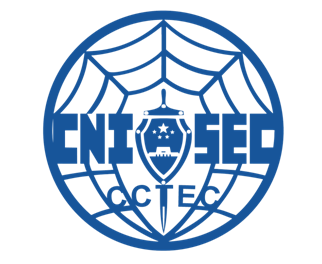
**湘潭市环保局数字环保系统**

**渗透测试报告**

****

|  |  |
| --- | --- |
| 委托单位： | 湘潭市环保局 |
| 报告日期： | 2018年12月14日 |

中国信息安全测评中心华中测评中心

湖南省信息安全测评中心

**声 明**

1. 本报告是独立的第三方测评机构对被测试单位的信息系统进行安全性测评后得出的客观结论。
2. 本报告的结论仅对测试时间段内信息系统现有的状况有效。
3. 本报告中给出的结论，不得作为对被测系统内相关产品的结论。
4. 本报告未经被测单位和中国信息安全测评中心华中测评中心（湖南省信息安全测评中心）书面允许不得节选和复印，复印件需重新加盖“中国信息安全测评中心华中测评中心（湖南省信息安全测评中心）”公章才有效。
5. 任何情况下，若需引用本报告中的内容都应保持其本来意义， 不得擅自增加、修改、伪造或掩盖本报告的原有内容。
6. 本报告无“ 中国信息安全测评中心华中测评中心（湖南省信息安全测评中心）”公章无效，涂改无效；报告无编制人、审核人和批准人签字无效。
7. 对本报告如有异议，可于收到报告之日起十五日内向我单位提出申诉。
8. 本报告一式两份，一份提交委托单位，一份留存本中心。

（盖章）

二〇一八年十二月十四日

**报告基本信息**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **委托单位信息** | | | | | | | | |
| **单位名称** | 湘潭市环保局 | | | | | | | |
| **单位地址** | 湖南省湘潭市建设路 | | | | | | | |
| **项目名称** | 湘潭环保局数字环保系统安全等级测评 | | | | | | | |
| **联系部门** |  | | | | | | | |
| **联系人** |  | | | | 电话 | |  | |
| **评估单位信息** | | | | | | | | |
| **单位名称** | 中国信息安全测评中心华中测评中心  (湖南省信息安全测评中心) | | | | | | | |
| **联系地址** | 湖南省长沙市芙蓉区和光路102号 | | | | | | 邮编 | 410001 |
| **联系方式** | 项目经理 | | 陈果 | 电话 | | | (0731) 84733345 | |
| **测评日期** | **2018年‎12‎月‎12日至2018‎年‎12‎月‎13‎日** | | | | | | | |
| **报告审批信息** | | | | | | | | |
| 编制： | | 审核： | | | | 批准： | | |
| 日期： | | 日期： | | | | 日期： | | |

# 报告综述

受湘潭市环保局委托，中国信息安全测评中心华中测评中心（湖南省信息安全测评中心）（以下简称“华中测评中心”）于2018年‎12‎月‎12日至2018年‎12‎月‎1‎3日对湘潭市环保数字环保系统进行了安全测评。

本次涉及到的测试范围是湘潭市环保局数字环保系统。具体测评内容包括渗透测试和综合风险分析与研判等。通过测评发现被测系统存在安全隐患，主要表现在：

**渗透性测试方面**：SQL注入漏洞、跨站脚本攻击漏洞、任意文件上传、任意文件下载、垂直越权漏洞、平行越权漏洞、Struts2框架漏洞，服务端请求伪造。

**目 录**

[报告综述 i](#_Toc532550778)

[第1章 评估综述 1](#_Toc532550779)

[1.1 背景 1](#_Toc532550780)

[1.2 参考标准 1](#_Toc532550781)

[1.3 测评时间及地点 1](#_Toc532550782)

[第2章 测评对象 2](#_Toc532550783)

[2.1 系统构成 2](#_Toc532550784)

[2.1.1 应用系统 2](#_Toc532550785)

[第3章 测评方法 3](#_Toc532550786)

[第4章 测评记录 4](#_Toc532550787)

[4.1 应用安全 4](#_Toc532550788)

[网上办事大厅审批系统 4](#_Toc532550789)

[湘潭市机动车环保管理信息系统 9](#_Toc532550790)

[移动执法系统 13](#_Toc532550791)

[重点污染源自动监控与基础数据库系统 16](#_Toc532550792)

[第5章 测评总结 19](#_Toc532550793)

# 评估综述

## 背景

2018年‎12‎月‎1‎2日至2018年‎12‎月‎1‎3日，中国信息安全测评中心华中测评中心（湖南省信息安全测评中心）受湘潭市环保局的委托和授权，对湘潭市环保局数字环保系统进行了安全测评。

此次安全性测试的目的在于，基于现行的应用系统自身的安全功能以及系统网络、主机以及数据安全，通过配置核查、漏洞扫描以及渗透性测试等安全检测方法，测试并发掘被测系统存在的安全问题，事先地、主动地暴露湘潭市环保局网站系统存在的安全脆弱点和漏洞，进而可以对其进行消除、弥补处理，避免将来可能产生的经济上、名誉上的损失。

本文档主要描述中国信息安全测评中心华中测评中心（湖南省信息安全测评中心）对湘潭市环保局网站系统安全性测试的过程和结果，侧重于测试结果描述及其影响后果，并对相关安全漏洞问题提出整改建议。

## 参考标准

* GB/T 20274-2006 《信息系统安全保障评估框架》
* GB/T 20984-2007 《信息安全风险评估规范》
* GB/T 18336-2008 《信息技术安全性评估准则》
* GB/T 22239-2008 《信息系统安全保护等级基本要求》

## 测评时间及地点

此次安全性测试评估的工作时间为：2018年‎12‎月12日至2018年‎12‎月13‎日。

此次工作地点位于湘潭市环保局。

# 测评对象

## 系统构成

本次测评对象所包含的应用系统的资产清单如下：

### 应用系统

| 序号 | 应用系统名称 | 应用IP域名 | IP地址 |
| --- | --- | --- | --- |
| 1 | 湘潭市环保局办公系统 | http://10.43.48.57:4833/ | 10.43.48.57 |
| 2 | 湘潭市机动车环保管理信息系统 | http://10.43.48.63:8888/jdczx/ | 10.43.48.63 |
| 3 | 重点污染源监控系统 | http://10.43.48.5:8080/jointframe/app | 10.43.48.5 |
| 4 | 移动执法系统 | http://10.43.48.10:8000/ydzfxt/ | 10.43.48.10 |
| 5 | 网上办事大厅审批系统 | http://10.43.48.55:8080/wssp/ | 10.43.48.55 |

# 测评方法

本次安全测评的主要方式如下表所示：

表 3‑1 主要测评方式

| **序号** | **测评方式** | **具体测评方法** |
| --- | --- | --- |
|  | 配置核查 | 根据最佳实践所总结出的核查表单对网络设备、安全设备、操作系统、数据库、中间件和应用服务进行手工配置核查。 |
|  | 漏洞扫描 | 分为基于WEB的扫描和非WEB的扫描。基于WEB的扫描主要针对WEB应用系统，非WEB的扫描则主要对选定网段的主机进行扫描。 |
|  | 渗透测评 | 包括内部和外部的渗透测评：  模拟内部职员向主机端渗透；  模拟互联网用户向主机端渗透。 |
|  | 访谈 | 根据文档审核和技术测评的结果，与相关人员访谈了解、确认系统的安全状况。 |
|  | 文档审核 | 审核系统设计、开发、部署、运行维护的制度、流程、记录。 |
|  | 观察 | 通过观察配合人员的技术操作流程验证安全管理的有效性。 |

# 测评记录

## 应用安全

### 网上办事大厅审批系统

#### 大量sql注入漏洞

**漏洞描述：**通过把SQL命令插入到Web表单提交、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。攻击者通过该漏洞可以获取数据库的敏感信息，如数据库中的帐号、密码等也可能查看、删除、修改数据库记录和表。

