

安全评估报告

【生态环境局】

文档版本：V1.0

文档信息

|  |  |  |  |
| --- | --- | --- | --- |
| 基本信息 | | | |
| 报告编号 | Aliyun-yundun-mss-sc-2019061101 | | |
| 客户名称 | 晋城市生态环境局 | | |
| 客户接口人 |  | 客户联系方式 |  |
| 服务专家 | 任逸 | 服务专家联系方式 | 18435105726 |
| 文档编写 | 任逸 | 文档审批 | 秀行 |
| 扩散范围 | 【阿里云】、【晋城市生态环境局】、【晋城市信息中心】 | | |

变更记录

|  |  |  |  |
| --- | --- | --- | --- |
| 文档变更记录 | | | |
| 时间 | 变更内容/操作内容 | 版本号 | 变更人/操作员 |
| 2019-06-11 | 文档创建 | V1.0 | 任逸 |
|  |  |  |  |

特别说明

\*本文档所包含的信息是仅限于【阿里云】、【晋城市生态环境局】、【晋城市信息中心】传播。在未事先得到阿里云计算有限公司书面同意之前，本文档全部或部分内容不得用于其他任何用途或交与第三方。

目录

[文档信息 1](#_Toc28376)

[变更记录 1](#_Toc31424)

[1概述 4](#_Toc17473)

[1.1 检测范围 4](#_Toc7424)

[1.2 检测时间 4](#_Toc15408)

[1.3 检测方法 4](#_Toc18117)

[2整体检测结论 6](#_Toc328)

[2.1 整体安全度 6](#_Toc19179)

[2.2 检测对象安全汇总 6](#_Toc10924)

[2.3 检测对象迁云建议 6](#_Toc7385)

[3测试结果 8](#_Toc31668)

[3.1IIS短文件名泄露漏洞【高风险】 8](#_Toc16872)

[漏洞描述 8](#_Toc32306)

[漏洞地址 8](#_Toc14104)

[漏洞证明 8](#_Toc13255)

[修复意见 10](#_Toc13698)

[3.2 Apache Tomcat版本过低【高风险】 10](#_Toc16169)

[漏洞描述 10](#_Toc21275)

[漏洞地址 10](#_Toc11331)

[漏洞证明 11](#_Toc10946)

[修复意见 11](#_Toc30350)

[3.3 SQL注入漏洞【高风险】 11](#_Toc19902)

[漏洞描述 11](#_Toc10018)

[漏洞地址 11](#_Toc4619)

[漏洞证明 12](#_Toc28740)

[修复意见 13](#_Toc11303)

[3.4 跨站脚本攻击【高风险】 14](#_Toc6790)

[漏洞描述 14](#_Toc14403)

[漏洞地址 14](#_Toc30636)

[漏洞证明 14](#_Toc13828)

[修复意见 14](#_Toc29171)

[3.5 弱口令漏洞【高风险】 15](#_Toc21299)

[漏洞描述 15](#_Toc17014)

[漏洞地址 15](#_Toc1299)

[漏洞证明 15](#_Toc28604)

[修复意见 16](#_Toc11569)

[4其他 17](#_Toc32183)

[附录1:漏洞参考标准 18](#_Toc11752)

# 1概述

* 1. 检测范围

本次安全检查范围包括：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **业务系统名称** | **域名/IP** | **所属单位** |
| 1 | VOCs信息管理平台建设 | http://203.207.104.237/organization/login.jsp | 晋城市生态环境局 |
| 2 | 晋城市空气质量实时数据发布系统 | http://10.1.20.213:81 http://203.207.104.223:8076 | 晋城市生态环境局 |
| 3 | 数据传输与网络化质控平台 | <http://10.100.20.151:81> | 晋城市生态环境局 |
| 4 | 晋城市市控数据网络化质控平台 | http://10.1.20.225:91 http://10.100.20.149:8001 | 晋城市生态环境局 |
| 5 | 重点监控企业自行监测发布平台 | http://203.207.104.222:7001/jinchengauto/jsp/login.jsp | 晋城市生态环境局 |
| 6 | 晋城市环境监察移动执法系统 | http://203.207.104.227 | 晋城市生态环境局 |
| 7 | 晋城市无组织颗粒物监控系统 | http://203.207.104.221:9999 | 晋城市生态环境局 |
| 8 | 晋城市噪声自动监测系统 | <http://10.100.20.138:9999> | 晋城市生态环境局 |
| 9 | 晋城市地表水水质自动监测系统 | <http://10.100.20.158/watersite> | 晋城市生态环境局 |
| 10 | 重点污染源自动监控与基础数据库系统 | <http://10.100.20.142:8080/jointframe/app> | 晋城市生态环境局 |
| 11 | 晋城市环境网格化管理系统 | http://203.207.104.229:12002/jinhuanbaoms/ | 晋城市生态环境局 |

