感信息，也可能指向通过当前脚本不可查看的站点区域。

临时文件下载

TOC

测试类型：
基础结构测试

威胁分类：
可预测资源位置

原因：
在生产环境中留下临时文件

安全性风险：
可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

受影响产品：

X-Force：
52887

引用：
WASC 威胁分类：可预期的资源位置

技术描述：
Web 服务器通常会使“公共网关接口（CGI）”文件扩展名（如 .pl）与 Perl 之类的某个处理程序相关联。 当 URL 路径结尾是 .pl 时，路径所指定的文件名会发送给 Perl 执行；文件内容不会返回给浏览器。 然而，当在适当的位置编辑脚本文件时，编辑器可以用新的文件扩展名来保存所编辑的脚本的备份副本，例如：.bak、.sav、.old、~ 等等。Web 服务器通常没有这些文件扩展名的特定处理程序。 如果攻击者请求这类文件，文件内容会直接发送到浏览器。
从虚拟目录下除去这些临时文件很重要，因为它们可能含有调试目的所用的敏感信息，也可能显露有并非当前逻辑，但仍可能受到利用的应用程序逻辑攻击。

直接访问管理页面

TOC

测试类型：
应用程序级别测试

威胁分类：
可预测资源位置

原因：
Web 服务器或应用程序服务器是以不安全的方式配置的

安全性风险：
可能会升级用户特权并通过 Web 应用程序获取管理许可权

CWE:
306

X-Force：
52579

引用：
CWE-425：直接请求（“强制浏览”）

技术描述：
公共用户可以通过简单的冲浪（即按照 Web 链接）来访问站点上的特定页面。不过，也有页面和脚本可能无法通过简单的冲浪来访问（即未链接的页面和脚本）。
攻击者也许能够通过猜测名称（例如 admin.php、admin.asp、admin.cgi、admin.html 等）来访问这些页面。
请求名称为“admin.php”的脚本的示例： http://[SERVER]/admin.php

不具备适当的授权，便不应允许访问管理脚本，因为攻击者可能会因而获取特许权利。

利用的样本：
http://[SERVER]/admin.php
http://[SERVER]/admin.asp
http://[SERVER]/admin.aspx
http://[SERVER]/admin.html
http://[SERVER]/admin.cfm
http://[SERVER]/admin.cgi

自动填写未对密码字段禁用的 HTML 属性

TOC

测试类型：
应用程序级别测试

威胁分类：
信息泄露

原因：
Web 应用程序编程或配置不安全

安全性风险：
可能会绕开 Web 应用程序的认证机制

受影响产品：

CWE:
522

X-Force：
85989

技术描述：
“autocomplete”属性已在 HTML5 标准中进行规范。W3C 的站点声明该属性有两种状态：“on”和“off”，完全忽略时等同于设置为“on”。
该页面易受攻击，因为“input”元素的“password”字段中的“autocomplete”属性没有设置为“off”。
这可能会使未授权用户（具有授权客户机的本地访问权）能够自动填写用户名和密码字段，并因此登录站点。

HTML 注释敏感信息泄露

TOC

测试类型：
应用程序级别测试

威胁分类：
信息泄露

原因：
程序员在 Web 页面上留下调试信息

安全性风险：
可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

受影响产品：

CWE:
615

X-Force：
52601

引用：
WASC 威胁分类：信息泄露
CWE-615：通过注释泄露信息

技术描述：

很多 Web 应用程序程序员使用 HTML 注释，以在需要时帮助调试应用程序。尽管添加常规注释有助于调试应用程序，但一些程序员往往会遗留重要数据（例如：与 Web 应用程序相关的文件名、旧的链接或原非供用户浏览的链接、旧的代码片段等）。

应用程序错误

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

- 未对入局参数值执行适当的边界检查
- 未执行验证以确保用户输入与预期的数据类型匹配

安全性风险：

可能会收集敏感的调试信息

受影响产品：

CWE:

550

X-Force：

52502

引用：

使用单引号入侵站点的示例，可参阅“How I hacked PacketStorm (by Rain Forest Puppy), RFP's site”
“Web Application Disassembly with ODBC Error Messages”（作者：David Litchfield）
CERT 咨询（CA-1997-25）：清理 CGI 脚本中用户提供的数据

技术描述：

如果攻击者通过伪造包含非应用程序预期的参数或参数值的请求，来探测应用程序（如以下示例所示），那么应用程序可能会进入易受攻击的未定义状态。 攻击者可以从应用程序对该请求的响应中获取有用的信息，且可利用该信息，以找出应用程序的弱点。
例如，如果参数字段是单引号括起来的字符串（如在 ASP 脚本或 SQL 查询中），那么注入的单引号将会提前终止字符串流，从而更改脚本的正常流程/语法。
错误消息中泄露重要信息的另一个原因，是脚本编制引擎、Web 服务器或数据库配置错误。

以下是一些不同的变体：
[1] 除去参数
[2] 除去参数值

[3] 将参数值设置为空值
[4] 将参数值设置为数字溢出（+/- 99999999）
[5] 将参数值设置为危险字符，如 ' " \' \") ;
[6] 将某字符串附加到数字参数值
[7] 在参数名称后追加“.”（点）或“[]”（尖括号）

应用程序数据

已访问的 URL 48

TOC

URL
http://172.20.7.168:8083/amOnline/app/AppLogin.page
http://172.20.7.168:8083/amOnline/app/AppLogin.page
http://172.20.7.168:8083/amOnline/app/j_spring_security_check
http://172.20.7.168:8083/amOnline/app/AppLogin.page
http://172.20.7.168:8083/amOnline/app/AppLogin.page?loginError=auth_failed
http://172.20.7.168:8083/amOnline/app/j_spring_security_check
http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page
http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page
http://172.20.7.168:8083/amOnline/app/AppLogin.page?loginError=auth_failed
http://172.20.7.168:8083/amOnline/app/AppLogin.page
http://172.20.7.168:8083/amOnline/app/AppLogin.page?loginError=auth_failed
http://172.20.7.168:8083/amOnline/app/AppMain.page
http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page
http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page
http://172.20.7.168:8083/amOnline/app/revisedmanage/revisedAction!list.page
http://172.20.7.168:8083/amOnline/app/account/accountAction!list.page
http://172.20.7.168:8083/amOnline/app/loginfo/loginfoAction!list.page
http://172.20.7.168:8083/amOnline/app/j_spring_security_logout
http://172.20.7.168:8083/amOnline/app/account/accountAction!list.page?search_name=1234&search_status=1234
http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page?columns=
http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page?search_startEndTimeParm=1234
http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page?search_acceptStatus=-99
http://172.20.7.168:8083/amOnline/app/revisedmanage/revisedAction!list.page?mpItem=1234&dataSourceItem=1234&dataStatusItem=1234&monitorItem=1234&dateDouble=1234
http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!jsonList.page
http://172.20.7.168:8083/amOnline/app/j_spring_security_check
http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!listPsInfo.page?psid=&_=1561344886440
http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!getPollutantsWithPsID.page?psID=510101055565
http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!findAcceptInfos.page
http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!findStopInfos.page
http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!list.page
http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page

http://172.20.7.168:8083/amOnline/app/j_spring_security_check
http://172.20.7.168:8083/amOnline/app/onlinemonadmin/onlineAction!history.page
http://172.20.7.168:8083/amOnline/app/monitorspotadmin/spotAction!list.page
http://172.20.7.168:8083/amOnline/app/monitorspotadmin/stopAction!list.page
http://172.20.7.168:8083/amOnline/app/accountadmin/accountAction!list.page
http://172.20.7.168:8083/amOnline/app/loginfoadmin/loginfoAction!list.page
http://172.20.7.168:8083/amOnline/app/abnormityadmin/abnormityAction!jsonList.page
http://172.20.7.168:8083/amOnline/app/abnormity/admin/abnormityAction!jsonList.page
http://172.20.7.168:8083/amOnline/app/psinfoadmin/psInfo!listPsInfo.page?psid=
http://172.20.7.168:8083/amOnline/app/psinfo/admin/psInfo!listPsInfo.page?psid=
http://172.20.7.168:8083/amOnline/app/onlinemonadmin/onlineAction!getPollutantsWithPsID.page?psID=510101055565
http://172.20.7.168:8083/amOnline/app/onlinemon/admin/onlineAction!getPollutantsWithPsID.page?psID=510101055565
http://172.20.7.168:8083/amOnline/app/monitorspotadmin/spotAction!findAcceptInfos.page
http://172.20.7.168:8083/amOnline/app/monitorspot/admin/spotAction!findAcceptInfos.page
http://172.20.7.168:8083/amOnline/app/monitorspotadmin/stopAction!findStopInfos.page
http://172.20.7.168:8083/amOnline/app/monitorspot/admin/stopAction!findStopInfos.page
http://172.20.7.168:8083/amOnline/app/j_spring_security_check