**整改建议：**使用预处理执行SQL语句，对所有传入SQL语句中的变量，做绑定。这样，用户拼接进来的变量，无论内容是什么，都会被当做替代符号“?”所替代的值，数据库也不会把恶意用户拼接进来的数据，当做部分SQL语句去解析。

**测试截图：**



**图1‑1**存在漏洞的查询处



**图1‑2**注入出的数据库名以及payload

#### 服务端请求伪造漏洞（ssrf）

**漏洞描述：**服务器端请求伪造，利用漏洞伪造服务器端发起请求，从而突破客户端获取不到数据限制。一般情况下，SSRF攻击的目标是从外网无法访问的内部系统。

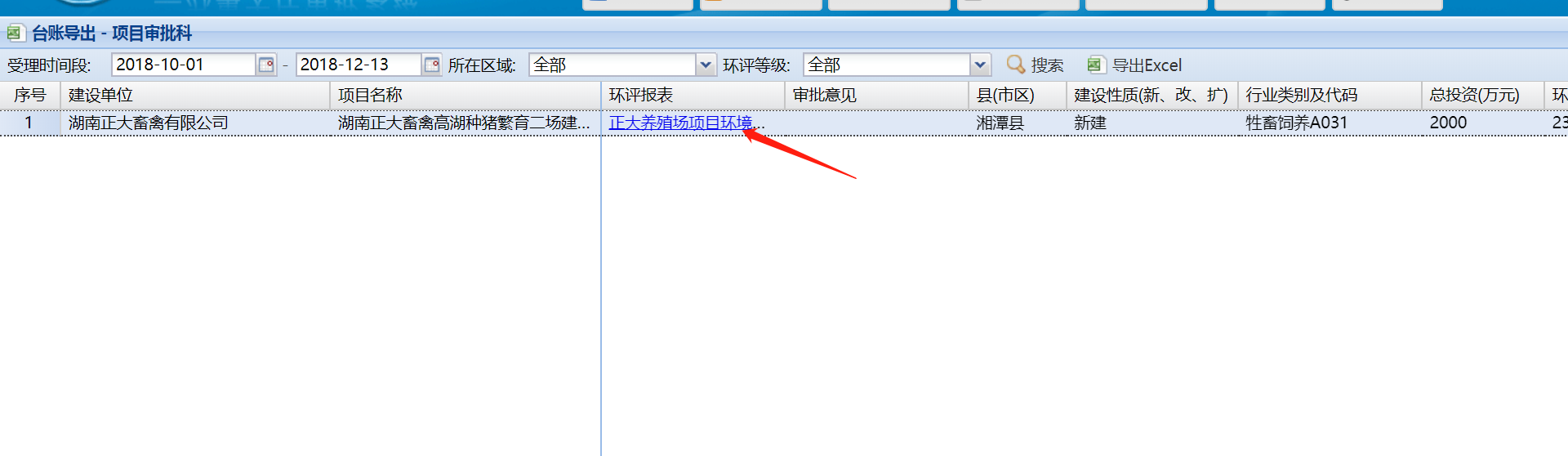
**漏洞链接：**

<http://10.43.48.55:8080/wssp/fileDownloadAction!downloadfile?fileName=http://10.43.48.18:808/jsxm/%E6%AD%A3%E5%A4%A7%E5%85%BB%E6%AE%96%E5%9C%BA%E9%A1%B9%E7%9B%AE%E7%8E%AF%E5%A2%83%E5%BD%B1%E5%93%8D%E6%8A%A5%E5%91%8A%E4%B9%A6%E5%85%A8%E6%96%87%E6%9C%AC_20181105164740486.pdf>

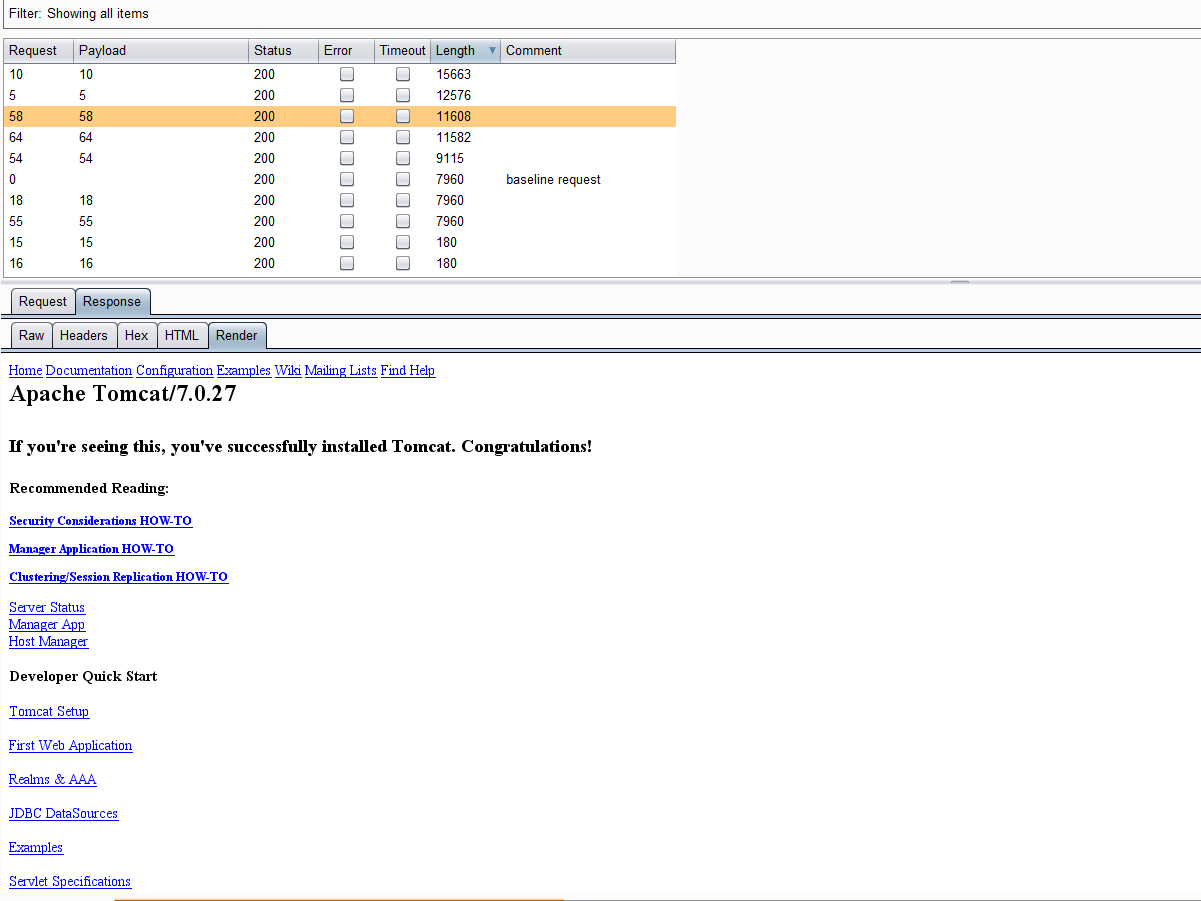
**整改建议：**

1,过滤返回信息，验证远程服务器对请求的响应是比较容易的方法。如果web应用是去获取某一种类型的文件。那么在把返回结果展示给用户之前先验证返回的信息是否符合标准。2, 统一错误信息，避免用户可以根据错误信息来判断远端服务器的端口状态。3,限制请求的端口为http常用的端口，比如，80,443,8080,8090。4,黑名单内网ip。避免应用被用来获取获取内网数据，攻击内网。5,禁用不需要的协议。仅仅允许http和https请求。可以防止类似于file:///,gopher://,ftp:// 等引起的问题。

