奇安信
新一代网络安全领军者

# 泸州市生态环境局

## 重点污染源自动监控与基础数据库系统

## 渗透测试报告

网神信息技术（北京）股份有限公司

2019 年 11 月 19 日

## 版权声明



## 版本变更记录

| 时间 | 版本 | 说明 | 修改人 |
| --- | --- | --- | --- |
| 2019-11-19 | V1.0 | 创建 | 李轶 |
| 2019-11-19 | V1.1 | 修订 | 张瀚文 |

## 适用性说明

本模板用于撰写**奇安信集团**中各种正式文件，包括技术手册、标书、白皮书、会议通知、公司制度等文档使用。

# 目 录

# 1 摘要

经泸州市生态环境局授权，网神于 2019 年 11 月 18 日-2019 年 11 月 19 日对泸州市生态环境局重点污染源自动监控与基础数据库系统进行渗透测试。

# 2 项目信息

## 2.1 委托单位信息

| | | | |
|---|---|---|---|
| **单位名称** | 泸州市生态环境局 | | |
| **委托项目名称** | 泸州市生态环境局关键信息系统安全保障服务项目 | | |
| **单位地址** | 泸州市江阳区春华路二段 66 号 | | |
| **邮政编码** | | **传真** | |
| **联系人** | 罗光华 | **联系电话** | 13568130024 |
| **联系人 E-MAIL** | | | |

## 2.2 测评单位信息

| | | | |
|---|---|---|---|
| **单位名称** | 网神信息技术（北京）股份有限公司 | | |
| **单位地址** | 北京市海淀区昆明湖南路 51 号中关村军民融合产业园 D 座 | | |
| **单位网址** | https://www.qianxin.com/ | | |
| **邮政编码** | | **传真** | |
| **联系人** | 李轶 | **联系电话** | 18200389976 |
| **联系人 E-MAIL** | liyi03@qianxin.com | | |
| 项目组成员：李轶、张瀚文<br>质量监督员：陈浪 | | | |

# 3 项目概述

## 3.1 测试目的

通过本项目的实施，在坚持科学、客观、公正原则的基础上，全面、完整地了解当前**泸州市生态环境局**的安全状况，分析系统所面临的各种风险，模拟攻击者可能利用的漏洞，全面检验泸州市生态环境局网络安全防御体系的有效性。根据测试结果发现系统存在的安全问题，并对严重的问题提出加固的建议。

本次测试预期达到的目标为：

- 通过渗透测试发现泸州市生态环境局目标系统的安全漏洞；
- 针对发现的漏洞提供加固方案及防护建议；

## 3.2 测试范围

本次渗透测试的范围如下：

| 序号 | 名 称 | 备注 |
| --- | --- | --- |
| 1 | 重点污染源自动监控与基础数据库系统 | http://10.194.67.163:8080/jointframe/app/AppMain!index.page |

## 3.3 测试依据

渗透测试服务将参考下列规范进行工作。

- 信息安全技术信息安全风险评估规范（GB/T 20984-2007）
- 信息技术信息安全管理实用规则（GB/T 19716-2005)(ISO/IEC 17799:2000)
- 信息系统安全风险评估实施指南
- 信息系统审计标准（ISACA）
- OWASP OWASP_Testing_Guide_v3
- OWASP OWASP_Development_Guide_2005
- OWASP OWASP_Top_10_2010_Chinese_V1.0

## 3.4 测试工具

- 拓扑分析工具：DNS Sweep、Nslookup 等；
- 自动化扫描工具：Nessus、AIScanner 等；
- 端口扫描、服务检测：Nmap、SuperScan 等；
- 嗅探分析工具：Wireshark、Entercap、Dsniff 等；
- Exploiting 利用工具：Metasploit Framework、Core Impact、Canvas 等；
- 应用缺陷分析工具：SQLMAP 等。