* 1. 检测时间

2019-6-10至2019-6-14

* 1. 检测方法

本次安全评估是完全站在攻击者的角度，从公网对客户授权范围内的相关域名、IP进行安全检测。检测方法为通过工具和的安全扫描系统进行，扫描系统将自动对目标进行端口、服务、应用等层面的安全漏洞检测。

除了自动化的工具扫描外，安全专家也会手工方式对目标进行检测，手工检测主要用于发现一些使用自动化工具无法检测的安全风险，主要是各类逻辑漏洞，如：登录过程绕过、暴力破解漏洞、任意次数短信发送、绕过表单限制提交资料、越权更改其他用户密码、越权修改用户资料

为避免自动化扫描带来的误报，在扫描完成后，安全服务专家会对扫描结果进行分析处理，排除误报，综合分析漏洞的影响，将最终分析结果汇报给客户。

# 2整体检测结论

2.1 整体安全度

本次检测共发现高危漏洞7个,中危漏洞387个，低危漏洞73个。

本次检测对象的总体安全风险为: 高风险

## 2.2 检测对象安全汇总

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **业务名称** | **URL** | **高危** | **中危** | **低危** |
| 1 | VOCs信息管理平台建设 | http://203.207.104.237/organization/login.jsp | / | / | 2 |
| 2 | 晋城市空气质量实时数据发布系统 | http://10.1.20.213:81 http://203.207.104.223:8076 | 3 | 1 | 10 |
| 3 | 数据传输与网络化质控平台 | <http://10.100.20.151:81> | / | 6 | 6 |
| 4 | 晋城市市控数据网络化质控平台 | http://10.1.20.225:91 http://10.100.20.149:8001 | 0 | 12 | 12 |
| 5 | 重点监控企业自行监测发布平台 | http://203.207.104.222:7001/jinchengauto/jsp/login.jsp | 0 | 2 | 1 |
| 6 | 晋城市环境监察移动执法系统 | http://203.207.104.227 | 1 | 353 | 25 |
| 7 | 晋城市无组织颗粒物监控系统 | http://203.207.104.221:9999 | 0 | 1 | 5 |
| 8 | 晋城市噪声自动监测系统 | <http://10.100.20.138:9999> | 0 | 3 | 4 |
| 9 | 晋城市地表水水质自动监测系统 | <http://10.100.20.158/watersite> | 2 | 3 | 3 |
| 10 | 重点污染源自动监控与基础数据库系统 | <http://10.100.20.142:8080/jointframe/app> | 1 | 5 | 2 |
| 11 | 晋城市环境网格化管理系统 | http://203.207.104.229:12002/jinhuanbaoms/ | 0 | 1 | 3 |

## 2.3 检测对象迁云建议

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **业务名称** | **URL** | **迁云建议** |
| 1 | VOCs信息管理平台建设 | http://203.207.104.237/organization/login.jsp | 可直接迁云 |
| 2 | 晋城市空气质量实时数据发布系统 | http://10.1.20.213:81 http://203.207.104.223:8076 | 漏洞修复后可迁云 |
| 3 | 数据传输与网络化质控平台 | <http://10.100.20.151:81> | 可直接迁云 |
| 4 | 晋城市市控数据网络化质控平台 | http://10.1.20.225:91 http://10.100.20.149:8001 | 可直接迁云 |
| 5 | 重点监控企业自行监测发布平台 | http://203.207.104.222:7001/jinchengauto/jsp/login.jsp | 可直接迁云 |
| 6 | 晋城市环境监察移动执法系统 | http://203.207.104.227 | 漏洞修复后可迁云 |
| 7 | 晋城市无组织颗粒物监控系统 | http://203.207.104.221:9999 | 可直接迁云 |
| 8 | 晋城市噪声自动监测系统 | <http://10.100.20.138:9999> | 可直接迁云 |
| 9 | 晋城市地表水水质自动监测系统 | <http://10.100.20.158/watersite> | 漏洞修复后可迁云 |
| 10 | 重点污染源自动监控与基础数据库系统 | <http://10.100.20.142:8080/jointframe/app> | 漏洞修复后可迁云 |
| 11 | 晋城市环境网格化管理系统 | http://203.207.104.229:12002/jinhuanbaoms/ | 可直接迁云 |