**测试截图：**



**图1‑3存在ssrf漏洞功能处**



**图1‑4扫描探测内网主机**

#### 万能密码漏洞

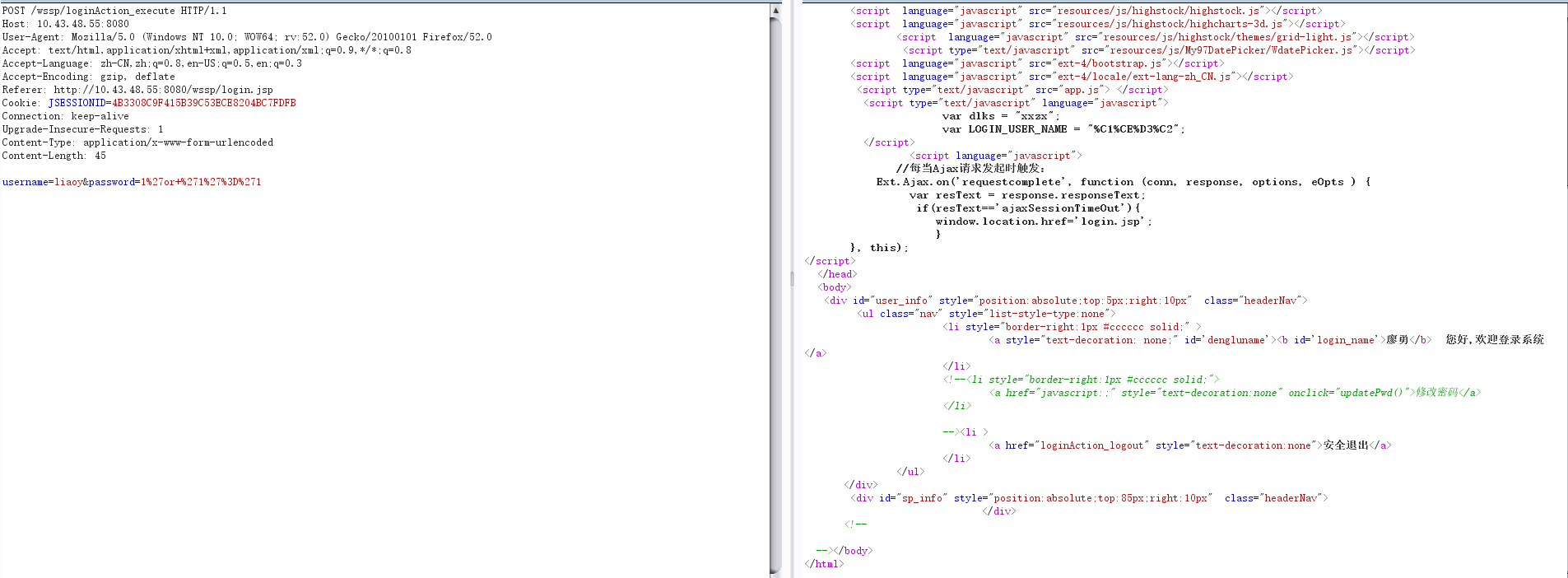
**漏洞描述：**由于登陆处未对用户输入做验证，并且存在sql拼接形式，用户构造语句绕过密码验证登陆判断条件。

**整改建议：**使用预处理执行SQL语句，对所有传入SQL语句中的变量，做绑定。这样，用户拼接进来的变量，无论内容是什么，都会被当做替代符号“?”所替代的值，数据库也不会把恶意用户拼接进来的数据，当做部分SQL语句去解析。

**测试截图：**



**图1‑5绕过用户名验证登陆系统**

****



**图1‑6绕过密码限制登陆系统**

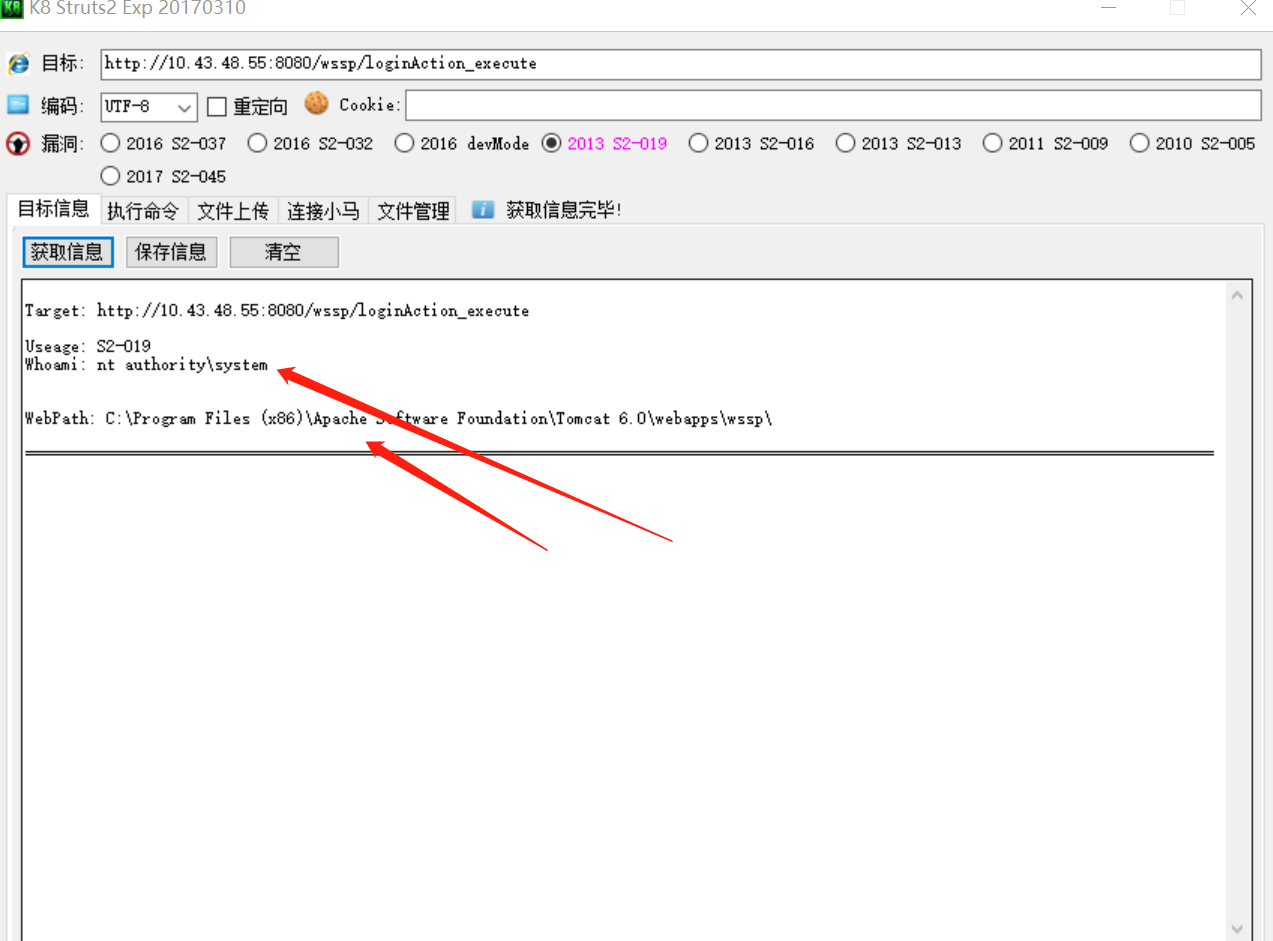
#### Struts2框架漏洞（远程代码执行）

**漏洞描述：**用户通过[浏览器](https://baike.baidu.com/item/%E6%B5%8F%E8%A7%88%E5%99%A8/213911)提交执行命令，由于服务器端没有针对执行函数做过滤，导致在没有指定[绝对路径](https://baike.baidu.com/item/%E7%BB%9D%E5%AF%B9%E8%B7%AF%E5%BE%84/481185)的情况下就执行命令，可能会允许攻击者通过改变 $PATH 或程序执行环境的其他方面来执行一个恶意构造的代码。