参数 47

TOC

名称	值	URL	类型
j_lt	2c9487286b79d3e4016b8766909512e0 2c9487286b79d3e4016b8767117d12ed	http://172.20.7.168:8083/amOnline/app/AppLogin.page	隐藏
j_logintype	front front_user	http://172.20.7.168:8083/amOnline/app/j_spring_security_check	隐藏
dataSourceItem	1234	http://172.20.7.168:8083/amOnline/app/revisedmanage/revisedAction!list.page?mpItem=1234&dataSourceItem=1234&dataStatusItem=1234&monitorItem=1234&dateDouble=1234	文本
search_startTime	2019-06-17	http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!jsonList.page	主体
comfirmPwd	Acme-Hackme Corp.	http://172.20.7.168:8083/amOnline/app/AppLogin.page	密码
j_slt		http://172.20.7.168:8083/amOnline/app/j_spring_security_check	隐藏
showPageList	false	http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!findStopInfos.page	主体
columns		http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page?columns=	隐藏
search_startTime	2019-04-24	http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!findStopInfos.page	主体

pageSize	20	http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!findStopInfos.page	主体
dataStatusItem	1234	http://172.20.7.168:8083/amOnline/app/revisedmanage/revisedAction!list.page?mpItem=1234&dataSourceItem=1234&dataStatusItem=1234&monitorItem=1234&dateDouble=1234	文本
cmUsername	1234	http://172.20.7.168:8083/amOnline/app/AppLogin.page	文本
_	1561344886440	http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!listPsInfo.page?psid=&_=1561344886440	简单链接
loginError	auth_failed	http://172.20.7.168:8083/amOnline/app/AppLogin.page?loginError=auth_failed	简单链接
showPageList	false	http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!jsonList.page	主体
psID	510101055565	http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!getPollutantsWithPsID.page?psID=510101055565	简单链接
loginType	front	http://172.20.7.168:8083/amOnline/app/AppLogin.page	隐藏
search_acceptStatus	-99	http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page?search_acceptStatus=-99	文本
mpItem	1234	http://172.20.7.168:8083/amOnline/app/revisedmanage/revisedAction!list.page?mpItem=1234&dataSourceItem=1234&dataStatusItem=1234&monitorItem=1234&dateDouble=1234	文本
j_password	hfjcd	http://172.20.7.168:8083/amOnline/app/j_spring_security_check	密码
pageSize	15	http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!jsonList.page	主体
search_startEndTimeParm	1234	http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page?search_startEndTimeParm=1234	文本
showPageInfo	true	http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!findStopInfos.page	主体
search_pageSize	20	http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!findAcceptInfos.page	主体
psID	510101055565	http://172.20.7.168:8083/amOnline/app/onlinemon/admin/onlineAction!getPollutantsWithPsID.page?psID=510101055565	简单链接
dateDouble	1234	http://172.20.7.168:8083/amOnline/app/revisedmanage/revisedAction!list.page?mpItem=1234&dataSourceItem=1234&dataStatusItem=1234&monitorItem=1234&dateDouble=1234	文本
pageNo	1	http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!jsonList.page	主体
showPageInfo	true	http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!jsonList.page	主体
j_lt	2c9487286b79d3e4016b8767113e12eb	http://172.20.7.168:8083/amOnline/app/j_spring_security_check	隐藏
pageNo	1	http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!findStopInfos.page	主体

search_alarmType	2	http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!jsonList.page	主体
newPwd	hfjcd	http://172.20.7.168:8083/amOnline/app/AppLogin.page	密码
verificationCode	1234	http://172.20.7.168:8083/amOnline/app/AppLogin.page	文本
psid		http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!listPsInfo.page?psid=&_=1561344886440	简单链接
search_endTime	2019-06-24	http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!findStopInfos.page	主体
search_disposeType	1	http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!jsonList.page	主体
search_name	1234	http://172.20.7.168:8083/amOnline/app/account/accountAction!list.page?search_name=1234&search_status=1234	文本
search_acceptStatus	-99	http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!findAcceptInfos.page	主体
psid		http://172.20.7.168:8083/amOnline/app/psinfoadmin/psInfo!listPsInfo.page?psid=	简单链接
psID	510101055565	http://172.20.7.168:8083/amOnline/app/onlinemonadmin/onlineAction!getPollutantsWithPsID.page?psID=510101055565	简单链接
psid		http://172.20.7.168:8083/amOnline/app/psinfo/admin/psInfo!listPsInfo.page?psid=	简单链接
search_endTime	2019-06-24	http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!jsonList.page	主体
j_username	13981937605	http://172.20.7.168:8083/amOnline/app/j_spring_security_check	文本
monitorItem	1234	http://172.20.7.168:8083/amOnline/app/revisedmanage/revisedAction!list.page?mpItem=1234&dataSourceItem=1234&dataStatusItem=1234&monitorItem=1234&dateDouble=1234	文本
search_status	1234	http://172.20.7.168:8083/amOnline/app/account/accountAction!list.page?search_name=1234&search_status=1234	文本
search_pageNo	1	http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!findAcceptInfos.page	主体
loginType	front	http://172.20.7.168:8083/amOnline/app/j_spring_security_check	隐藏

失败的请求 13

TOC

URL	原因
http://172.20.7.168:8083/amOnline/app/psinfo/static/am/template/psinfo/opt/deleteInfo.html	响应状态“404” — 找不到

http://172.20.7.168:8083/amOnline/app/psinfo/static/am/template/psinfo/setFlowRlation.html	响应状态“404” — 找不到
http://172.20.7.168:8083/amOnline/app/psinfo/static/am/template/psinfo/setInstallationLocation.html	响应状态“404” — 找不到
http://172.20.7.168:8083/amOnline/app/psinfo/static/am/template/psinfo/monitorItem_watermp.html	响应状态“404” — 找不到
http://172.20.7.168:8083/amOnline/app/psinfo/static/am/template/psinfo/monitorItem_airmp.html	响应状态“404” — 找不到
http://172.20.7.168:8083/amOnline/app/psinfo/static/am/template/psinfo/monitorItem_inmp.html	响应状态“404” — 找不到
http://172.20.7.168:8083/amOnline/app/psinfo/static/am/template/childrenAccount/contacts_info.html	响应状态“404” — 找不到
http://172.20.7.168:8083/amOnline/app/account/static/am/template/childrenAccount/user_edit.html	响应状态“404” — 找不到
http://172.20.7.168:8083/amOnline/app/monitorspot/static/am/template/onsite/mpstop_merge.html	响应状态“404” — 找不到
http://172.20.7.168:8083/amOnline/app/monitorspot/static/am/template/abnormity/abnormal_filelist.html	响应状态“404” — 找不到
http://172.20.7.168:8083/amOnline/app/monitorspot/static/am/template/onsite/onsit_merge_sc.html	响应状态“404” — 找不到
http://172.20.7.168:8083/amOnline/app/monitorspot/static/am/template/onsite/onsit_merge.html	响应状态“404” — 找不到
http://172.20.7.168:8083/amOnline/app/revisedmanage/static/am/template/revisedmanage/dataRound-rounding.html	响应状态“404” — 找不到

已过滤的 URL 112

TOC

URL	原因
http://172.20.7.168:8083/amOnline/static/images/favicon.ico	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/themes/default/ui.css	一般正则表达式
http://172.20.7.168:8083/amOnline/static/themes/default/login.css	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/themes/icon.css	一般正则表达式
http://172.20.7.168:8083/amOnline/static/themes/default/app.css	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/jquery2.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/jquery2.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/jquery-migrate-1.2.1.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/jquery-migrate-1.2.1.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/jquery.ui.js	一般正则表达式

http://172.20.7.168:8083/amOnline/static/script/jquery.ui.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/locale/ui-lang-zh_CN.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/locale/ui-lang-zh_CN.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/core.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/core.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/common.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/common.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/AppLogin.js?v=20171023	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/AppLogin.js?v=20171023	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/vendor/zxkf/kefu.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/vendor/zxkf/kefu.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/vendor/zxkf/zxkf.css	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/jquery.qrcode.min.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/jquery.qrcode.min.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/qr.code.login.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/script/qr.code.login.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/themes/default/images/l_m_title_info.png	一般正则表达式
http://172.20.7.168:8083/amOnline/static/8.jpg	一般正则表达式
http://qymonitor.envsc.cn/amHelp/main.html	未测试的 Web Server
http://172.20.7.168:8083/amOnline/static/images/login_type_sm.png	一般正则表达式
http://172.20.7.168:8083/amOnline/static/images/login_type_yh.png	一般正则表达式
http://172.20.7.168:8083/amOnline/static/images/login_type_yzm.png	一般正则表达式
http://172.20.7.168:8083/amOnline/app/j_spring_security_check	类似 DOM
http://172.20.7.168:8083/amOnline/app/AppLogin.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/AppLogin.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/j_spring_security_check	类似 DOM
http://172.20.7.168:8083/amOnline/app/j_spring_security_check	类似 DOM
http://172.20.7.168:8083/amOnline/app/AppLogin.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/AppLogin.page?loginError=auth_failed	类似 DOM

http://172.20.7.168:8083/amOnline/app/j_spring_security_check	类似 DOM
http://172.20.7.168:8083/amOnline/app/AppLogin.page?loginError=auth_failed	类似 DOM
http://172.20.7.168:8083/amOnline/static/am/themes/default/main.css	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/themes/default/psview.css	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/script/all.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/script/all.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/script/jf-view.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/script/jf-view.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/vendor/help/css/jquery.pagewalkthrough.css	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/vendor/help/script/jquery.pagewalkthrough.min.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/vendor/help/script/jquery.pagewalkthrough.min.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/themes/vocs/images/link_info.png	一般正则表达式
http://172.20.7.168:8083/amOnline/static/themes/vocs/images/link_info_hover.png	一般正则表达式
http://172.20.7.168:8083/amOnline/static/layui/css/layui.css	一般正则表达式
http://172.20.7.168:8083/amOnline/static/layui/images/ooopic_1509436490.png	一般正则表达式
http://172.20.7.168:8083/amOnline/static/layui/layui.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/layui/layui.js	一般正则表达式
http://m.envsc.cn/WXIndexPSForQYD.aspx?key=wPLFgACAKGA&pscode=140000000223&userid=032CFE6B-3293-47DA-957A-2F0C21A2AA63')	未测试的 Web Server
http://172.20.7.168:8083/amOnline/app/j_spring_security_check	类似 DOM
http://172.20.7.168:8083/amOnline/static/am/script/jf-autocomplete.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/script/jf-autocomplete.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/vendor/my97datepicker/WdatePicker.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/vendor/my97datepicker/WdatePicker.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/vendor/uploadfy/swfobject.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/vendor/uploadfy/swfobject.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/vendor/uploadfy/jquery.uploadify.v2.1.0.min.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/vendor/uploadfy/jquery.uploadify.v2.1.0.min.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/vendor/echarts/dist/echarts.js	一般正则表达