# 3测试结果

## 3.1IIS短文件名泄露漏洞【高风险】

### 漏洞描述

Internet Information Services（IIS，互联网信息服务）是由微软公司提供的基于运行Microsoft Windows的互联网基本服务。

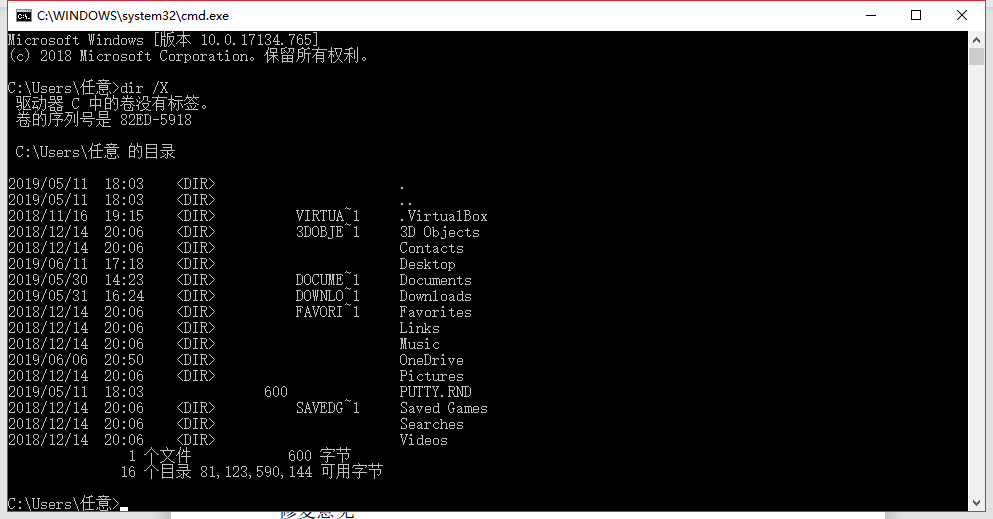
Microsoft IIS在实现上存在文件枚举漏洞，攻击者可以利用“~”字符猜解或遍历服务器中的文件名，或对IIS服务器中的.Net Framework进行拒绝服务攻击。

### 漏洞地址

* <http://203.207.104.223:8076/>
* http://10.1.20.213:81

### 漏洞证明

为了兼容16位MS-DOS程序，Windows为文件名较长的文件（和文件夹）生成了对应的windows 8.3 短文件名。 在Windows下查看对应的短文件名，可以使用命令 dir /x



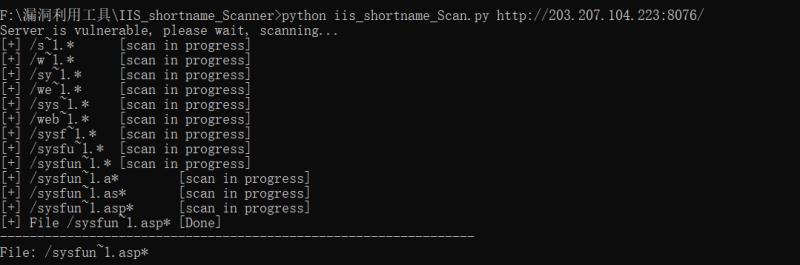
只有前六位字符直接显示，后续字符用~1指代。其中数字1还可以递增，如果存在多个文件名类似的文件（名称前6位必须相同，且后缀名前3位必须相同）。后缀名最长只有3位，多余的被截断。我们可以在启用.net的IIS下暴力列举短文件名，原因是：