# 4 漏洞详情

渗透测试结果及风险分布如下：

- ☑ 高危问题：0 个
- ☑ 中危问题：3 个
- ☑ 低危问题：1 个

| 系统名称 | 地址 | 漏洞名称 | 危害程度 |
|---|---|---|---|
| 重点污染源自动监控与基础数据库系统 | http://10.194.67.163:8080/jointframe/app/AppMain!index.page | 未授权访问 | 中危 |
| | | 用户名密码明文传输 | 低危 |
| | | 暴力破解 | 中危 |
| | | 任意文件上传 | 中危 |

## 4.1 重点污染源自动监控与基础数据库系统

### 4.1.1 用户名密码明文传输

#### 4.1.1.1 漏洞级别

| 漏洞级别 | 高危 | | 中危 | | 低危 | ■ |
|---|---|---|---|---|---|---|

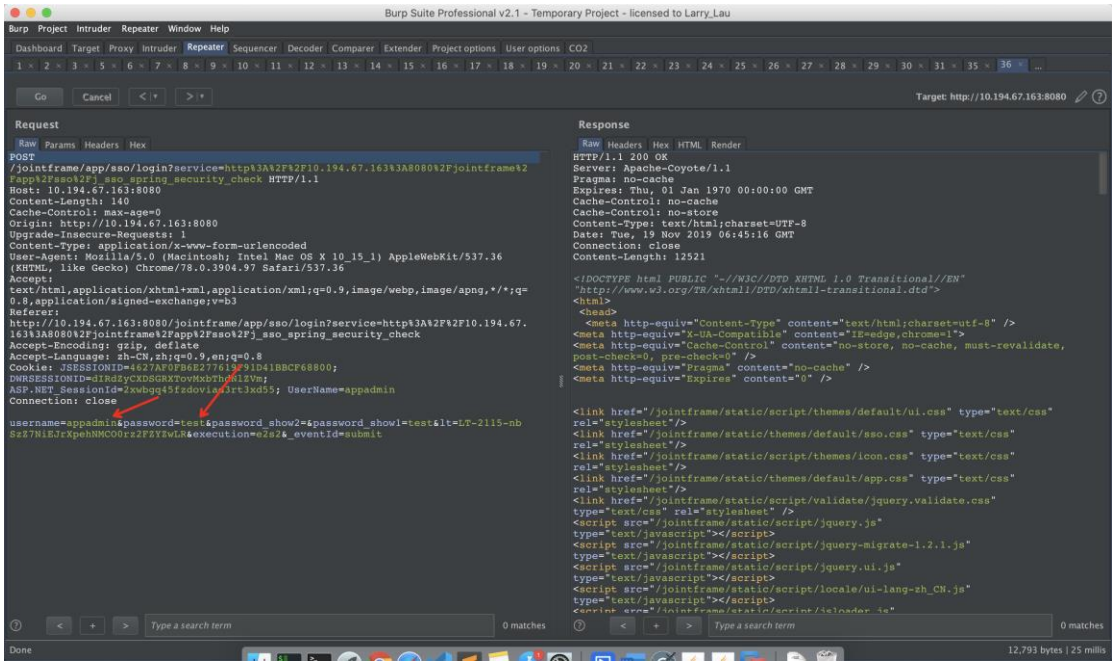
#### 4.1.1.2 漏洞危害

密码明文传输一般存在于 web 网站登录页面，用户名或者密码采用了明文传输，容易被嗅探软件截取。

#### 4.1.1.3 详细信息

在重点污染源自动监控与基础数据库系统登录界面中：


报文如下。




发现密码使用 Http 明文传输。

#### 4.1.1.4 修复建议

- 建议按照网站的密级要求，需要对密码传输过程中进行加密得使用加密的方式传输，如使用 HTTPS，但加密的方式增加成本，或许会影响用户体验。如果不用 HTTPS，可以在网站前端用 Javascript 做密码加密，