**漏洞链接：**http://10.43.48.55:8080/wssp/loginAction\_execute

**整改建议：**升级struts2框架。

**测试截图：**



**图4‑7利用struts2poc工具执行获得服务器的信息。**

### 湘潭市机动车环保管理信息系统

#### 大量sql注入漏洞

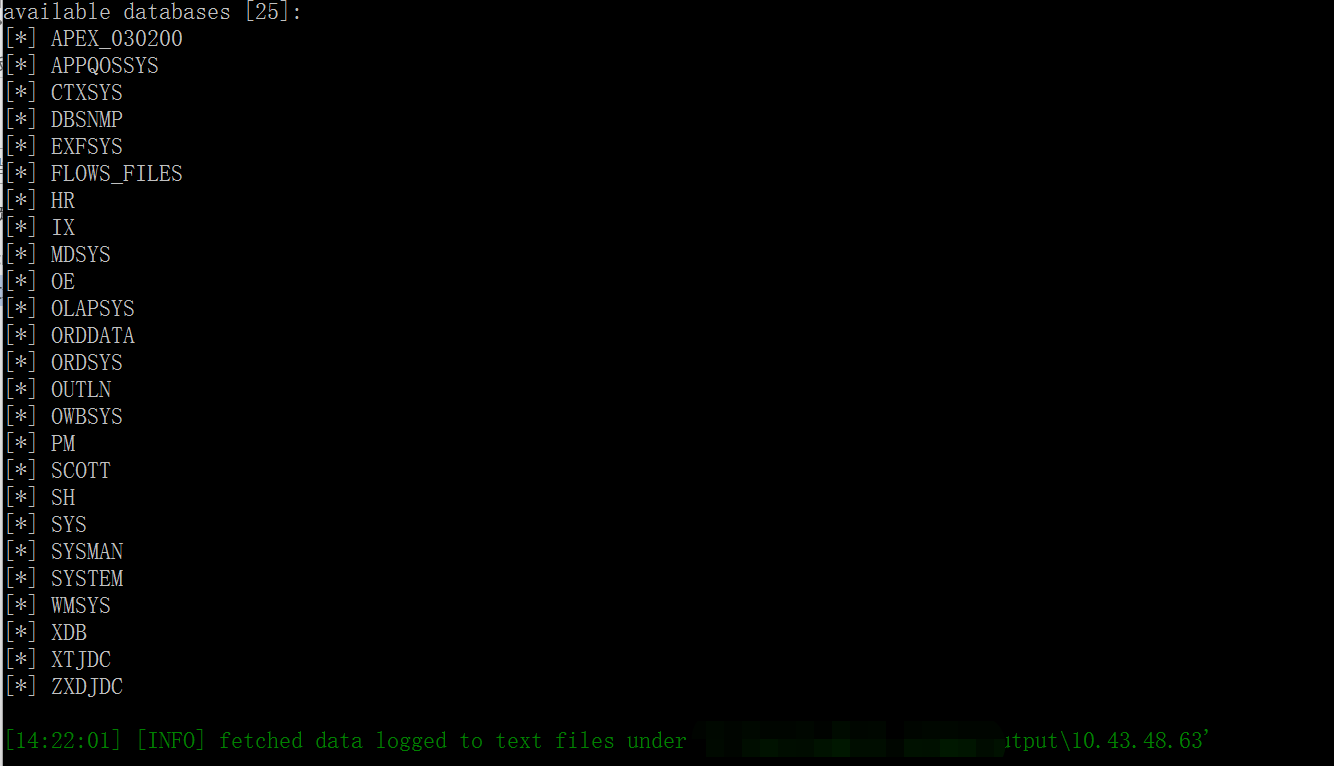
**漏洞描述：**通过把SQL命令插入到Web表单提交、输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。攻击者通过该漏洞可以获取数据库的敏感信息，如数据库中的帐号、密码等也可能查看、删除、修改数据库记录和表。

**整改建议：**使用预处理执行SQL语句，对所有传入SQL语句中的变量，做绑定。这样，用户拼接进来的变量，无论内容是什么，都会被当做替代符号“?”所替代的值，数据库也不会把恶意用户拼接进来的数据，当做部分SQL语句去解析。

**测试截图：**



**图4‑8**存在漏洞的查询处



**图4‑9**注入出的数据库名

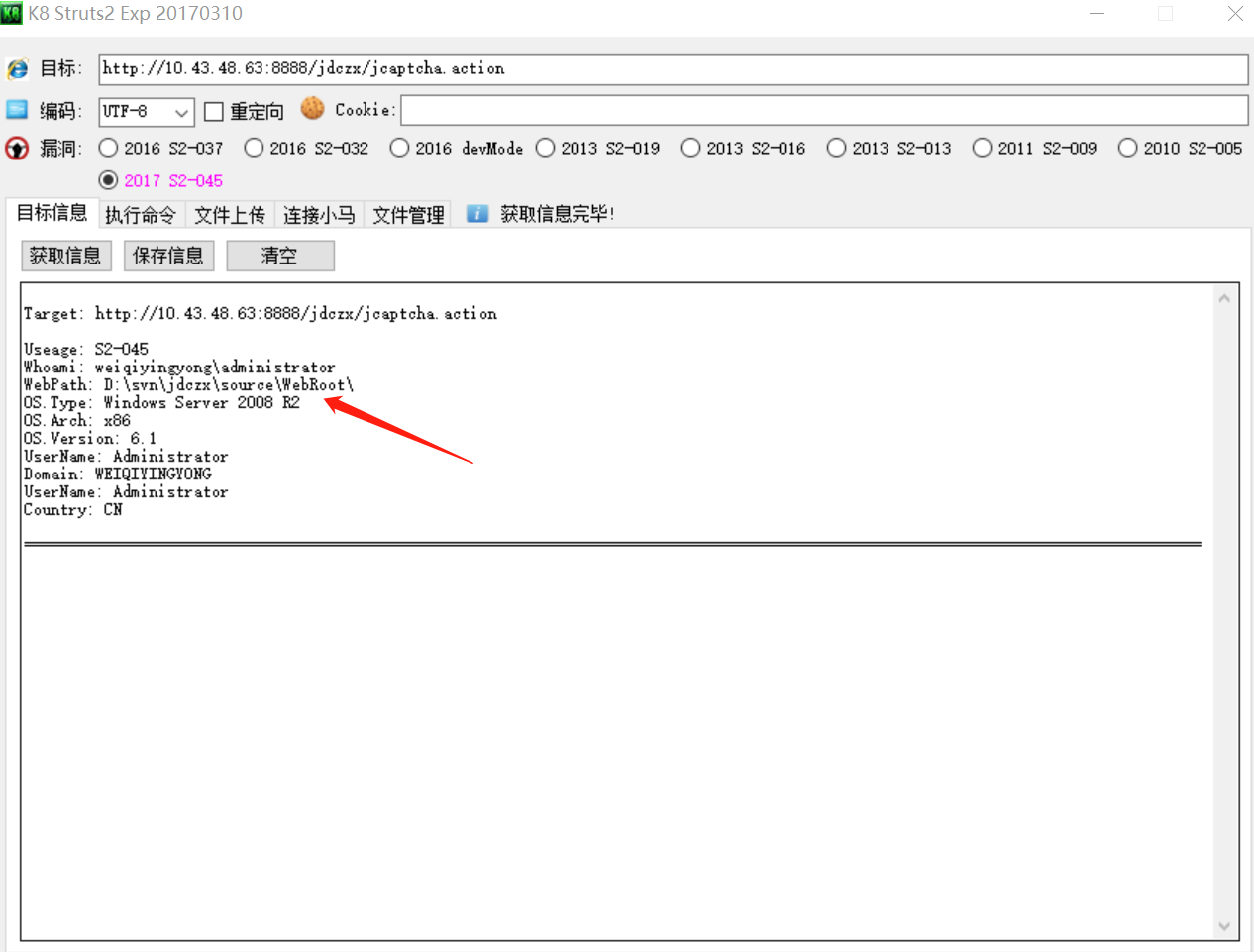
#### Struts2框架漏洞（远程代码执行）

**漏洞描述：**用户通过[浏览器](https://baike.baidu.com/item/%E6%B5%8F%E8%A7%88%E5%99%A8/213911)提交执行命令，由于服务器端没有针对执行函数做过滤，导致在没有指定[绝对路径](https://baike.baidu.com/item/%E7%BB%9D%E5%AF%B9%E8%B7%AF%E5%BE%84/481185)的情况下就执行命令，可能会允许攻击者通过改变 $PATH 或程序执行环境的其他方面来执行一个恶意构造的代码。