	式
http://172.20.7.168:8083/amOnline/static/am/vendor/echarts/dist/echarts.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/vendor/lodop/LodopFuncs.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/vendor/lodop/LodopFuncs.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/script/historyData.js?version=20181219	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/script/historyData.js?version=20181219	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/vendor/echarts/dist/echarts-all.js	一般正则表达式
http://172.20.7.168:8083/amOnline/static/am/vendor/echarts/dist/echarts-all.js	一般正则表达式
http://172.20.7.168:8083/amOnline/app/AppLogin.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/AppLogin.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/j_spring_security_check	类似 DOM
http://172.20.7.168:8083/amOnline/app/j_spring_security_check	类似 DOM
http://172.20.7.168:8083/amOnline/app/AppLogin.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/AppMain.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/account/accountAction!list.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/AppMain.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!listPsInfo.page?psid=&_=1561344969637	类似 DOM
http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!getPollutantsWithPsID.page?psID=510101055565	类似 DOM
http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!findAcceptInfos.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!findStopInfos.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!list.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/account/accountAction!list.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/psinfoadmin/psInfo!view.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/revisedmanageadmin/revisedAction!list.page	类似 DOM
http://172.20.7.168:8083/amOnline/static/themes/exception.css	一般正则表达式
http://172.20.7.168:8083/amOnline/app/AppMain.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!view.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!listPsInfo.page?psid=&_=1561348844955	类似 DOM
http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!history.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!getPollutantsWithPsID.page?psID=5	类似 DOM

10101055565	
http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!list.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!findAcceptInfos.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!list.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/monitorspot/stopAction!findStopInfos.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!list.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!abnormity.page	类似 DOM
http://172.20.7.168:8083/amOnline/app/account/accountAction!list.page	类似 DOM

注释 39

TOC

URL	注释
http://172.20.7.168:8083/amonline/app/applogin.page	在线客服
http://172.20.7.168:8083/amonline/app/applogin.page	扫码登陆
http://172.20.7.168:8083/amonline/app/applogin.page	在线客服Begin
http://172.20.7.168:8083/amonline/app/appmain.page	头部区域（可配合layui已有的水平导航）
http://172.20.7.168:8083/amonline/app/appmain.page	<dd>信息填报</dd>
http://172.20.7.168:8083/amonline/app/appmain.page	<li class="layui-nav-item" >数据标记 <li class="layui-nav-item" >信息督办
http://172.20.7.168:8083/amonline/app/appmain.page	注意：如果你直接复制所有代码到本地，上述js路径需要改成你本地的
http://172.20.7.168:8083/amonline/app/psinfo/psinfo!view.page	[if lt IE 9]> <script src="../../static/am/vendor/help/script/html5.js"></script> <![endif]
http://172.20.7.168:8083/amonline/app/psinfo/psinfo!view.page	右侧- - begin
http://172.20.7.168:8083/amonline/app/psinfo/psinfo!view.page	右侧- - end
http://172.20.7.168:8083/amonline/app/account/accountaction!list.page	查询条件栏-多行- - begin
http://172.20.7.168:8083/amonline/app/account/accountaction!list.page	<td>行政区划：<input class="textBox w220" value="" id="search_regionCode" data-tag="region" name="search_regionCode" /></td>
http://172.20.7.168:8083/amonline/app/account/accountaction!list.page	查询条件栏-多行- - end

http://172.20.7.168:8083/amonline/app/account/accountaction!list.page	表格工具栏- - begin
http://172.20.7.168:8083/amonline/app/account/accountaction!list.page	表格工具栏- - end
http://172.20.7.168:8083/amonline/app/account/accountaction!list.page	表格- - begin
http://172.20.7.168:8083/amonline/app/account/accountaction!list.page	表格- - end
http://172.20.7.168:8083/amonline/app/account/accountaction!list.page	对话框- - begin
http://172.20.7.168:8083/amonline/app/account/accountaction!list.page	对话框-end
http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!history.page	[if lt IE 9]> <script src="../../static/am/vendor/help/script/html5.js"></script> <![endif]
http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!history.page	nav- - begin
http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!history.page	1小时数据，2日数据，3分钟数据，4实时数据
http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!history.page	实 时 日
http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!history.page	报修
http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!history.page	nav- - end
http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!history.page	浮动提示框-begin
http://172.20.7.168:8083/amonline/app/loginfo/loginfoaction!list.page	表格工具栏-加查询-begin
http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!list.page	顶部工具栏- - end
http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!list.page	查询条件- - begin
http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!list.page	查询条件- - end
http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!list.page	context- - begin
http://172.20.7.168:8083/am	context- - end

online/app/monitorspot/spotaction!list.page	
http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!list.page	tip-提示-begin
http://172.20.7.168:8083/amonline/app/revisedmanage/revisedaction!list.page	左侧简单查询- - end
http://172.20.7.168:8083/amonline/app/revisedmanage/revisedaction!list.page	查询条件栏-begin
http://172.20.7.168:8083/amonline/app/revisedmanage/revisedaction!list.page	查询条件栏-end
http://172.20.7.168:8083/amonline/app/abnormity/abnormityaction!abnormity.page	查询条件栏- - begin
http://172.20.7.168:8083/amonline/app/abnormity/abnormityaction!abnormity.page	查询条件栏- - end
http://172.20.7.168:8083/amonline/app/abnormity/abnormityaction!list.page	顶部工具栏- - begin

JavaScript 43

TOC

URL / 代码

http://172.20.7.168:8083/amonline/app/applogin.page

```
var context = '/amOnline';
var authorizeType = '1';
var enableCaptcha = 'false';
var loginTicket = '2c9487286b79d3e4016b8766909512e0';
```

http://172.20.7.168:8083/amonline/app/applogin.page

```
$('.aLoginSm').click(function(){
 $("#content2").show();
 $("#content3").hide();
 $("#content4").hide();
 $("#content5").hide();
});
$('.aLoginYh').click(function(){
 $("#content2").hide();
 $("#content3").show();
 $("#content4").hide();
 $("#content5").hide();
});
$('.aLoginYzm').click(function(){
 $("#content2").hide();
 $("#content3").hide();
 $("#content4").show();
```

```
 $("#content5").hide();
});


$('#mobileLoginsss_cz').click(function(){
 $('#cmUsername').attr('value', '');
 $('#verificationCode').attr('value', '');
 $('#cmUsername').focus();
});


$('#mobileLoginss_cz').click(function(){
 $('#newPwd').attr('value', '');
 $('#comfirmPwd').attr('value', '');
 $('#newPwd').focus();
});
```

http://172.20.7.168:8083/amonline/app/applogin.page

```
void(0);
```

http://172.20.7.168:8083/amonline/app/applogin.page

```
javascript:$('#divFloatToolsView').animate({width: 'show', opacity: 'show'}, 'normal',function(){
$('#divFloatToolsView').show();kf_setCookie('RightFloatShown', 0, '', '/', 'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:none');$('#aFloatTools_Hide').attr('style','display:block');
```

http://172.20.7.168:8083/amonline/app/applogin.page

```
javascript:$('#divFloatToolsView').animate({width: 'hide', opacity: 'hide'}, 'normal',function(){
$('#divFloatToolsView').hide();kf_setCookie('RightFloatShown', 1, '', '/', 'www.shopnc.net');
});$('#aFloatTools_Show').attr('style','display:block');$('#aFloatTools_Hide').attr('style','display:none');
```

http://172.20.7.168:8083/amonline/app/applogin.page

```
submitCheck()
```

http://172.20.7.168:8083/amonline/app/applogin.page

```
var context = '/amOnline';
var authorizeType = '1';
var enableCaptcha = 'false';
var loginTicket = '2c9487286b79d3e4016b8767113e12ec';
```

http://172.20.7.168:8083/amonline/app/applogin.page

```
var context = '/amOnline';
var authorizeType = '1';
var enableCaptcha = 'false';
var loginTicket = '2c9487286b79d3e4016b8767113e12eb';
```

http://172.20.7.168:8083/amonline/app/applogin.page

```
var context = '/amOnline';
var authorizeType = '1';
var enableCaptcha = 'false';
var loginTicket = '2c9487286b79d3e4016b8767117d12ed';
```

http://172.20.7.168:8083/amonline/app/applogin.page

```
var context = '/amOnline';
var authorizeType = '1';
var enableCaptcha = 'false';
var loginTicket = '2c9487286b79d3e4016b8767136112f1';
```

http://172.20.7.168:8083/amonline/app/applogin.page

```
var context = '/amOnline';
var authorizeType = '1';
var enableCaptcha = 'false';
var loginTicket = '2c9487286b79d3e4016b8767136112f0';
```