加密后再进行传输。

### 4.1.2 暴力破解

#### 4.1.2.1 漏洞级别

| 漏洞级别 | 高危 | | 中危 | ■ | 低危 | |
|---|---|---|---|---|---|---|

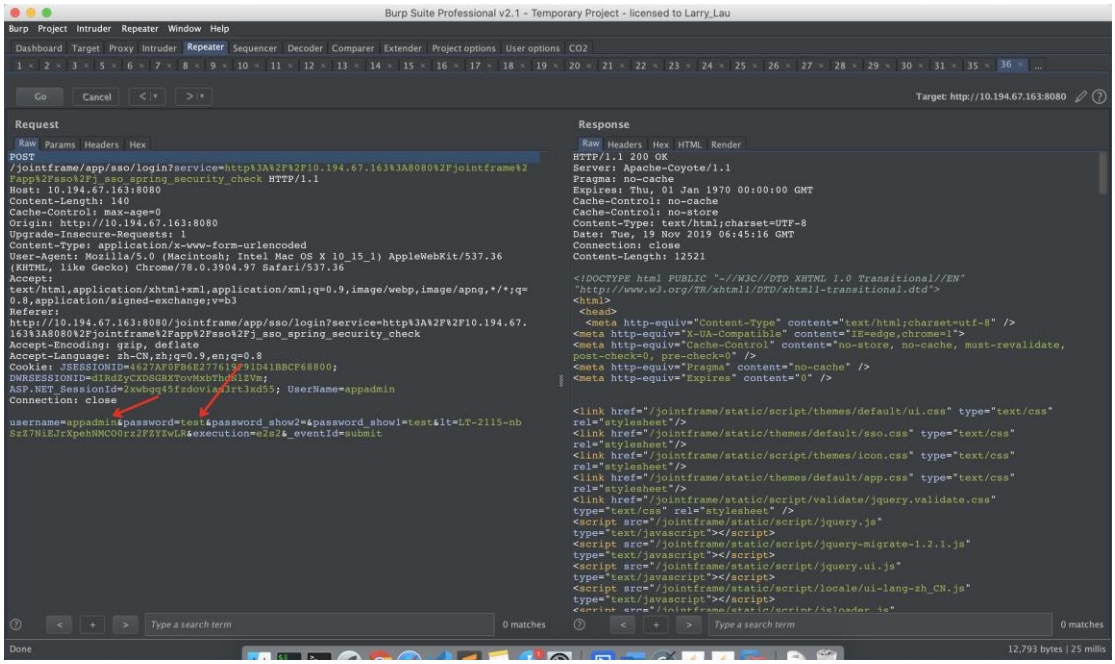
#### 4.1.2.2 漏洞危害

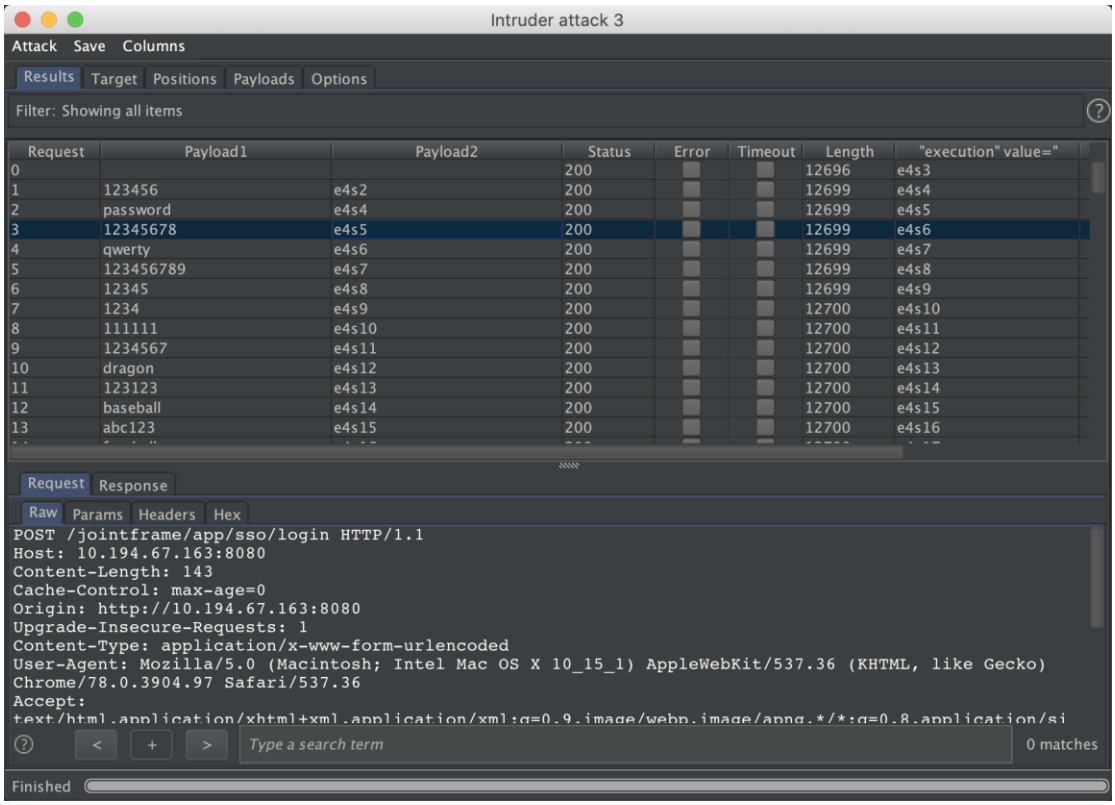
暴力破解的基本思想是根据题目的部分条件确定答案的大致范围，并在此范围内对所有可能的情况逐一验证，直到全部情况验证完毕。若某个情况验证符合题目的全部条件，则为本问题的一个解；若全部情况验证后都不符合题目的全部条件，则本题无解。常常存在于网站的登录系统中，通过对已知的管理员用户名，进行对其登录口令的大量尝试。

#### 4.1.2.3 详细信息

在重点污染源自动监控与基础数据库系统登录界面中：


报文如下。




可对密码进行爆破。

#### 4.1.2.4 修复建议

防止暴力攻击的一些方法如下：

- 账户锁定

账户锁定是很有效的方法，因为暴力破解程序在 5-6 次的探测中猜出密码的可能性很小。但是同时也拒绝了正常用户的使用。如果攻击者的探测是建立在用户名探测成功之后的行为，那么会造成严重的拒绝服务攻击。对于对大量用户名只用一个密码的探测攻击账户锁定无效。如果对已经锁定的账户并不返回任何信息，可能迷惑攻击者。

- 返回信息

  如果不管结果如何都返回成功的信息，破解软件就会停止攻击。但是对人来说很快就会被识破。

- 页面跳转

  产生登录错的的时候就跳到另一个页面要求重新登录。比如 126 和校内网都是这样做的。局限性在于不能总是跳转页面，一般只在第一次错误的时候跳转，但是第一次之后又可以继续暴力探测了。

- 适当的延时

  检查密码的时候适当的插入一些暂停，可以减缓攻击，但是可能对用户造成一定的影响。

- 封锁多次登录的 IP 地址
- 验证码。验证码是阻止暴力攻击的好方法，但设计不好的验证码是可以绕过的，而且对于特定目标的手工探测来说验证码是没有作用的。

## 4.1.3 任意文件上传漏洞

### 4.1.3.1 漏洞级别

| 漏洞级别 | 高危 | ■ | 中危 | | 低危 | |
|---|---|---|---|---|---|---|

### 4.1.3.2 漏洞危害

文件上传漏洞，直面意思可以利用 WEB 上传一些特定的文件。一般情况下文件上传漏洞是指用户上传了一个可执行的脚本文件，并通过此脚本文件获得了执行服务器端命令的能力。文件上传本身是 web 中最为常见的一种功能需求，关键