访问构造的某个存在的短文件名，会返回404错误。





返回错误404，证明存在该漏洞。



工具验证结果如上图

### 修复意见

* 1.关闭NTFS 8.3文件格式的支持。该功能默认是开启的，对于大多数用户来说无需开启。
* 2.如果是虚拟主机空间用户,可采用以下修复方案：

1）修改注册列表HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation的值为1(此修改只能禁止NTFS8.3格式文件名创建,已经存在的文件的短文件名无法移除)。

2）如果你的web环境不需要asp.net的支持你可以进入Internet 信息服务(IIS)管理器 --- Web 服务扩展 - ASP.NET 选择禁止此功能。

3）升级net framework 至4.0以上版本。

* 3.将web文件夹的内容拷贝到另一个位置，比如D:\www到D:\www.back，然后删除原文件夹D:\www，再重命名D:\www.back到D:\www。如果不重新复制，已经存在的短文件名则是不会消失的。

## 3.2 Apache Tomcat版本过低【高风险】

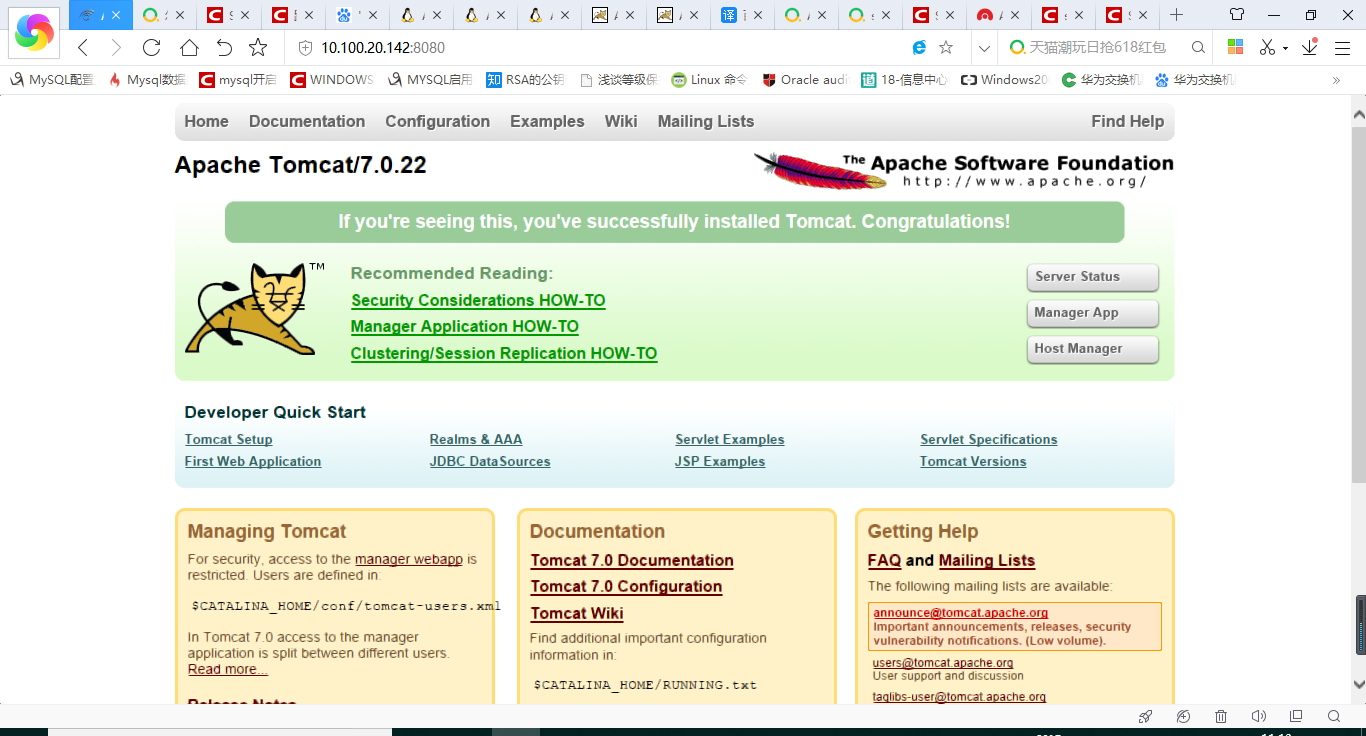
### 漏洞描述

Apache Tomcat版本过低，存在CVE-2012-0022、CVE-2012-2733、CVE-2012 -4534、CVE-2012-3439、CVE-2012-3544、CVE-2012-3546、CVE-2012-4431漏洞。这些漏洞在7.0.32版本中已修复。