**漏洞链接：**http://10.43.48.63:8888/jdczx/jcaptcha.action

**整改建议：**升级struts2框架。

**测试截图：**



**图4‑10利用struts2poc工具执行获得服务器的信息。**

#### 任意文件上传

**漏洞描述：**Web应用程序在处理用户上传的文件时，没有判断文件的扩展名是否在允许的范围内，就把文件保存在服务器上，导致恶意用户可以上传任意文件，甚至上传脚本木马到web服务器上，直接控制web服务器。

**整改建议：**处理用户上传文件，要做以下检查：

检查上传文件扩展名白名单，不属于白名单内，不允许上传。

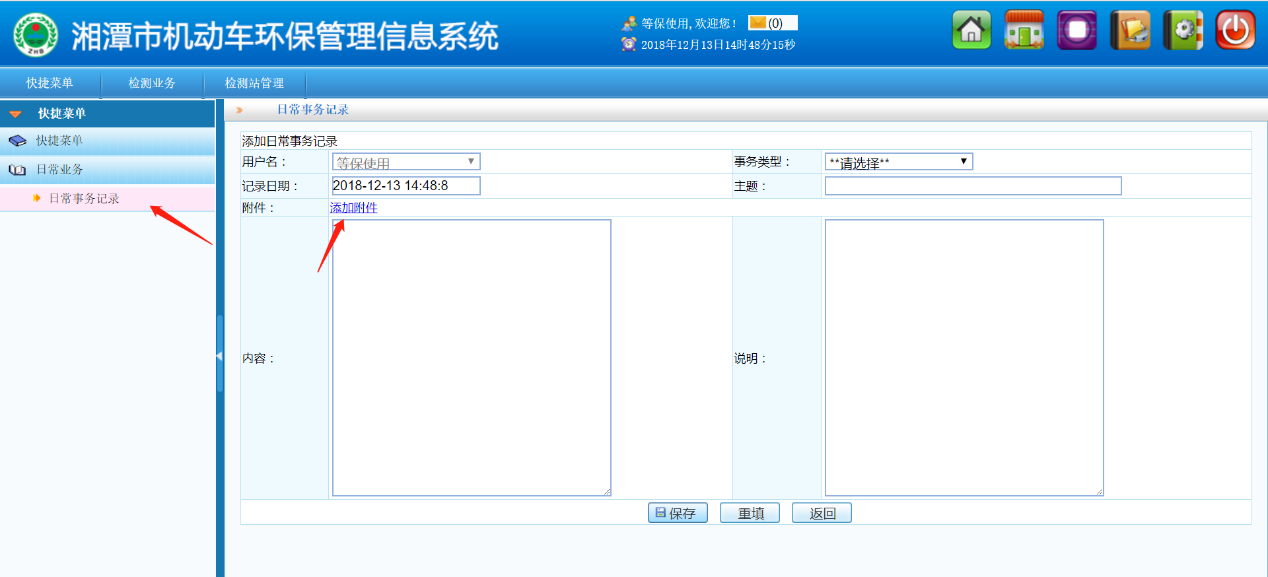
上传文件的目录必须是http请求无法直接访问到的。如果需要访问的，必须上传到其他（和web服务器不同的）域名下，并设置该目录为不解析jsp等脚本语言的目录。