是文件上传之后服务器端的处理、解释文件的过程是否安全。一般的情况有：

1. 上传文件 WEB 脚本语言，服务器的 WEB 容器解释并执行了用户上传的脚本，导致代码执行；

2. 上传文件 FLASH 策略文件 crossdomain.xml，以此来控制 Flash 在该域下的行为；

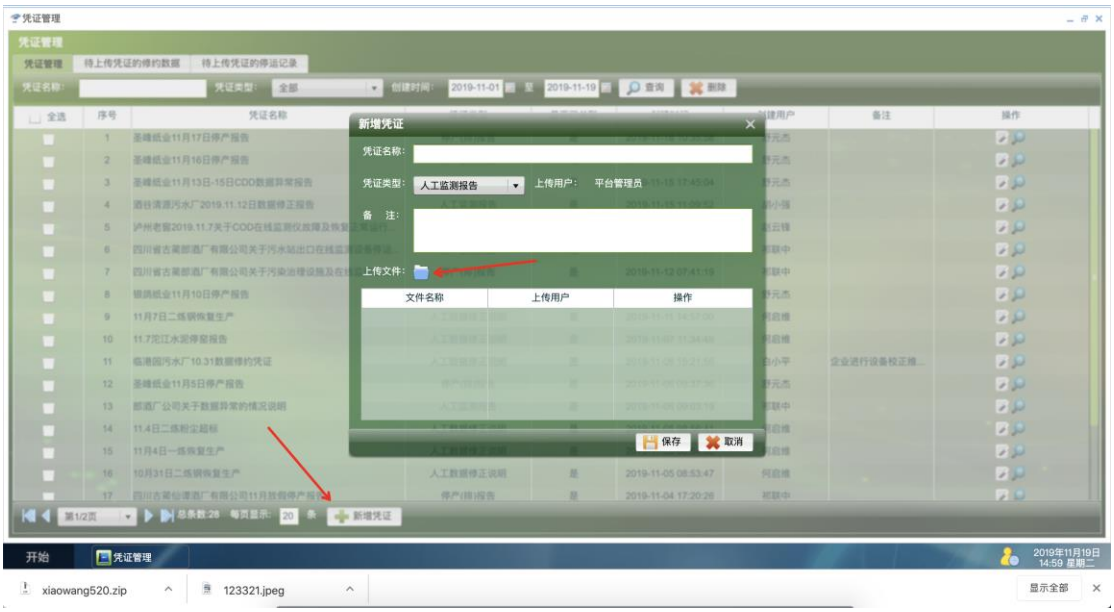
3. 上传文件是病毒、木马文件，攻击者用以诱骗用户或管理员下载执行；

4. 上传文件是钓鱼图片或为包含了脚本的图片，某些浏览器会作为脚本执行，实施钓鱼或欺诈；

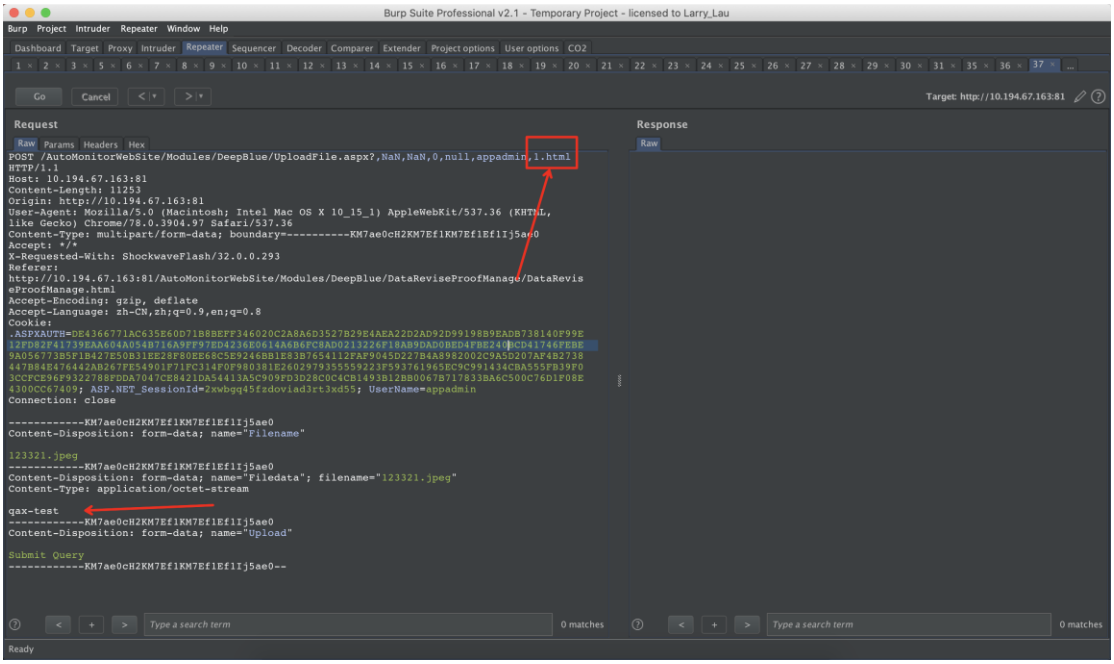
#### 4.1.3.3 详细信息

对在重点污染源自动监控与基础数据库系统测试中。

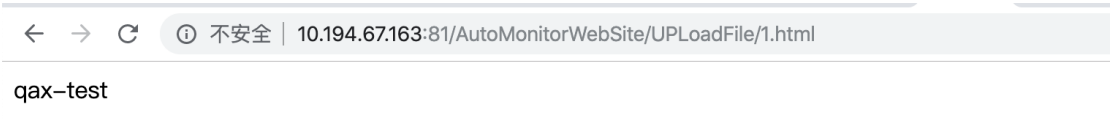