http://172.20.7.168:8083/amonline/app/appmain.page

```
    layui.use('element', function(){
        var element = layui.element; //导航的hover效果、二级菜单等功能，需要依赖element模块

        //监听导航点击
        element.on('nav(demo)', function(elem){
            layer.msg(elem.text());
        });
    });

    function changeFrameHeight(){
        var ifm= document.getElementById("frame_lgpblpww");
        ifm.height=document.documentElement.clientHeight-64;
    }
    changeFrameHeight()
    //changeFrameHeight();
    window.onresize=function(){
        changeFrameHeight();
    }
    //退出系统
    function logoutSys(ifrSrc){
         window.location.href='/amOnline/app/j_spring_security_logout';
    }
```

```
   function loadIframe(ifrSrc){
    var ifm= document.getElementById("frame_lgpblpww");
    ifm.src='/amOnline/'+ifrSrc;
   }

   var regionCode='510101000';
   if(regionCode!=''&&regionCode.substr(0, 2)=='64'){
       document.getElementById("xcdzhgl").innerHTML = "";
       var html="";
       html+="<dd><a href=\"#\" onclick=\"loadIframe('app/monitorspot/spotAction!list.page')\">设备验收</a>
</dd>";

       html+="<dd><a href=\"#\" onclick=\"loadIframe('app/viewmonitor/monitorDataAction!list.page')\">信息填报
</a></dd> ";
       /*
       html+="<dd><a href=\"#\" onclick=\"loadIframe('app/monitorspot/stopAction!list.page')\">停运管理</a>
</dd> ";
       html+="<dd><a href=\"#\" onclick=\"loadIframe('app/mprepair/mpRepairAction!list.page')\">报修管理</a>
</dd> ";

          html+="<dd><a href=\"#\" onclick=\"loadIframe('app/stove/stoveAction!list.page')\">启停炉填报</a>
</dd> ";

       html+="<dd><a href=\"#\" onclick=\"loadIframe('app/viewmonitor/monitorDataAction!list.page')\">信息填报
</a></dd> "; */

       document.getElementById("xcdzhgl").innerHTML = html;
   }else  if(regionCode!=''&&regionCode.substr(0, 2)=='51'){
       document.getElementById("xcdzhgl").innerHTML = "";
       var html="";
       html+="<dd><a href=\"#\" onclick=\"loadIframe('app/monitorspot/spotAction!list.page')\">设备验收</a>
</dd>";
       html+="<dd><a href=\"#\" onclick=\"loadIframe('app/monitorspot/stopAction!list.page')\">停运管理</a>
</dd> ";
       html+="<dd><a href=\"#\" onclick=\"loadIframe('app/abnormity/abnormityAction!list.page')\">异常数据标记
</a></dd> ";
       /*  html+="<dd><a href=\"#\" onclick=\"loadIframe('app/stove/stoveAction!list.page')\">启停炉填报</a>
</dd> ";

       html+="<dd><a href=\"#\" onclick=\"loadIframe('app/viewmonitor/monitorDataAction!list.page')\">信息填报
</a></dd> "; */
       document.getElementById("xcdzhgl").innerHTML = html;


       if(isIE()){
            document.getElementById("reviseLi").removeNode(true);
    }else{
        document.getElementById("reviseLi").remove();
    }
   }else{
    if(isIE()){
            document.getElementById("reviseLi").removeNode(true);
    }else{
        document.getElementById("reviseLi").remove();
    }

   }
   /*
    判断是否IE浏览器
   */
   function isIE(){
   if(!!window.ActiveXObject || "ActiveXObject" in window){
         return true;
   }else{
             return false;
   }
   }
```

http://172.20.7.168:8083/amonline/app/appmain.page

```
;
```

http://172.20.7.168:8083/amonline/app/appmain.page

```
loadIframe('app/psinfo/psInfo!view.page')
```

http://172.20.7.168:8083/amonline/app/appmain.page

```
loadIframe('app/onlinemon/onlineAction!history.page')
```

http://172.20.7.168:8083/amonline/app/appmain.page

```
loadIframe('app/monitorspot/spotAction!list.page')
```

http://172.20.7.168:8083/amonline/app/appmain.page

```
loadIframe('app/monitorspot/stopAction!list.page')
```

http://172.20.7.168:8083/amonline/app/appmain.page

```
loadIframe('app/revisedmanage/revisedAction!list.page')
```

http://172.20.7.168:8083/amonline/app/appmain.page

```
loadIframe('app/account/accountAction!list.page')
```

http://172.20.7.168:8083/amonline/app/appmain.page

```
loadIframe('app/loginfo/loginfoAction!list.page')
```

http://172.20.7.168:8083/amonline/app/appmain.page

```
logoutSys()
```

http://172.20.7.168:8083/amonline/app/psinfo/psinfo!view.page

```

```

```
 var _viewpsid = '';
 var _delobj={};//       删除对象
 var _mpobj={};
 var _param={};
 var _psType={};
 var customtagid='';
 var userdata={};
 var _mpItemObj={};



 load('');//       加载视图



 //       加载视图
    function load(id) {

        var strurl = 'app/psinfo/psInfo!listPsInfo.page';
        var url = baseUrl(strurl+'?psid='+id);
        Loading();
        JqAjax(url,'get',{},function(data){
         Psinfo = data;
            draw();
            hideLoading();
        });
        _viewpsid=id;
    }
    /*
      操作
      sourceType 污染源，水排口，气排口，水进口，监控点，水监测设备，气监测设备等 用来确定表
      opt,操作类型 如查看，删除，安装设备，移动等..用来确定操作
      id 操作把柄 查询条件
      */
  function opt(sourceType, opt, id) {
      var title = Psinfo.Title; //+''+paras.join(',');
      if (sourceType == 'ps') { //       企业
          if (opt == 'edit') {
                  _psType={};
                  _psType.type=Psinfo.psClassCode;
                  _psType.id=id;
              jf.loadWindow(title, baseUrl('static/am/template/psinfo/psinfo.html?id=' + id), 820,
530);
          } else if (opt == 'addout') {
                  _psType={};
                  _psType.type=Psinfo.psClassCode;
                  _psType.title=title;
              jf.loadWindow(title + '--       选择排口类型',
baseUrl('static/am/template/psinfo/opt/outputType.html?psId=' + id), 470, 300);
          } else if (opt == 'addpte') {
              jf.loadWindow(title + '--       新增治理设施', baseUrl('static/am/template/psinfo/pte.html?psId='
+ id), 820, 530);
          } else if (opt == 'delete') {
                  jf.sendNotice('       提示','前往污染源列表删除',2,2);
              //jf.loadWindow(title+'--       删除确
认',baseUrl('static/am/template/psinfo/opt/psDeleteInfo.html?id='+id),820,530);
          }
      } else if (sourceType == 'output') { //       进水口
          title += '--       增加排口';
          if (opt == 'add') {
                  _psType={};
                  _psType.title=title;
                  _psType.type=Psinfo.psClassCode;
              jf.loadWindow(title + '--       选择排口类型',
baseUrl('static/am/template/psinfo/opt/outputType.html?psId=' + id), 470, 300);
          }
      } else if (sourceType == 'output-water') { //       水排口
          _psType.title=title;
          var output = jsonObjectById(Psinfo, id); //       获取output对象
          if(output==undefined){
                  jf.sendNotice('       提示','正在刷新界面数据，请稍后再试...。',2,2);
          }
          title += '--'+output.Title;
          if (opt == 'edit') {
              jf.loadWindow(title + '--       修改水排口', baseUrl('static/am/template/psinfo/output-
water.html?psId=' + Psinfo.Id + '&id=' + id), 820, 530);
          } else if (opt == 'addmp') {
              jf.loadWindow(title + '--       增加水监控点', baseUrl('static/am/template/psinfo/monitor-
water.html?psId=' + Psinfo.Id + '&outletid=' + id+ '&flowid=' + id), 820, 530);
```

```
          } else if (opt == 'delete') {
              _delobj = {
                  type: 1,//'output-water',
                  id: id
              }
              jf.loadWindow(title + '--       删除确认',
baseUrl('static/am/template/psinfo/opt/deleteInfo.html'),  470, 280);
          }
      } else if (sourceType == 'output-gas') { //       排气口
          _psType.title=title;
          var output = jsonObjectById(Psinfo, id); //       获取output对象
          if(output==undefined){
                  jf.sendNotice('       提示','正在刷新界面数据，请稍后再试...。',2,2);
          }
                 title += '--'+output.Title;
          if (opt == 'edit') {
              jf.loadWindow(title + '--       修改气排口', baseUrl('static/am/template/psinfo/output-gas.html?
psId=' + Psinfo.Id + '&id=' + id), 820, 530);
          } else if (opt == 'addmp') {
              jf.loadWindow(title + '--       增加气监控点', baseUrl('static/am/template/psinfo/monitor-
gas.html?psId=' + Psinfo.Id + '&outletid=' + id + '&flowid=' + id), 820, 530);
          } else if (opt == 'delete') {
              _delobj = {
                  type:2,// 'output-gas',
                  id: id
              }
              jf.loadWindow(title, baseUrl('static/am/template/psinfo/opt/deleteInfo.html'),  470,
280);
          }
      } else if (sourceType == 'output-in') { //       进水口
          _psType.title=title;
          var output = jsonObjectById(Psinfo, id); //       获取output对象
          if(output==undefined){
                  jf.sendNotice('       提示','正在刷新界面数据，请稍后再试...。',2,2);
          }
              title += '--'+output.Title;
          if (opt == 'edit') {
              jf.loadWindow(title + '--       修改进水口', baseUrl('static/am/template/psinfo/output-in.html?
psId=' + Psinfo.Id + '&id=' + id), 820, 530);
          } else if (opt == 'addmp') {
              jf.loadWindow(title + '--       增加进水监控点', baseUrl('static/am/template/psinfo/monitor-
in.html?psId=' + Psinfo.Id + '&outletid=' + id+ '&flowid=' + id), 820, 530);
          } else if (opt == 'delete') {
              _delobj = {
                  type:3,// 'output-in',
                  id: id
              }
              jf.loadWindow(title + '--       删除确认',
baseUrl('static/am/template/psinfo/opt/deleteInfo.html'),  470, 280);
          }
      } else if (sourceType == 'mp') { //       监控点
          var mp,output;
          var obj = jsonObjectById(Psinfo, id); //       获取mp对象
          if(obj==undefined){
                  jf.sendNotice('       提示','正在刷新界面数据，请稍后再试...。',2,2);
          }
                 ...
```

http://172.20.7.168:8083/amonline/app/psinfo/psinfo!view.page

```
this.src='../../static/themes/vocs/images/link_info.png'
```

http://172.20.7.168:8083/amonline/app/psinfo/psinfo!view.page

```
this.src='../../static/themes/vocs/images/link_info_hover.png'
```

http://172.20.7.168:8083/amonline/app/psinfo/psinfo!view.page

```
openPagess();
```