### 漏洞地址

* http://10.100.20.142:8080/jointframe/app

### 漏洞证明



### 修复意见

* 建议升级Tomcat版本到7.0.32，修复低版本带来的漏洞。

## 3.3 SQL注入漏洞【高风险】

### 漏洞描述

SQL注入，就是通过把SQL命令插入到Web表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。具体来说，它是利用现有应用程序，将(恶意的)SQL命令注入到后台数据库引擎执行的能力，它可以通过在Web表单中输入(恶意)SQL语句得到一个存在安全漏洞的网站上的数据库，而不是按照设计者意图去执行SQL语句。

### 漏洞地址

* <http://10.100.20.158/watersite>
* <http://10.1.20.213:81/>

### 漏洞证明



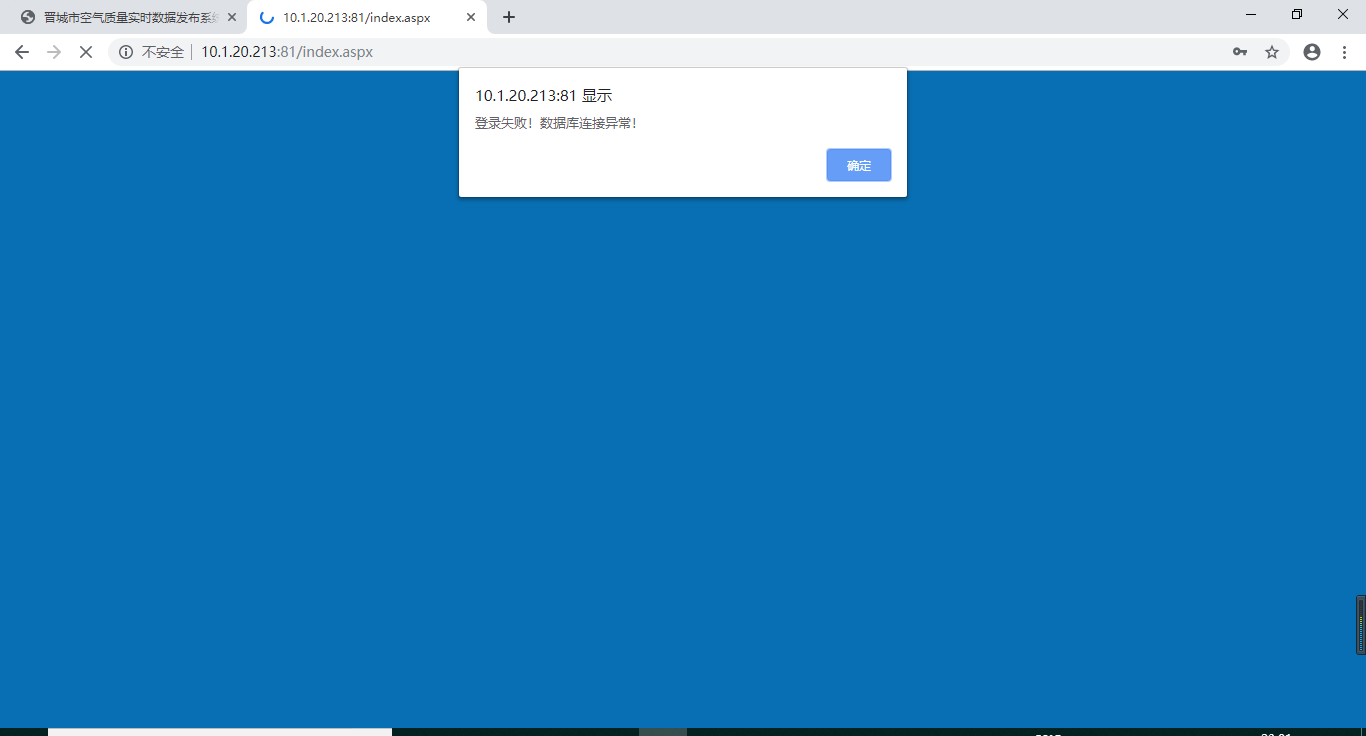
在登录界面输入框构造简单sql语句，注释掉密码内容。



回车登陆后未提示账号密码错误，而是直接报出错误信息。



在登录界面输入框构造简单sql语句，注释掉密码内容。



回车登陆后未提示账号密码错误，而是直接报出数据库错误信息。

### 修复意见

过滤所有输入框输入语句，对数据类型进行校验，过滤敏感和恶意参数符号。

## 3.4 跨站脚本攻击【高风险】

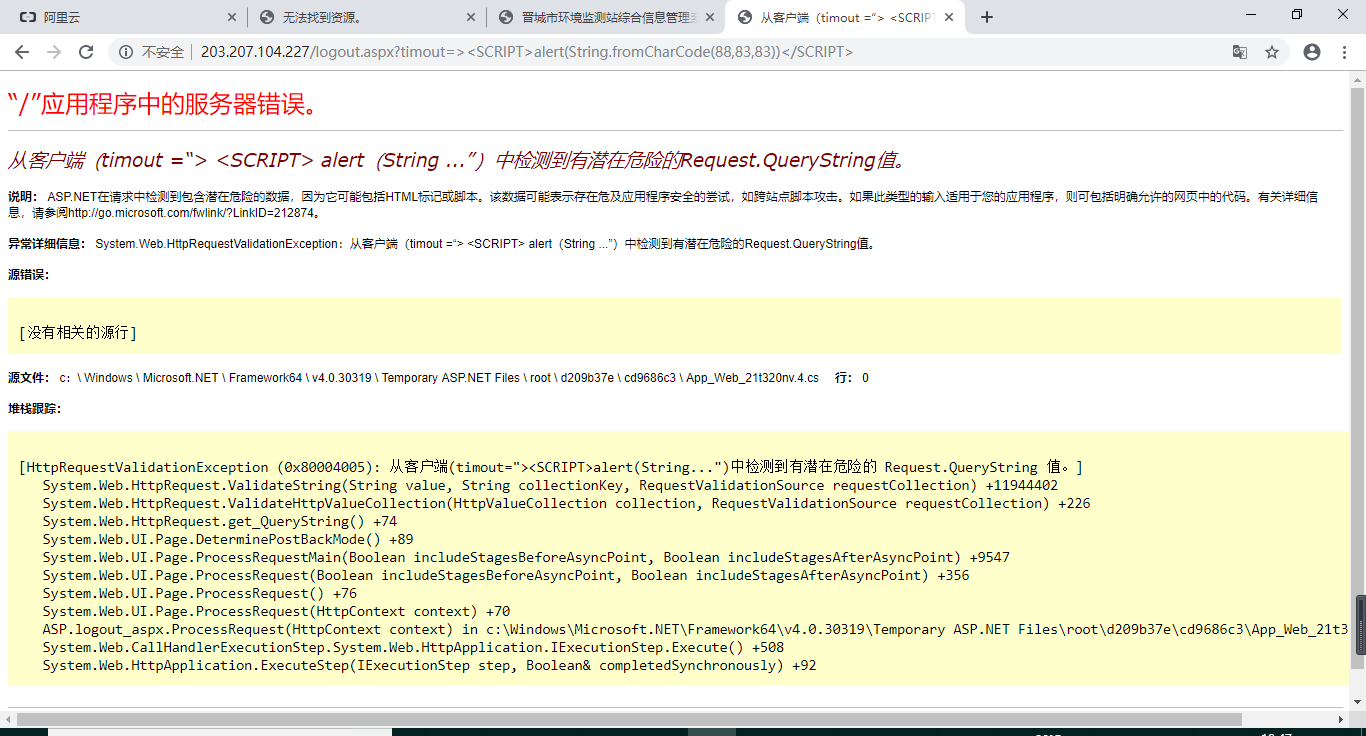
### 漏洞描述

跨站脚本攻击（也称为XSS）指利用网站漏洞从用户那里恶意盗取信息。用户在浏览网站、使用即时通讯软件、甚至在阅读电子邮件时，通常会点击其中的链接。攻击者通过在链接中插入恶意代码，就能够盗取用户信息或在终端用户系统上执行恶意代码。