在“开始-污染源自动监控-凭证管理”模块中存在任意文件上传。




选择文件，抓取数据包,修改 get 数据中文件名未 1.html。

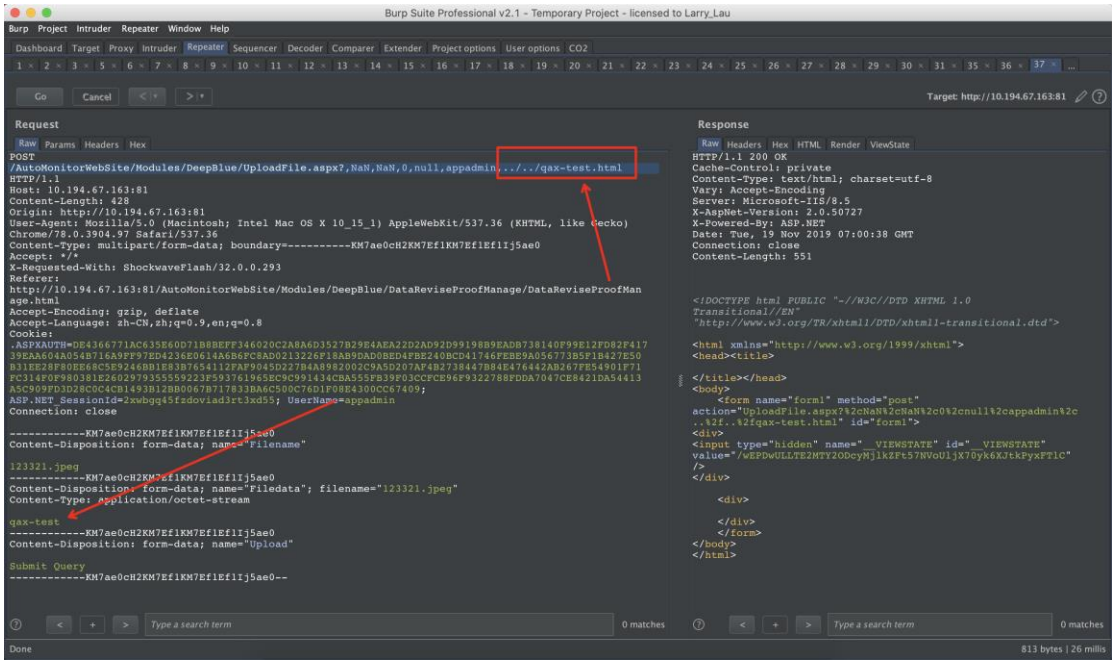



发现成功上传：

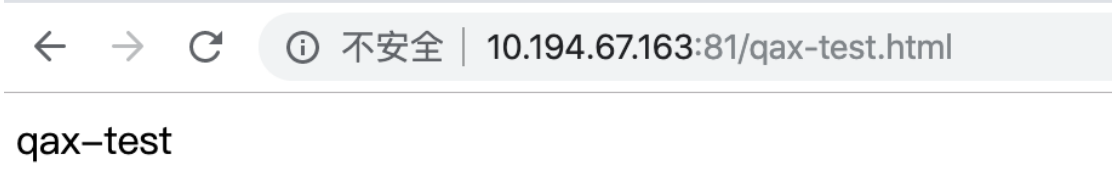



qax-test

尝试使用”../”上传至任意目录。




发现上传成功：




qax-test

此处上传可以指定任意目录和文件名，并可以覆盖任意文件。

#### 4.1.3.4 修复建议

- 建议针对文件上传漏洞的特点和必须具备的三个条件，我们阻断任何一个条件就可以达到组织文件上传攻击的目的：