http://172.20.7.168:8083/amonline/app/account/accountaction!list.page

```
var grid,pageSize=20;
var _regiondata;

jf.initPage = function () {

        $('#search_status').jfchoice({
                data:[{"id":"0","text":"       全部"},{"id":"1","text":"启用"},{"id":"-1","text":"未启用"}],
                text: 'text',
                height: 140,
                defaultIndex: 0,
                value: 'id'
        });

    /*
             获取设置当前登录用户行政区划

    var url = baseUrl('app/standard/discharge/commons/autoUser!getLogonUser.page');
        JqAjax(url,'post',null,function(data){
                if(data){
                        $.get(Actions.common.region).done(function(regiondata){
                   var objregion=jsonObjectById(regiondata,data.regionCode);
                   $('#search_regionCode').val(data.regionCode);
                   $('input[name="search_regionCode_name"]').val(objregion.short_name);
                   _regiondata=regiondata;
                               serchListInfo(1);

                       });
                       }
        });*/
        serchListInfo(1);

        $(window).resize(function(){
           $("#enterpriseList").datagrid("resize");
       });
};

function serchListInfo(pageNo){
        var psn="";
        if($('#search_name').val()=='       用户账号'){
                psn="";
        }else{
                psn=$('#search_name').val()
               }
        var paramQuery = {
                search_pageNo:pageNo,
                search_pageSize:pageSize,
                search_name :psn,
                search_status : $('input[name="search_status"]').val(),
                search_regionCode : $("input[name='search_regionCode']").val()
        }       ;

        grid=$('#enterpriseList').datagrid({
           method: 'post',
           width: '100%',
           url: baseUrl('app/account/accountAction!jsonList.page'),
           pageSize:pageSize,
           pageNumber:pageNo,
           columns:[[
                   {field:'username',title:'       账号',width:300},
                   {field:'true_name',title:'       真实姓名',width:200},
                   {field:'userType',title:'       用户职责',width:200},
                   {field:'create_date',title:'       创建日期',width:200,formatter:dateFormat},
                   {field:'status',title:'       状态',width:200,formatter:formatUserStatus},
                   {field:'describ',title:'       备注',width:200},
                   /*{field:'trueName',title:'       真实姓名',width:100},
```

```
                    {field:'password',title:'       用户密码',width:150},
                    {field:'eMail',title:'       用户邮箱',width:150},
                    {field:'idCard',title:'       身份证号',width:150},
                    {field:'require_sms_check',title:'       执法证号',width:100},
                    {field:'sms_check_code',title:'       执法部门',width:150},
                    {field:'sms_valid',title:'       手机号码',width:100}, */
                    {field:'id',title:'       操作',width:200,formatter:formatOpt}
                ]],
            queryParams:paramQuery,
            singleSelect: true,
            nowrap: true,
            pagination:true,
            selectOnCheck:false,
            checkOnSelect:false,
            scrollbarSize: 0,
            fit:true
        });
        }

 //       表格操作列
  function formatOpt(val, row, index){
         var str='<div class="opt_psl">';
         str+='<a onclick="updUserInfo(\'{0}\')" title="       编辑"><span class="icon icon-edit"></span>
</a>'.format(index);
         /*str+='<a onclick="delUserInfo(\'{0}\')" title="       删除"><span class="icon icon-delete ml12">
</span></a>'.format(row.id);*/
         if(row.status=='-1'){
                 str+='<a onclick="approvalUserInfo(\'{0}\')" title="       启用该用户"><span class="icon icon-
relate ml12"></span></a>'.format(row.id);
         }else if(row.status=='1'){
                 str+='<a onclick="blockUserInfo(\'{0}\')" title="       停用该用户"><span class="icon icon-
relate-dis ml12"></span></a>'.format(row.id);
                 }
         str+='</div>';
         return str;
  }


 //       新增页面
 $(".bt_new").on("click",function(){
         var url = baseUrl('static/am/template/childrenAccount/user_edit.html');
         jf.loadWindow('       新增用户信息',url,500,450);
 })

 //       编辑页面
 var _row=null;
 function updUserInfo(index){
         _row=$("#enterpriseList").datagrid("getRows")[index];
       var url = baseUrl('static/am/template/childrenAccount/user_edit.html?id='+_row.id);
       jf.loadWindow('修改用户信息',url,500,450);
        }

 /*function delUserInfo(id){
         var _id;
            jf.confirm('提示','确认删除该条用户信息! ',function(){
              _id = id;
                   var url = baseUrl('app/standard/discharge/commons/userPerson!delUserInfo.page');
                   JqAjax(url,'post',{search_userID:_id},function(data){
                           if(data.result == 'success'){
                     $('#enterpriseList').datagrid('reload');
                     jf.sendNotice('       提示','操作成功',1,2)
                  }else{
                     jf.sendNotice('       提示',data.msg,0,2);
                  }
                    });
            });
 }*/

 //       启用
    function approvalUserInfo(id){
           var _id;
           jf.confirm('       提示','确认启用该用户',function(){
                   _id = id;
                   var url = baseUrl('app/account/accountAction!start.page');
                   JqAjax(url,'post',{id:_id},function(data){
                           if(data.result == 'success'){
                      $('#enterpriseList').datagrid('reload');
                      jf.sendNotice('       提示','启用用户成功',1,2)
                    }else{
```

```
                    jf.sendNotice('       提示',data.msg,0,2);
                }
                 });
          });
   }
//       停用
   function...
```

http://172.20.7.168:8083/amonline/app/account/accountaction!list.page

```
serchListInfo(1);
```

http://172.20.7.168:8083/amonline/app/onlinemon/onlineaction!history.page

```
 var _psid,_regionCode,_historydata={},ValueOrRevised='Revised',timenumber=0,pl_selected=
{},standard_flag=true;
 var _myChart,_selected,_pagesize=24,_isLocal=-1,_historyDataGrid;

 var option=new Object();
 var option2=new Object();

 var _PsPollutants,_MpPollutants;
 $(function(){
        _psid='510101055565'
        _regionCode='510101000'
        /       /初始化日期控件
        initJfDate();

        var url=baseUrl('app/onlinemon/onlineAction!getPollutantsWithPsID.page?psID='+_psid);
        JqAjax(url,'post',null,function(data){
                _PsPollutants=data;
                /       /加载监控点
                loadmp();
        });

        $(window).resize(function(){
                $("#historydataList").datagrid("resize");
        });
 });


 function loadmp(){
        cleardata();
        /       /加载监控点
        $('#mpcontrol').val('').jfchoice({
                empty:true,
                url:Actions.histroy.getmp+'?psid='+_psid,
                text:'name',
               value:'id',
               defaultIndex:0,
               onCheck:function(item,data,index){
                       _mpselect={item:item,data:data,index:index};
                       for(var i=0;i<_PsPollutants.length;i++){
                               if(data[index].id==_PsPollutants[i].mpID){
                                       _MpPollutants=_PsPollutants[i].pollCode;
                               }
                       }

                       ValueOrRevised='Revised';
                       $('#bar_xiu').addClass('on');
                        $('#bar_yuan').removeClass('on');
                        $('#bar_stop').removeClass('on');
                        $('#bar_repair').removeClass('on');
                        $('#bar_yi').removeClass('on');
                        delChartbg('all');
                        delChartIcon('all');
                        delChartYiLine();
                        removeStandard();
```

```
                        load_Data();
                }
        });
}
```

http://172.20.7.168:8083/amonline/app/loginfo/loginfoaction!list.page

```
//       查询参数/
var param,pageSize=20,grid,_psid;

jf.initPage=function(){
        _psid='510101055565'
        /       /加载模块下拉数据
         $('#search_moduleName').combobox({
             data: Actions.loginfo.loginfoModule.data,
             method: 'post',
             height:32,
             width:185,
             valueField: 'id',
             textField: 'text'
         });
        /       /初始化datagrid
        $('#loginfoTable').datagrid({
                method: 'post',
                url:'loginfoAction!jsonList.page?psID='+_psid,
            rownumbers:true,
                width: '100%',
                singleSelect: true,
                nowrap: true,
                selectOnCheck:false,
                checkOnSelect:false,
                scrollbarSize: 0,
                pageSize:pageSize,
                pagination: true,
                fit:true,
                onLoadSuccess:function(data){
                        if(data.total==0){
                                jf.sendNotice('       提示','当前暂无记录！',2,2)
                                return;
                        }
                       }
        });
       var edate1=  new Date();
       var sdate1 = new Date(edate1.getTime()-(7*24*60*60*1000));
       $('#search_startEndTimeParm').jfDoubleDate({
           sdate:sdate1,
           edate:edate1,
           range:1,
                rangeType:'Month'
       });
        var begindate = sdate1.format('yyyy-MM-dd');
        var enddate = edate1.format('yyyy-MM-dd');
       $('#search_startEndTimeParm').val(begindate+'至'+enddate);
        $(window).resize(function(){
                $("#loginfoTable").datagrid("resize");
        });
       }



/*
         查询
 */
function serchListInfo(pageNo){
    $('#loginfoTable').datagrid('clearSelections');
        var queryParams = $('#loginfoTable').datagrid('options').queryParams;
        var search_moduleId =$("input[name='search_moduleName']").val();
        var search_startEndTime =$("#search_startEndTimeParm").val();
        queryParams.psID = _psid;
        queryParams.search_moduleId = search_moduleId;
        queryParams.search_startEndTime = search_startEndTime;
```

```
        queryParams.pageNo = 1;
        $('#loginfoTable').datagrid('options').queryParams = queryParams;
        $('#loginfoTable').datagrid('options').pageNumber=pageNo;
        var pager = $('#loginfoTable').datagrid('getPager');
        pager.pagination('refresh',{ pageNumber:pageNo  });
        $("#loginfoTable").datagrid('reload');
       }

//       表格操作列
function formatModuleName(val, row, index) {
        if(val==11){
                return val = "       现场端验收信息维护";
        }else if(val==14){
                return val = "       现场端停运管理";
        }else if(val==15){
                return val = "       现场端报修管理";
        }else if(val==16){
                return val = "       异常数据标记";
        }else if(val==24){
                return val = "       启停炉";
        }else{
                return val = "       基本信息维护";
               }
       }

//       内容显示
function formatRecord(val, row, index){
        return '<span title="{0}">{0}</span>'.format(val);
       }
```