上传文件要保存的文件名和目录名由系统根据时间生成，不允许用户自定义。

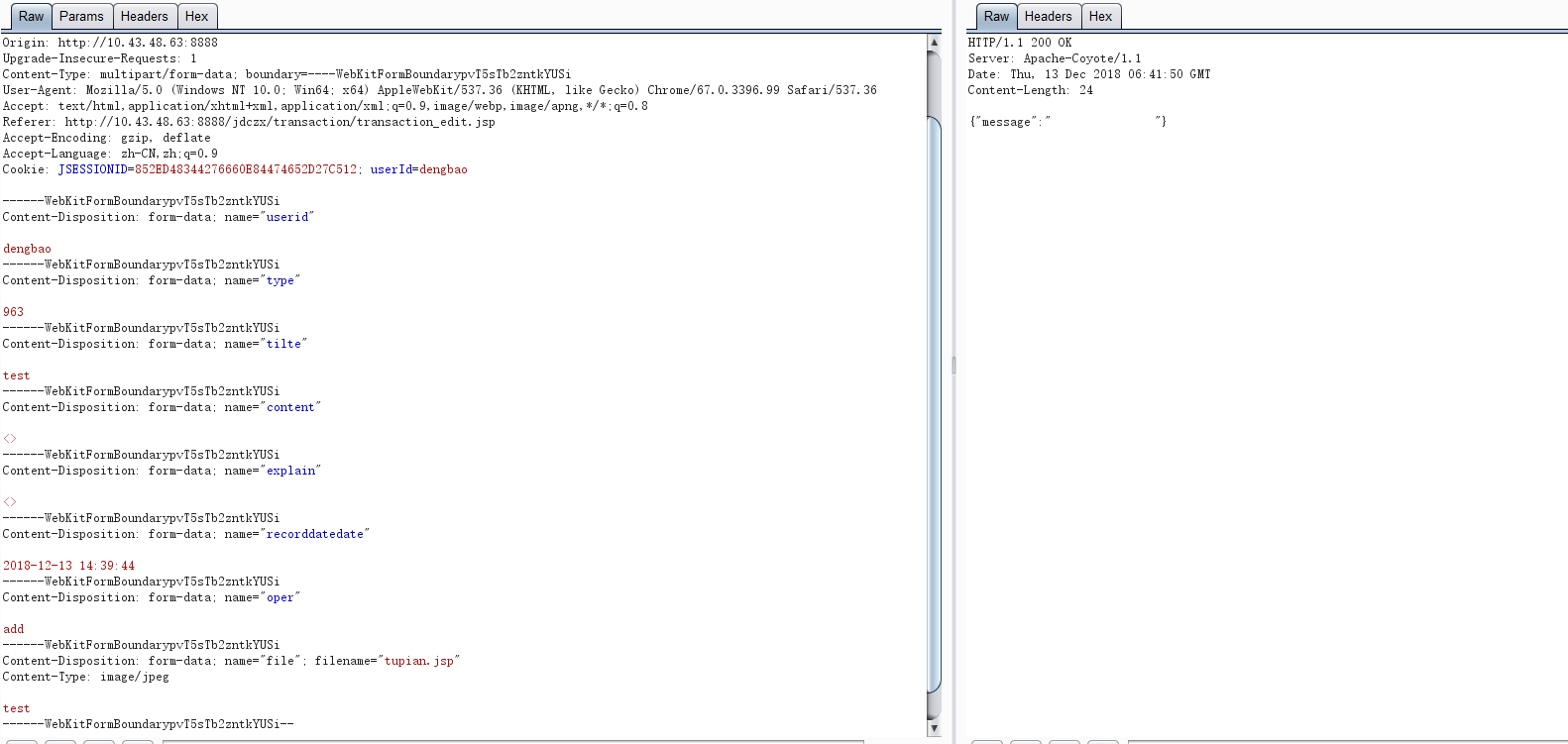
图片上传，要通过处理（缩略图、水印等），无异常后才能保存到服务器。

上传文件需要做日志记录。

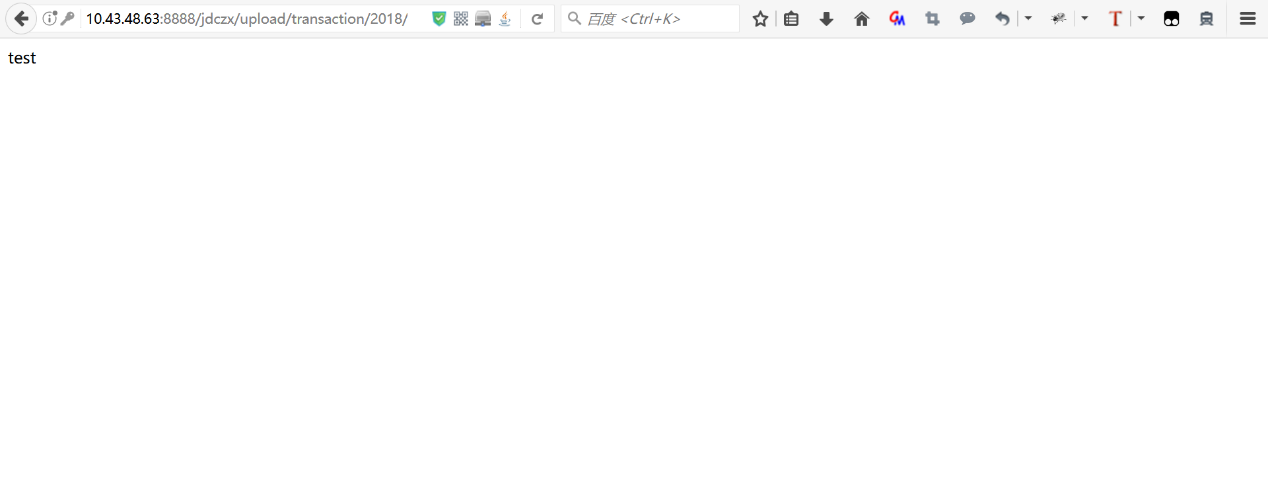
**测试截图：**



**图4‑11上传文件的位置**



**图4‑12上传可执行脚本**



**图4‑13访问上传可执行脚本url**

### 移动执法系统

#### 任意文件上传，路径操纵

**漏洞描述：**Web应用程序在处理用户上传的文件时，没有判断文件的扩展名是否在允许的范围内，就把文件保存在服务器上，并且能用户自定义目录名，导致恶意用户可以上传任意文件，甚至上传脚本木马到web服务器上，直接控制web服务器。

**整改建议：**处理用户上传文件，要做以下检查：

写入网站的目录不要用户自定义输入。

检查上传文件扩展名白名单，不属于白名单内，不允许上传。

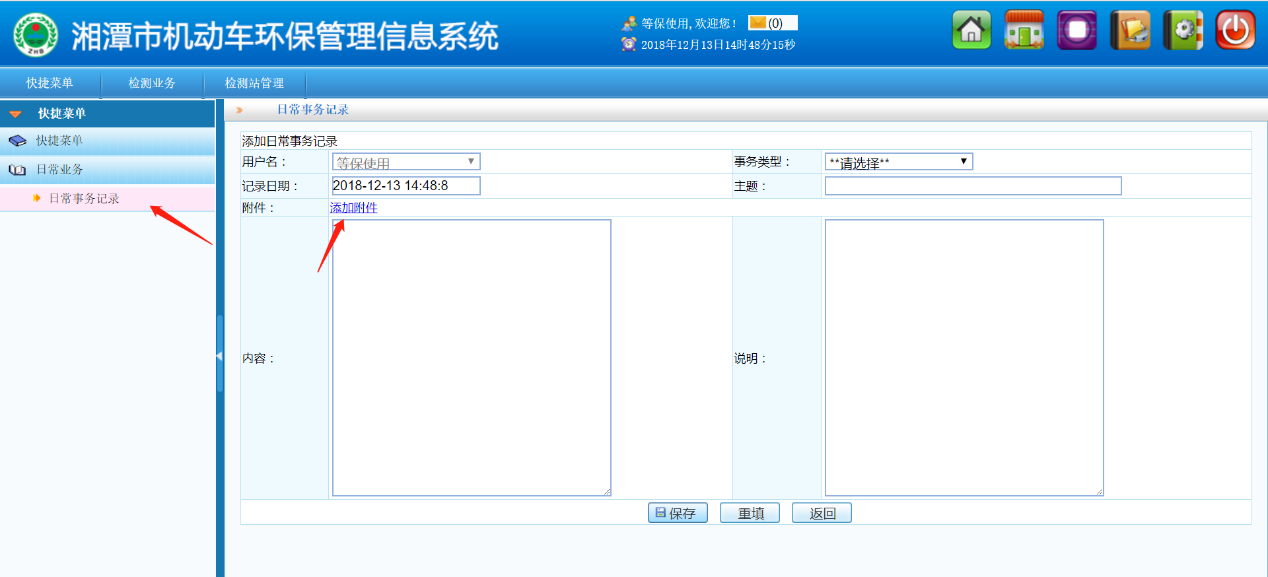
上传文件的目录必须是http请求无法直接访问到的。如果需要访问的，必须上传到其他（和web服务器不同的）域名下，并设置该目录为不解析jsp等脚本语言的目录。