- 最有效的，将文件上传目录直接设置为不可执行，对于 Linux 而言，撤销其目录的’x’权限；实际中很多大型网站的上传应用都会放置在独立的存储上作为静态文件处理，一是方便使用缓存加速降低能耗，二是杜绝了脚本执行的可能性；
- 文件类型检查：强烈推荐白名单方式，结合 MIME Type、后缀检查等方式（即只允许允许的文件类型进行上传）；此外对于图片的处理可以使用压缩函数或 resize 函数，处理图片的同时破坏其包含的 HTML 代码；
- 使用随机数改写文件名和文件路径，使得用户不能轻易访问自己上传的

文件；

- 单独设置文件服务器的域名；

### 4.1.4 未授权授权访问

#### 4.1.4.1 漏洞级别

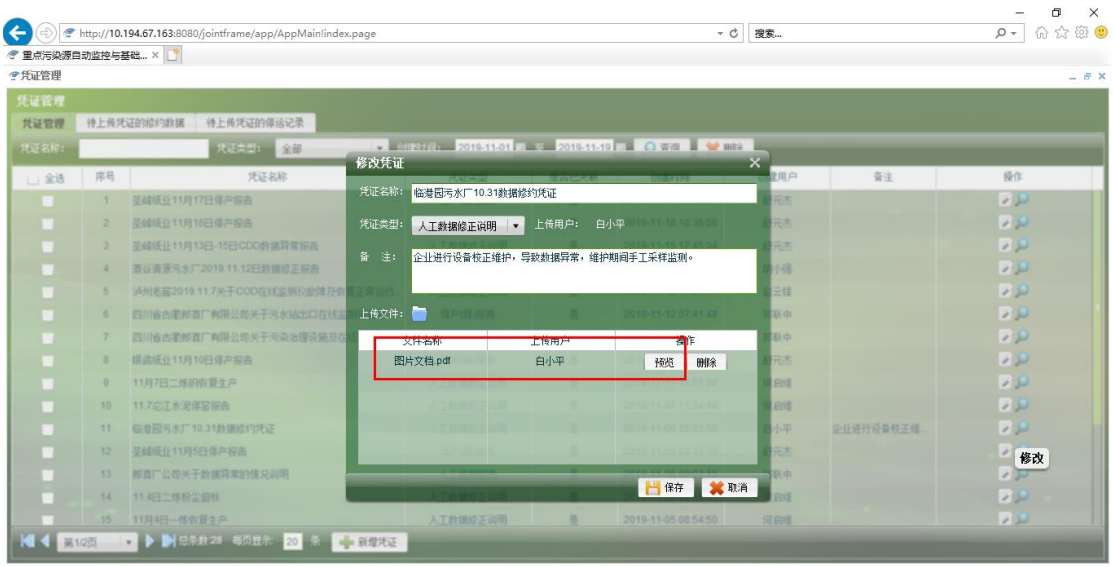
| 漏洞级别 | 高危 | ■ | 中危 | | 低危 | |
|---|---|---|---|---|---|---|