http://172.20.7.168:8083/amonline/app/loginfo/loginfoaction!list.page

```
serchListInfo(1)
```

http://172.20.7.168:8083/amonline/app/monitorspot/stopaction!list.page

```
   var beginTime="",endTime="",methodName="" ;
//        查询参数/
   var param,pageSize=20,searchFlag=0;

jf.initPage=function(){

        var sdate1 = new Date();
        var edate1=  new Date();
        sdate1.addDays(-60);
        $('#search_startEndTimeParm').jfDoubleDate({
                sdate:sdate1,
                edate:edate1
        });
        formatTime();

        $('#mpStopInfoList').datagrid({
                method: 'post',
                url: baseUrl('app/monitorspot/stopAction!findStopInfos.page'),
                queryParams:{
                        search_startTime:beginTime,
                        search_endTime:endTime
               },
               rownumbers:true,
                pageSize:pageSize,
                width: '100%',
                singleSelect: true,
                nowrap: true,
                pagination: true,
                selectOnCheck:false,
                checkOnSelect:false,
                scrollbarSize: 0,
```

```
                fit:true,
                onLoadSuccess:function(data){
                        if(data.total==0){
                                jf.sendNotice('       提示','无符合当前查询条件的停运记录！',2,2)
                                return;
                        }
                       }
         });

         $(window).resize(function(){
                $("#mpStopInfoList").datagrid("resize");
         });
        }

 //       污染源
 function formatListName(val, row, index) {
         return '<span  class="cut-normal maxW280" title="{0}">{0}</span>'.format(val);
        }

 //       表格操作列
 function formatOpt(val, row, index) {
         var delMsgStr="       是否删除 【{0}-{1}  {2}至{3}】 停运记
录".format(row.psName,row.mpName,row.stopDate,row.endDate);
         if(row.sfsz=='1'){
                if(row.isDelete=='1'){
                        return '<div class="opt_psl">' +
                        '<a href="javascript:;"  ><span class="icon icon-edit"
onclick="editMpStopInfo(\'{0}\',\'{1}\',\'{2}\',\'{3}\',\'{4}\',\'{5}\')"></span>
</a>'.format(row.id,row.psName,row.mpName,row.isGd,row.proofId) +
                        '<a href="javascript:;"  ><span class="icon icon-delete ml12"
onclick="delStopInfoByID(\'{0}\',\'{1}\',\'{2}\')"></span></a>'.format(row.id,delMsgStr,row.proofId) +
                        '</div>';
                }else{
                        return '<div class="opt_psl">' +
                        '<a href="javascript:;"  ><span class="icon icon-edit"
onclick="editMpStopInfo(\'{0}\',\'{1}\',\'{2}\',\'{3}\',\'{4}\',\'{5}\')"></span></a>'.format(row.id,
row.psName,row.mpName,row.isGd,row.proofId ) +
                        '<a href="javascript:;"  ><span class="icon icon-edit-gray ml12"   title="
{0}"></span></a>'.format("当前记录已经存档，无法删除") +
                        '</div>';
                       }
         }else{
                        return '<div class="opt_psl">' +
                        '<a href="javascript:;"  ><span class="icon icon-edit-gray11 ml12"  title="
{0}"></span></a>'.format("当前记录已经存档，无法编辑" ) +
                        '<a href="javascript:;"  ><span class="icon icon-edit-gray ml12"   title="
{0}"></span></a>'.format("当前记录已经存档，无法删除") +
                        '</div>';
                }
        }
    /*
     删除停运记录
    */
 function delStopInfoByID(id,delMsg,attachId){
         jf.confirm('       提示',delMsg,function(){
                var url=baseUrl('app/monitorspot/stopAction!delete.page?
id='+id+'&search_proofId='+attachId);
                JqAjax(url,'post',null,function(data){
                        if(data.result == 'success'){
                                $("#mpStopInfoList").datagrid('reload');
                                jf.sendNotice('       提示','停运记录删除成功.',1,2)
                        }else{
                                jf.sendNotice('       提示','删除失败，抱歉给您的工作带来不便，请尝试重新操作！',0,2)
                               }
                })       ;
               });
        }
 //       表格操作列-监控点
 function formatMonitorPoint(val, row, index) {
         var mpType=row.mpType;
         if(mpType=='4'||mpType=='6'){
                return '<div   class="monitorPoint"><a  style="max-width:150px;" class="monitorPoint-
cut" title="{0}">{0}</a><span class="tips kao inline">水</span></div>'.format(val);
         }else{
                return '<div   class="monitorPoint"><a style="max-width:150px;" class="monitorPoint-
cut" title="{0}">{0}</a><span class="tips que">气</span></div>'.format(val);
               }
        }
```

```
//       表格起止时间
function formatStopTime(val, row, index) {
        return '<span>{0} — {1}</span>'.format(row.stopDate,row.endDate);
       }

//       表格影响时间
function formatOptTime(val, row, index) {
        return '<span>{0} — {1}</span>'.format(row.checkEndDate,row.checkStopDate);
       }



/*
         查询
  @param pageNo
 */
function serchMpStopInfo(pageNo){
        var beginEndTime=$("input[name='search_startEndTimeParm']").val();
        beginTime=beginEndTime.split("       至")[0];
        endTime=beginEndTime.split("       至")[1];
    $('#mpStopInfoList').datagrid('clearSelections');
        var queryParams = $('#mpStopInfoList').datagrid('options').queryParams;
        queryParams.search_startTime =beginTime;
        queryParams.search_endTime =endTime;
        $('#mpStopInfoList').datagrid('options').queryParams = queryParams;
        $('#mpStopInfoList').datagrid('options').pageNumber=pageNo;
        var pager = $('#mpStopInfoList').datagrid('getPager');
        pager.pagination('refresh',{ pageNumber:pageNo  });
        $("#mpStopInfoList").datagrid('reload');
       }


var  mpStopInfoID="",mpStopInfoEpoFlag="",mpStopInfoGdFlag="";
var  _stopPsName='',_stopMpName='',_proofId='';
/*
         添加监控点停运信息
 */
function addMpStopInfo(){
        mpStopInfoID="", mpStopInfoGdFlag='';
        methodName='save';
        var url=baseUrl('static/am/template/onsite/mpstop_merge.html');
        jf.loadWindow("       新增停运记录",url,860,530);
       }

/*
        编辑监控点停运记录信息
*/
function editMpStopInfo(ID, stopPsName,stopMpName,gdFlag,proofId){
        mpStopInfoID=ID, mpStopInfoGdFlag=gdFlag;
        _stopPsName=stopPsName,_stopMpName=stopMpName,_proofId=proofId ;
        methodName='edit' ;
        var url=baseUrl('static/am/template/onsite/mpstop_merge.html');
        jf.loadWindow("       编辑停...
```

http://172.20.7.168:8083/amonline/app/monitorspot/stopaction!list.page

```
serchMpStopInfo(1)
```

http://172.20.7.168:8083/amonline/app/monitorspot/stopaction!list.page

```
addMpStopInfo()
```