上传文件要保存的文件名和目录名由系统根据时间生成，不允许用户自定义。

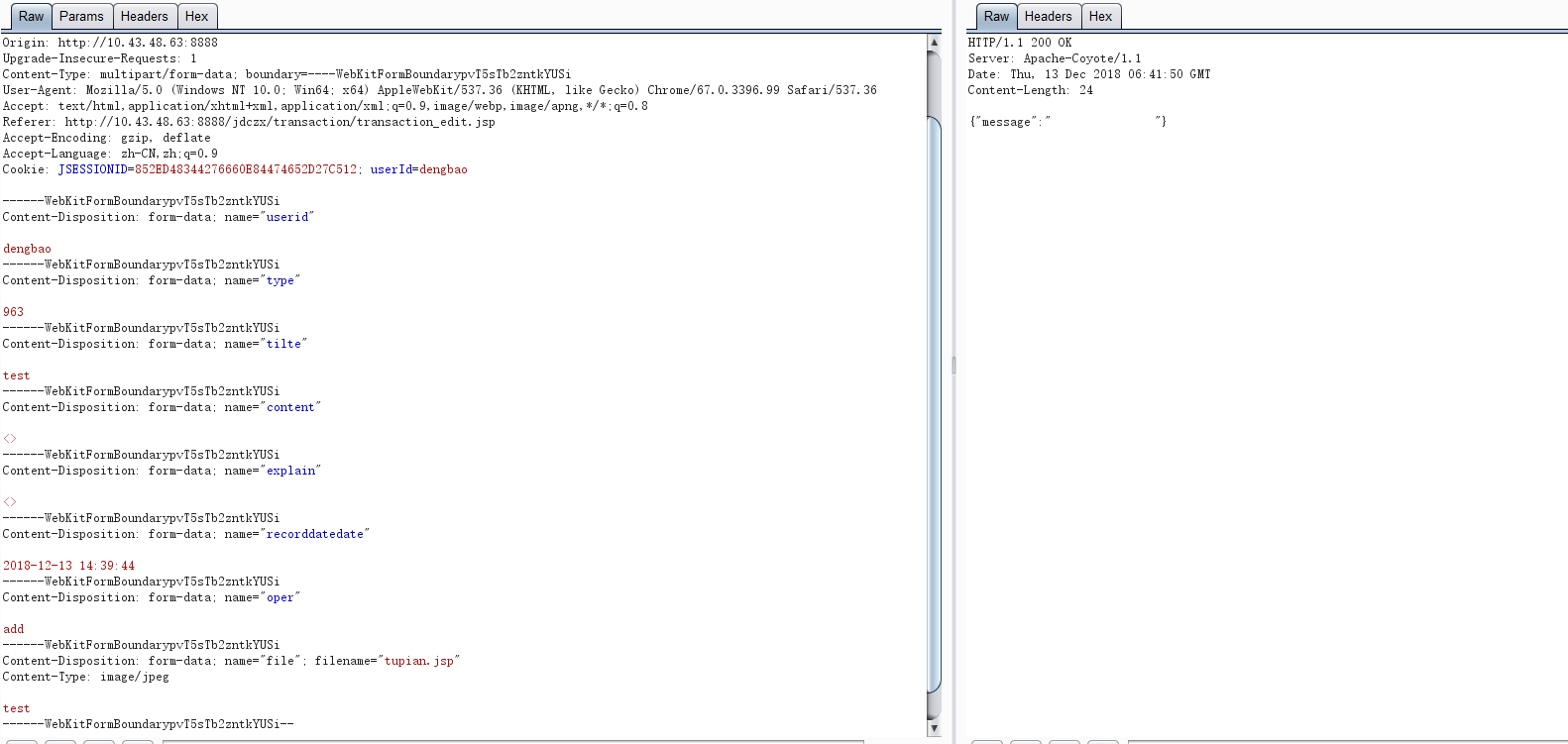
图片上传，要通过处理（缩略图、水印等），无异常后才能保存到服务器。

上传文件需要做日志记录。

**测试截图：**



**图1‑5上传文件的位置**



**图1‑6上传可执行脚本的位置**

#### 任意文件下载

**漏洞描述：**处理用户请求下载文件时，允许用户提交任意文件路径，并把服务器上对应的文件直接发送给用户，这将造成任意文件下载威胁。如果让用户提交文件目录地址，就把目录下的文件列表发给用户，会造成目录遍历安全威胁。

恶意用户会变换目录或文件地址，下载服务器上的敏感文件、数据库链接配置文件、网站源代码等。

**漏洞链接：**

http://10.43.48.10:8000/ydzfxt/ebcm/uploadFile?fjlx=2&url=/WEB-INF/UPLOAD\_FILE/2/21/../../7680015020/1544606174557/tupian.jsp

**修复建议：**

对文件操作功能，做到以下几点：

1，要下载的文件地址保存至数据库中。

2，文件路径保存至数据库，让用户提交文件对应ID下载文件。

3，下载文件之前做权限判断。

4，文件放在web无法直接访问的目录下。

5，记录文件下载日志（内容见日志章节）。

6，不允许提供目录遍历服务。

记录不符合规范的上传文件日志

漏洞截图：



**图3-3存在漏洞任意文件下载功能处**



**图3-4下载网站配置文件**

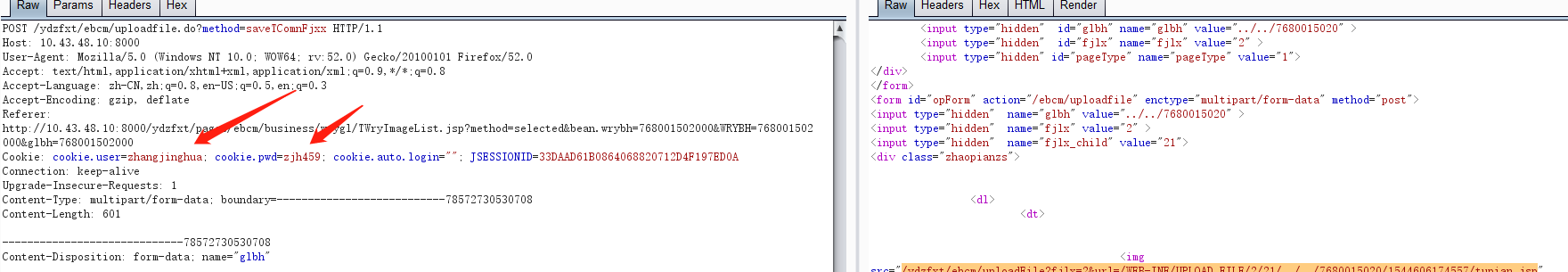
#### 敏感信息泄露

**漏洞描述：**系统返回用户信息时将用户密码等敏感信息返回给用户。

**修复建议：**

将用户的敏感信息脱敏处理。

**漏洞截图：**



**3-5请求中cookie信息携带有用户名和密码**。

### 重点污染源自动监控与基础数据库系统

#### 大量sql注入漏洞

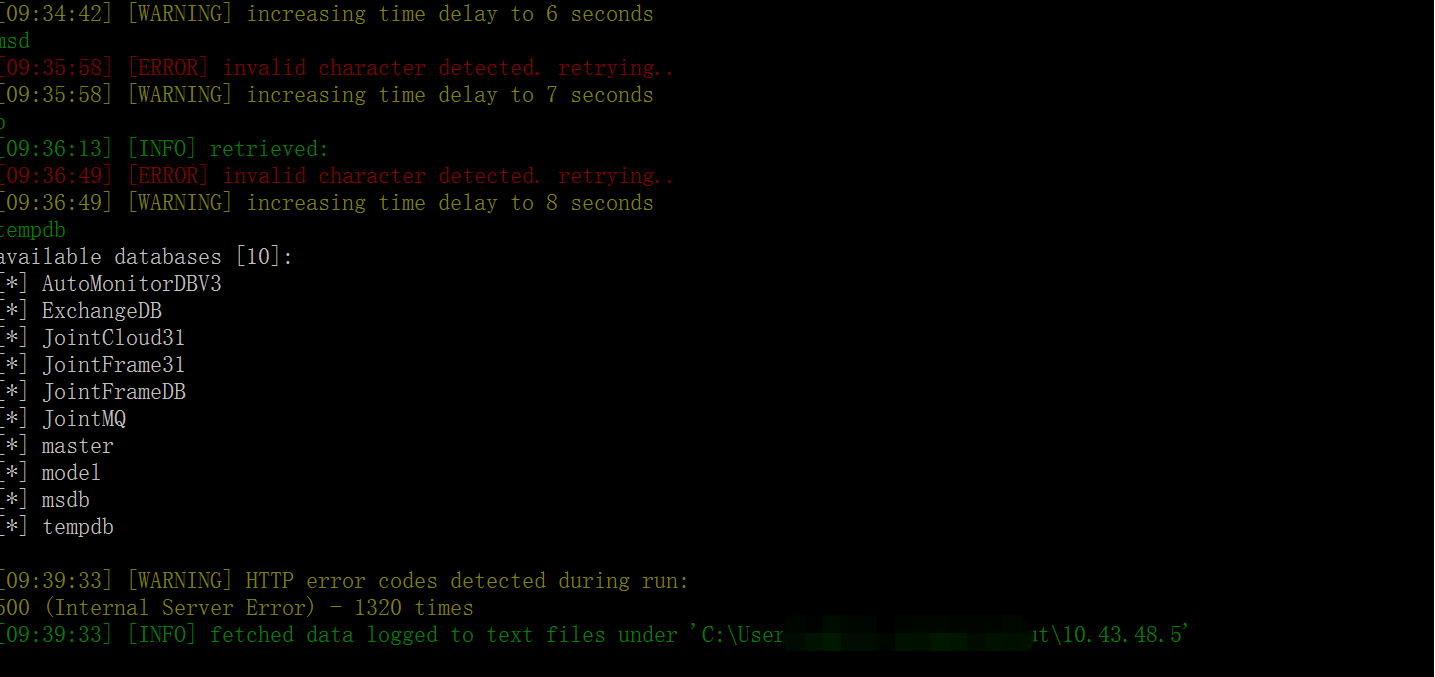
**漏洞描述：**通过把SQL命令插入到Web表单提交、输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。攻击者通过该漏洞可以获取数据库的敏感信息，如数据库中的帐号、密码等也可能查看、删除、修改数据库记录和表。