### 漏洞地址

* http://203.207.104.227

### 漏洞证明



构造带危险语句的url，回车后显示已被拦截。

### 修复意见

该漏洞经验证已被弥补。

## 3.5 弱口令漏洞【高风险】

### 漏洞描述

由于网站在登录时未对登录接口做严格限制，攻击者可通过机器进行大量账户或密码进行猜解，或者攻击者通过收集互联网已泄露的用户和密码信息，生成对应的字典表，尝试批量登陆网站。可导致直接进入系统的风险。

### 漏洞地址

* http://10.100.20.158/watersite

### 漏洞证明





通过手工尝试admin账户和部分简单密码，admin密码尝试成功。

通过测试发现网站并未出现验证码等锁定账户提示。

### 修复意见

* 将网站接入阿里云waf进行有效防护
* 登录处加入验证码或自动刷新验证码
* 设置单个IP登录错误次数

加入密码错误指定次数进行锁定账户

# 4其他

* 账户密码使用明文传输

建议采用SSL加密传输方式。

# 附录1:漏洞参考标准

根据漏洞的危害程度将漏洞等级分为【高】、【中】、【低】三个等级。由安全工程师结合利用场景中漏洞的严重程度、利用难度等综合因素，对漏洞进行定级。

**存在高危漏洞的业务系统应在漏洞修复后才能上云或对外开放访问，中低等级的漏洞可以先进行上云后部署，并选择合适的时机进行修复。**

漏洞等级的评分标准及漏洞类型如下：

**【高危】**

* 直接获取系统权限的漏洞（服务器权限、PC 客户端权限），包括但不限于远程命令执行、任意代码执行、上传获取 Webshell、SQL 注入获取系统权限、缓冲区溢出（包括可利用的 ActiveX 缓冲区溢出）等漏洞。
* 直接导致重要业务出现拒绝服务的漏洞，包括但不限于直接导致移动网关业务或 API 业务拒绝服务、网站应用拒绝服务等造成严重影响的远程拒绝服务漏洞。
* 重要的敏感信息泄漏，包括但不限于重要业务数据库的 SQL 注入漏洞、可获取大量企业核心业务数据等接口问题引起的敏感信息泄露。
* 严重的逻辑设计缺陷和流程缺陷，包括但不限于批量修改任意账号密码漏洞、涉及企业核心业务的逻辑漏洞等。
* 敏感信息越权访问，包括但不限于绕过认证直接访问管理后台、重要后台弱密码、获取大量内网敏感信息的服务器端请求伪造（SSRF）漏洞等。
* 重要业务越权敏感操作，包括但不限于账号越权修改重要信息、重要业务配置修改等较为重要的越权行为。
* 大范围影响用户的其他漏洞，包括但不限于可造成自动传播的重要页面的存储型跨站脚本攻击漏洞（包括存储型 DOM-XSS）。

**【中危】**

* 需交互方可影响用户的漏洞，包括但不限于一般页面的存储型跨站脚本攻击漏洞，涉及核心业务的跨站请求伪造（CSRF）漏洞等。
* 普通越权操作，包括但不限于绕过限制修改用户资料、执行用户操作等。
* 普通的逻辑设计缺陷和流程缺陷，包括但不限于不限次数的短信发送、任意手机邮箱信息注册等。

**【低危】**

* 本地拒绝服务漏洞，包括但不限于客户端本地拒绝服务（解析文件格式、网络协议产生的崩溃），以及由 Android 组件权限暴露、普通应用权限引起的问题等。
* 普通信息泄漏，包括但不限于客户端明文存储密码、以及 web 路径遍历、系统路径遍历漏洞等。

其他危害较低的漏洞，包括但不限于反射型跨站脚本攻击漏洞（包括反射型 DOM-XSS）、普通跨站请求伪造（CSRF）、URL跳转漏洞等。