http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!list.page

```
var _proofId,regionCodeProof;
var isUpdate;
   var _selFlagMerge=0,_selEquipIDMerge;
var acceptDatas,selIndex,acceptID,param,childListDatas,_updSaveFlag,_regoname;
var total=0,pageSize=20,searchFlag=0;
var regintemp="",reginName="";
var _customtagid="";
jf.initPage = function () {
        $('#acceptStatus').trigger('setVal',['-99']);
        /       /查询
        serchEquipAccptInfo(1);

        regionCodeProof='510101000'
};

var trAccpetTime,trAccpetStatus;
/*
         添加验收记录
 */
function addEquiptAccept(){
        isUpdate=0;
        acceptID='',_updSaveFlag=1;
        if(regionCodeProof.substring(0,2)=='51'){
                var url=baseUrl('static/am/template/onsite/onsit_merge_sc.html')
                jf.loadWindow("       新增验收信息",url,795,468);
        }else{
                var url=baseUrl('static/am/template/onsite/onsit_merge.html')
                jf.loadWindow("       新增验收信息",url,795,368);
               }
       }
/*
         维护验收记录
  @param id
    */
function updEquiptAccept(id,updFlag,regoname){
        isUpdate=1;
        _updSaveFlag=updFlag;
        acceptID=id;
        _regoname=regoname

        if(regionCodeProof.substring(0,2)=='51'){
                var url=baseUrl('static/am/template/onsite/onsit_merge_sc.html')
                jf.loadWindow("       验收信息维护",url,795,468);
        }else{
                var url=baseUrl('static/am/template/onsite/onsit_merge.html')
                jf.loadWindow("       验收信息维护",url,795,368);
        }
       }

var childInfoFlag=true;
/*
         通过验收设备获取下面的验收记录
  @param index
    */
function initChildData(index){
        if(selIndex==index&&childInfoFlag){  //       第二次点击影藏验收记录
                $("#childInfo").remove();
                var nTr=$("#"+acceptDatas[index].equipId);
                nTr.removeClass("on");
                childInfoFlag=false;
                return;
               }
        childInfoFlag=true;
        selIndex=index;
        trAccpetTime='';
        var tr=$("#"+acceptDatas[selIndex].equipId);
        $("#onsiteCheckInfoUl tr").removeClass("on");
        tr.addClass("on");
        var str='<tr id="childInfo" class=\"on-content \"><td colspan=\"4\" class=\"b-left b-right\">
<div class=\"detail\">';
        /       /新增按钮本级非本级判断
        if(acceptDatas[selIndex].epoFlag=='1'){
                str+='<p><input type=\"button\" class=\"bt_new\" id=\"add\" value=\"       新 增\"
onclick="addEquiptAccept()"/></p>';
        }else{
                str+='<p><input type=\"button\" title="{0}"  class=\"bt_new_gray\" id=\"add\"
value=\"新 增\" /></p>'.format("该企业信息管理权限属于"+acceptDatas[selIndex].epoName+", 请联
系"+acceptDatas[selIndex].epoName+"进行维护! ");
```

```
                }
        str+='<table class=\"table\" id="childTab" cellpadding=\"0\" cellspacing=\"0\">';
        var url = baseUrl('app/monitorspot/spotAction!findAcceptRecord.page?
search_equipId='+acceptDatas[selIndex].equipId+'&search_psId='+acceptDatas[selIndex].psId+'&search_mpId='+acc
eptDatas[selIndex].mpId);
        JqAjax(url,'post',null,function(data){
                $("#childTab").empty();
                childListDatas=data.rows;
                var listInfo=data.rows;
                for(var i=0;i<listInfo.length;i++){
                        if(i==0){
                                if(listInfo.length>1){
                                        trAccpetTime=listInfo[i].acceptTime;
                                       }

                                $("#accpetTime"+acceptDatas[selIndex].equipId).empty();

$("#accpetTime"+acceptDatas[selIndex].equipId).append(listInfo[i].acceptTime);

                                if('1'==listInfo[i].acceptStatus){
                                        $("#accpetStatus"+acceptDatas[selIndex].equipId).empty();

$("#accpetStatus"+acceptDatas[selIndex].equipId).attr('class','');
                                        $("#accpetStatus"+acceptDatas[selIndex].equipId).append('       通
过');
                                }else if('0'==listInfo[i].acceptStatus){
                                        $("#accpetStatus"+acceptDatas[selIndex].equipId).empty();

$("#accpetStatus"+acceptDatas[selIndex].equipId).attr('class','red');
                                        $("#accpetStatus"+acceptDatas[selIndex].equipId).append('       未通
过');
                                }else{
                                        $("#accpetStatus"+acceptDatas[selIndex].equipId).empty();

$("#accpetStatus"+acceptDatas[selIndex].equipId).attr('class','blue');
                                        $("#accpetStatus"+acceptDatas[selIndex].equipId).append('       未验
收');
                                       }
                                }

                        var updFlag=0;
                        if(i==0)
                                updFlag=1;
                        els       e
                                updFlag=0;

                        var chStr='<tr
onclick="updEquiptAccept(\'{0}\',\'{1}\',\'{2}\')">'.format(listInfo[i].id,updFlag,acceptDatas[selIndex].epoN
ame);
                        chStr+='<td>{0}'.format(listInfo[i].acceptTime);
                        var accStatus=listInfo[i].acceptStatus;
                        if(accStatus=='1'){
                                chStr+='<td><span class="gray">       验收：</span><span>通过</span></td>';
                        }else{
                                chStr+='<td><span class="gray">       验收：</span><span class="red">未通过
</span></td>';
                               }

                        chStr+='<td><span class="gray">       验收人：</span><span>{0}</span>
</td>'.format(listInfo[i].acceptUser);
                        chStr+='<td><span class="remarkInfo" title="{0}">       备注</span>
</td>'.format(ToHtmlString(listInfo[i].comment));
                        chStr+='</tr>';
                        $("#childTab").append(chStr);
                       }
        });
        str+='</table></div></td></tr>';
        $("#childInfo").remove();
        $(str).insertAfter(tr);
       }
 /*
          获取设备信息
  */
 function getMpStopJsonList(){
        var url = baseUrl('app/monitorspot/spotAction!findAcceptInfos.page');
        JqAjax(url,'post',param,function(data){
                $("#onsiteCheckInfoUl").empty();
                var listInfo=data.rows;
                total=data.total;
```

```
                acceptDatas=data.rows;
                if(total==0){
                        jf.sendNotice('       提示','无符合当前查询条件的设备信息！',2,2)
                }
                if(total>0){
                        for(var i=0;i<(listInfo.length>pageSize?pageSize:listInfo.length);i++){
                                va..       .
```

http://172.20.7.168:8083/amonline/app/monitorspot/spotaction!list.page

```
serchEquipAccptInfo(1)
```

http://172.20.7.168:8083/amonline/app/revisedmanage/revisedaction!list.page

```
 var _psId='',_regionCode='';
 var _items='';
 var _mpId='';
 var _beginTime='';
 var _endTime='';
 var _isLocal=1;
 var _monitorType='';
 var _dataRoundDataGrid;
 var clotting_flag=false;
 $(function(){
         _psId='510101055565'
         _regionCode='510101000'

         /       /引用左侧列表
         $('#leftpage').load(baseUrl('static/am/template/psinfo/opt/leftps.html?
monitorType='+GetUrlParam('monitorType')),function(){
         });
         /       /初始化时间控件
         InitDateTime();
         /       /加载数据来源
         loaddatasource();
         /       /加载数据状态
         loaddatastatus();
         /       /加载监控点
         if(_psId!=null || _psId!=''){
                 loadMP(_psId,false);
         }
 });

 //       初始化时间控件
 function InitDateTime(){
         /       /日历
         if(_endTime==null || _endTime=='' || _beginTime==null || _beginTime==''){
                 var sdate1 = new Date();
                 var edate1=  new Date();
                 $('#dateDouble').jfDoubleDate({
                         sdate:sdate1,
                         edate:edate1
                 })       ;
                 formatTime();
         }else{
                 var sdate1 = new Date(_beginTime);
                 var edate1=  new Date(_endTime);
                 $('#dateDouble').jfDoubleDate({
                         sdate:sdate1,
                         edate:edate1
                 })       ;
                 $("input[name='dateDouble']").val(_beginTime+"       至"+_endTime);
         }
        }

 /*
          初始化双日期控件值
   */
```

```
function formatTime(){
        var begin=new Date();
        _beginTime= begin.format("yyyy-MM-dd");
        _endTime=begin.format("yyyy-MM-dd");
        $("input[name='dateDouble']").val(_beginTime+"       至"+_endTime);
       }

/*
         日期类型格式化
  @param format         日期类型格式化类型格式 （yyyy-MM-dd）
  @returns {}
 */
Date.prototype.format = function(format) {
        var o = {
                "M+" : this.getMonth() + 1, // month
                "d+" : this.getDate(),      // day
                "h+" : this.getHours(),     // hour
                "m+" : this.getMinutes(),   // minute
                "s+" : this.getSeconds(),   // second
                "q+" : Math.floor((this.getMonth() + 3) / 3), // quarter
                "S" : this.getMilliseconds()
               }
        if (/(y+)/.test(format))
                format = format.replace(RegExp.$1, (this.getFullYear() + "")
                                .substr(4 - RegExp.$1.length));
        for ( var k in o)
                if (new RegExp("(" + k + ")").test(format))
                        format = format.replace(RegExp.$1, RegExp.$1.length == 1 ? o[k]
                                        : ("00" + o[k]).substr(("" + o[k]).length));
        return format;
       }


//       加载监控点
function loadMP(psid,flag){
        ResetControl(flag);
        _psId=psid;
        $("#jf-panel-mpItem").empty();
        $("input[name='mpItem']").val('');
        $('#mpItem').val('');
        $('#mpItem').jfchoice({
                url:baseUrl('app/mpoint/mpAction!getMpByPS_ID.page?psid='+psid),
                text:'name',
                value:'id',
                defaultIndex:0,
                onCheck:function(item,data,index){
                        /       /加载监测项
                        $('#mpType').val(data[index].type);
                        $('#mpId').val(data[index].id);
                        /       /如果是水监控点则将日期提前一天
                        var begin=new Date();
                        if('5'!=data[index].type){
                                $("input[name='dateDouble']").val(begin.addDays(-3).format("yyyy-MM-
dd")+"至"+begin.addDays(2).format("yyyy-MM-dd"));
                        }else{
                                $("input[name='dateDouble']").val(begin.format("yyyy-MM-
dd")+"至"+begin.format("yyyy-MM-dd"));
                               }
                        clotting_flag=data[index].clotting_flag;
                        setTimeout(function(){

loadMonitorItem(psid,data[index].type,data[index].id,data[index].clotting_flag);
                        },500);
                }       ,
                onSuccess:function(data){
                        if(data=='Undefined' || data==null || data.length<1){
                                $('#monitorItem').combobox('setValues', ['']);
                               }
                        if(_mpId){
                                $('#mpItem').trigger('setVal',['{0}'.format(_mpId)]);
                               }
                }       ,
                onLoadError:function(){
                        $('#monitorItem').combobox('setValues', ['']);
                       }
        });
       }

/*
```

```
        重置控件
 */
 function ResetControl(flag){
         $('#dataSourceItem').trigger('setVal',['-1']);
         $('#dataStatusItem').trigger('setVal',['-1']);
         mpType:$('#mpType').val('');
         mpId:$('#mpId').val();
         /       /初始化时间控件
         if(flag){
                 formatTime();
                 InitDateTime();
                }
         $('#monitorItem').combobox({
                 url:null,
                 valueField: 'code',
                 textField: 'name',
                 width: 220,
                 height: 32,
                 editable: false,
                 multiple:true,
                 panelHeight:'auto'
         });
         if(_dataRoundDataGrid){
                 var fields=_dataRoundDataGrid.datagrid('getColumnFields');
                 for(var i=0;i<fields.length;i++){
                         _dataRoundDataGrid.datagrid('hideColumn',fields[i]);
                        }
                 for(var i=0;i<arrayGroup.length;i++){
                         _dataRoundDataGrid.datagrid('hideColumn',arrayGroup[i].field);
                        }
                 _dataRoundDataGrid.datagrid('hideColumn','dataTime');
                 _dataRoundDataGrid.datagrid('loadData', { total: 0, rows: []});
         }

        }

 //       加载监测项目
 function loadMonitorItem(psid,mptype,mpid,clotting_flag){
         $('#monitorItem').combobox({
                 method:'get',
                 url:baseUrl('app/revisedmanage/revisedAction!GetMonitorItem.page?
psId='+psid+'&mpType='+mptype+'&mpId='+mpid),
                 valueField: 'code',
                 textField: 'name',
                 width: 220,
                 height: 32,
                 editable: false,
                 multiple:true,
                 panelHeight:'auto',
                 formatter: function (row) {
                         var opts = $(this).combobox('options');
                         if(row.code1=='B01'||row.code1=='B02'){
                                 return;
                                }
                         return '<input type="checkbox" class="combobox-checkbox">' +
row[opts.textField]
                 }       ,
                 onShowPanel: function () {
                         var opts = $(this).combobox('options');
                         var target = this;
                         var values = $(target).combobox('getValues');
                         $.map(va...
```