**整改建议：**使用预处理执行SQL语句，对所有传入SQL语句中的变量，做绑定。这样，用户拼接进来的变量，无论内容是什么，都会被当做替代符号“?”所替代的值，数据库也不会把恶意用户拼接进来的数据，当做部分SQL语句去解析。

**测试截图：**



**图1‑1**存在漏洞的查询处



**图1‑2**注入出的数据库名

#### 任意文件上传

**漏洞描述：**Web应用程序在处理用户上传的文件时，没有判断文件的扩展名是否在允许的范围内，就把文件保存在服务器上，导致恶意用户可以上传任意文件，甚至上传脚本木马到web服务器上，直接控制web服务器。

**整改建议：**处理用户上传文件，要做以下检查：

检查上传文件扩展名白名单，不属于白名单内，不允许上传。

上传文件的目录必须是http请求无法直接访问到的。如果需要访问的，必须上传到其他（和web服务器不同的）域名下，并设置该目录为不解析jsp等脚本语言的目录。

上传文件要保存的文件名和目录名由系统根据时间生成，不允许用户自定义。

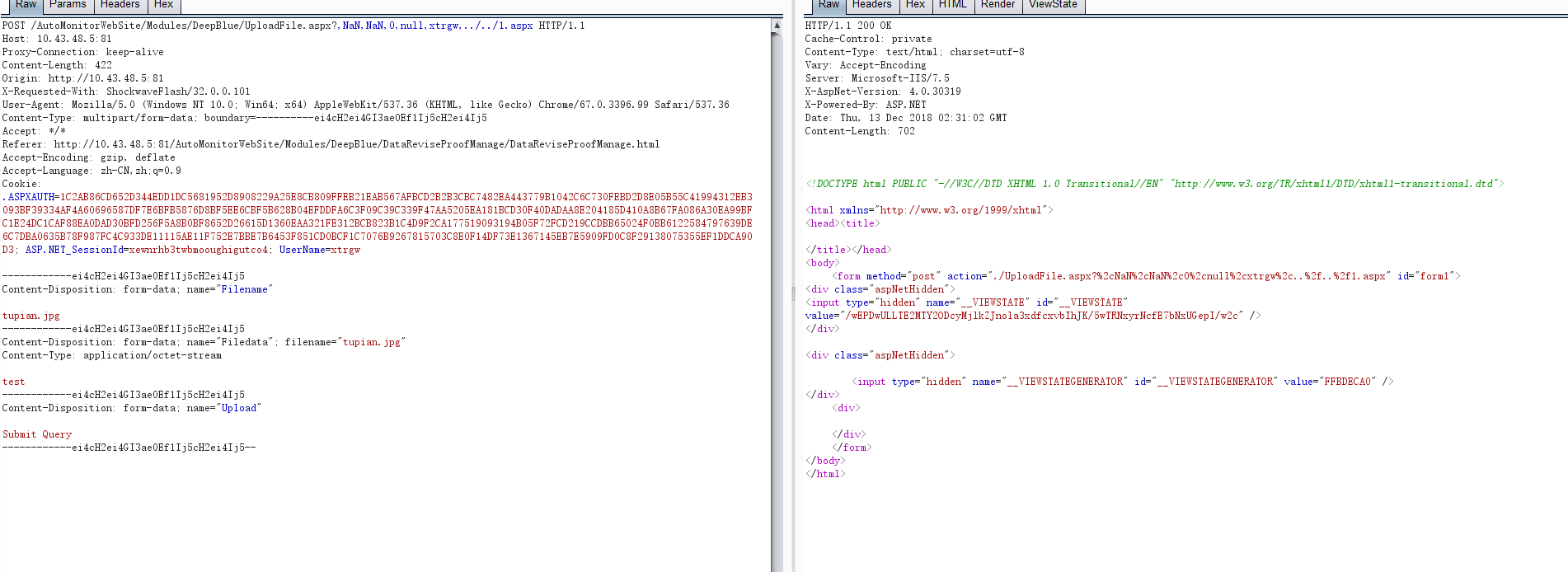
图片上传，要通过处理（缩略图、水印等），无异常后才能保存到服务器。

上传文件需要做日志记录。

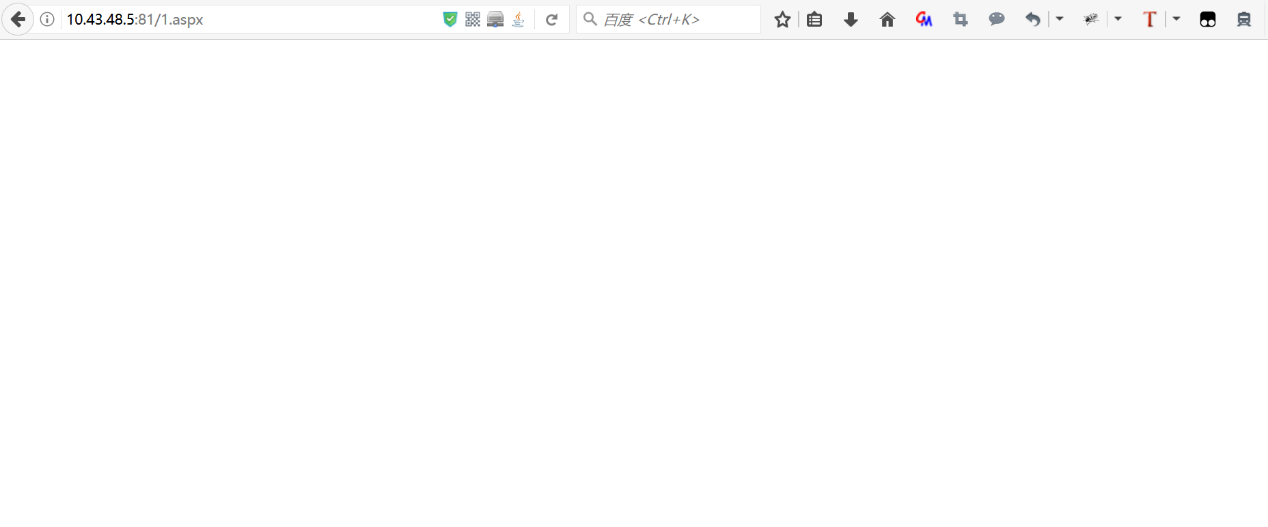
**测试截图：**



**图1‑5上传文件的位置**



**图1‑6抓包上传可执行脚本**

****

**图1‑6可执行脚本的位置**

# 测评总结

依据信息安全标准规范，采用风险分析的方法对测评过程中发现的问题风险分析及等级判定，如下表所示：

表 5‑1 信息系统安全问题风险分析表

| **序号** | **安全层面** | **问题描述** | **风险等级** |
| --- | --- | --- | --- |
|  | 渗透测试 | SQL注入漏洞 | 高 |
|  | 跨站脚本攻击漏洞 | 高 |
|  | 任意文件上传 | 高 |
|  | Struts2框架漏洞 | 高 |
|  | 任意文件下载 | 高 |
|  | 敏感信息泄露 | 高 |
|  | 万能密码漏洞 | 高 |
|  | 服务端请求伪造 | 中 |