http://172.20.7.168:8083/amonline/app/revisedmanage/revisedaction!list.page

```
btnQuery()
```

http://172.20.7.168:8083/amonline/app/applogin.page

```
var context = '/amOnline';
var authorizeType = '1';
var enableCaptcha = 'false';
var loginTicket = '2c9487286b79d3e4016b876723612f4';
```

http://172.20.7.168:8083/amonline/app/abnormity/abnormityaction!abnormity.page

```
//       加载报警数据
var pageNo=1;
var pageSize =20;
var beginTime='';
var endTime='';
var _dataStatus;
var alarmType = 2;
jf.initPage=function(){
        var sdate1 = new Date();
        var edate1=  new Date();
        sdate1.addDays(-7);
        $('#dateS').jfDoubleDate({
                sdate:sdate1,
                edate:edate1,
                emaxdate:new Date()
        });
        setTimes();
        $('#abnormityList').datagrid({
                method: 'post',
                url: baseUrl('app/abnormity/abnormityAction!jsonList.page'),
                queryParams:{
                        search_startTime:beginTime,
                        search_endTime:endTime,
                        search_alarmType:alarmType,
                        search_disposeType:$("input[name='disposeType']").val()
               },
                width: '100%',
                singleSelect: false,
           rownumbers:true,
           pageSize: 15,
           pageNo:1,
                nowrap: true,
                pagination:true,
                selectOnCheck:false,
                checkOnSelect:false,
                scrollbarSize: 0,
                fit:true,
                columns:[[
                          {field:'psName',title:'       污染源',width:200,align:'left',formatter:formatVal},
                          {field:'mpName',title:'       监控点',width:200,formatter:formatMonitorPoint},
                          {field:'pollutantName',title:'       污染物',width:200,formatter:formatVal},
                          {field:'abnormalValue',title:'       异常值',width:100},
                          {field:'standardValue',title:'       标准限值',width:100},
                          {field:'beginTime',title:'       异常时间范围',width:250,formatter:function(val,
row, index){
                                        var start=row.beginTime;
                                        var end=row.endTime;
                                        return start+"~"+end;

                                }},
                          {field:'explain',title:'       异常原因',width:200,formatter:formatExplain},
                          {field:'proofID',title:'       附件',width:200,formatter:formatFile},
                          {field:'comment',title:'       备注',width:200,formatter:formatVal},
                          {field:'dataStatus',title:'       操作',width:100,formatter:formatOpt},
                      ]]
        });
       }

/*
         初始化双日期控件值
  */
function setTimes(){
        var begin=new Date();
        var end=new Date();
        begin.addDays(-7);
```

```
          beginTime= begin.format("yyyy-MM-dd");
          endTime=end.format("yyyy-MM-dd");
          $("input[name='dateS']").val(beginTime+"       至"+endTime);
         }

 //       格式化附件
 function formatFile(val, row, index) {
     if(val != ''&& val != undefined){
         return '<div style="width:72px;margin:auto;"><a class="a-do"
onclick="findViewProof(\'{0}\')">查看附件</a></div>'.format(val);
                }
        }

 //       格式化操作列
 function formatOpt(val, row, index) {
         if(val==1){
                 return '<div class="w72" ><input type="button" class="bt_opt" value="       编辑"
onclick="editManage(\'{0}\')"/></div>'.format(index);
         }else if(val==-1){
             return '<div class="w72" ><input type="button" class="bt_opt" value="       查看"
onclick="lookManage(\'{0}\')"/></div>'.format(index);
                 }
   }

 function formatExplain(val, row, index){
         if(val==1){
                 return '       排放超标';
         }else if(val==2){
                 return '       在线设备故障';
         }else if(val==3){
                 return '       校准校验';
         }else if(val==4){
                 return '       氧量折算';
         }else if(val==5){
                 return '       标准设置错误';
         }else if(val==6){
                 return '       监管部门检查';
         }else if(val==7){
                 return '       其他';
                }
        }

 //       表格操作列-监控点
 function formatMonitorPoint(val, row, index) {
         var mpType=row.mpType;
         if(mpType=='4'||mpType=='6'){
                 return '<div   class="monitorPoint"><a  style="max-width:150px;" class="monitorPoint-
cut" title="{0}">{0}</a><span class="tips kao inline">水</span></div>'.format(val);
         }else if(mpType=='5'){
                 return '<div   class="monitorPoint"><a style="max-width:150px;" class="monitorPoint-
cut" title="{0}">{0}</a><span class="tips que">气</span></div>'.format(val);
                 }
        }

 //       表格起止时间
 function formatrePairTime(val, row, index) {
         return '<span>{0}-{1}</span>'.format(row.beginTime,row.endTime);
        }

 //       表格内容格式化
 function formatVal(val, row, index) {
         if(val!="" && val != undefined){
                 return '<span  class="cut-normal maxW450" title="{0}">{0}</span>'.format(val);
                }
        }

 var _explainId="";
 var _alarmDataId="";
 var _psName="";
 var _mpName="";
 var _updatedBy="";
 var _updatedTime="";
 var _pollutantName ='';
 var _abnormalValue ='';
 var _standardValue ='';
 var _abnormalTimes ='';
 var _explain='';
 var _comment='';
 var _proofId;
```

```
//============       批量编辑==========**********==========
function editSubmit(){

        var datagrid=$("#abnormityList").datagrid('getSelections');
        if(datagrid.length <= 0){
                jf.sendNotice('       警告','请选择需要标记的数据！',2,0);
                return;
               }

        if(containsSummitedData()){
                jf.sendNotice('       警告','已提交过的数据不能再标记！',2,0);
                return;
               }

         //       批量保存
        var datagrid=$("#abnormityList").datagrid('getSelections');
        var idAlarmDataArr=[];
        var idExplainIdArr=[];
        var psNameArr=[];
        var mpNameArr=[];
        var pollutantNameArr=[];
        var abnormalValueArr=[];
        var standardValueArr=[];
        var abnormalTimesArr=[];
        var explainArr=[];
        var commentArr=[];
        var proofIdArr=[];
        var updatedByArr=[];
        var updatedTimeArr=[];
        //var proofIDArr=[];
       if(datagrid.length!=0){
         for (var i=0;i<datagrid.length;i++){
                idAlarmDataArr.push(datagrid[i].alarmDataId);
                idExplainIdArr.push(datagrid[i].explainId);
                psNameArr...
```

http://172.20.7.168:8083/amonline/app/abnormity/abnormityaction!abnormity.page

```
btnQuery(1)
```

http://172.20.7.168:8083/amonline/app/abnormity/abnormityaction!abnormity.page

```
submitSave()
```

http://172.20.7.168:8083/amonline/app/abnormity/abnormityaction!abnormity.page

```
editSubmit()
```

http://172.20.7.168:8083/amonline/app/abnormity/abnormityaction!list.page

```
var anomalyType=2;
jf.initPage=function(){

        tabQuery();

       }
 //       切换报警类型
   function tabQuery(){
```

```
        $('#anomalyTab a').on('click',function(){
            $('#anomalyTab a').removeClass('on');
            $(this).addClass('on');
            $('#anomalyTab a').removeClass('on');
            $(this).addClass('on');
            anomalyType=$(this).children("span").attr("data-anomalyType");
            if(anomalyType==1){
                $('#abnormityIframe').attr('src','abnormityAction!exceed.page');
            }else if(anomalyType==2){
                $('#abnormityIframe').attr('src','abnormityAction!abnormity.page');
            }else if(anomalyType==6){
                $('#abnormityIframe').attr('src','abnormityAction!constant.page');
            }else{
                $('#abnormityIframe').attr('src','abnormityAction!zero.page');
            }

        });
    }
```

cookie 7

TOC

名称 值	首先设置 请求的 URL	域	安全 到期
JSESSIONID			False
2F054296B22CF446C215F74AF599D847	http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!jsonList.page		
JSESSIONID	http://172.20.7.168:8083/amOnline/app/AppLogin.page?loginError=auth_failed	172.20.7.168	False
0308DD52713329209493123C8AAC241F	http://172.20.7.168:8083/amOnline/app/AppLogin.page		
hasshown			False
1	http://172.20.7.168:8083/amOnline/app/onlinemon/onlineAction!getPollutantsWithPsID.page?psID=510101055565		
hasshown			False
1	http://172.20.7.168:8083/amOnline/app/abnormity/abnormityAction!jsonList.page		
hasshown			False
1	http://172.20.7.168:8083/amOnline/app/monitorspot/spotAction!findAcceptInfos.page		
hasshown			False
1	http://172.20.7.168:8083/amOnline/app/psinfo/psInfo!listPsInfo.page?psid=&_=1561344886440		
hasshown			False