#### 4.1.4.2 漏洞危害

未授权访问漏洞，是在攻击者没有获取到登录权限或未授权的情况下，或者不需要输入密码，即可通过直接输入网站控制台主页面地址，或者不允许查看的链接便可进行访问，同时进行操作。

#### 4.1.4.3 详细信息

对重点污染源自动监控与基础数据库系统测试过程中发现，在污染源自动监控->凭证管理/监控点停运管理->凭证->预览处，存在未授权访问。

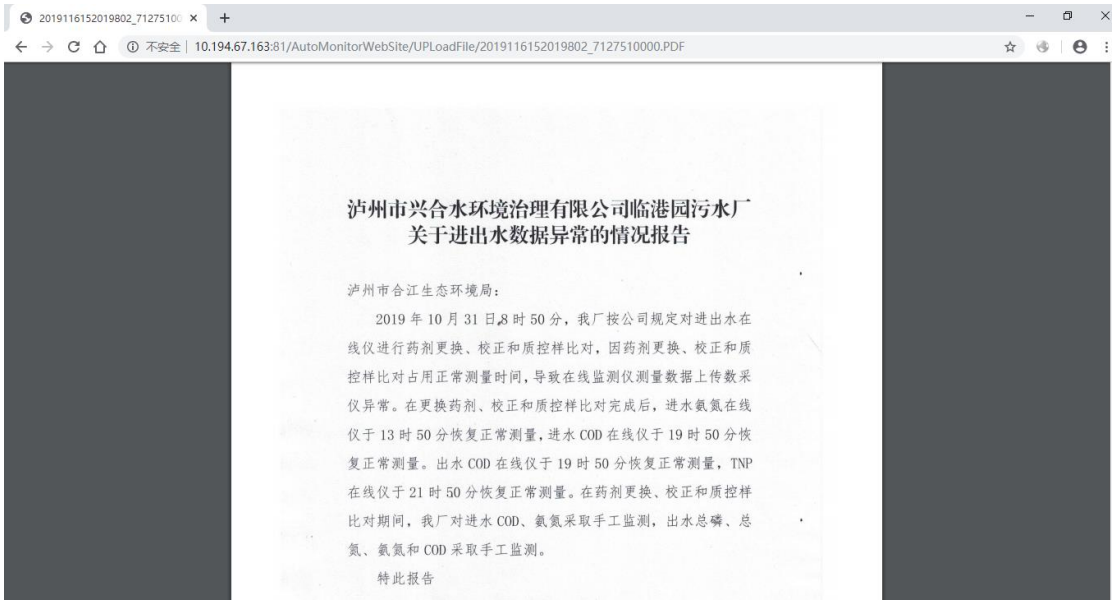



存在多处未授权访问接口

http://10.194.67.163:81/AutoMonitorWebSite/UPLoadFile/20191171137 58490_1406710000.PDF

http://10.194.67.163:81/AutoMonitorWebSite/UPLoadFile/20191161520
19802_7127510000.PDF

可未授权访问相关文件信息


## 4.1.4.4 修复建议

- 对于每个功能的访问，需要明确授予特定角色的访问权限
- 校验数据包的完整性
- 对存在未授权访问的相关信息，增加 token 和 cookie 等多重方式对身份进行验证，并且对 token 和 cookie 等进行加密处理，可有效防止越权漏

洞的产生。

# 5 安全态势说明

## 5.1 安全态势说明

**总体安全状态：**严重状态

**总体风险描述：**

通过本次对泸州市生态环境局进行渗透测试，发现泸州市生态环境局在现有的安全体系下仍然存在高安全风险。主要漏洞有：**用户名密码明传输、暴力破解、任意文件上传、未授权访问**需要运维和开发人员进行修复。泸州市生态环境局重点污染源自动监控与基础数据库系统的安全现状为严重状态。

# 附件 1

| 安全风险状况说明 | |
|---|---|
| 1 | 良好状态<br>信息系统处于良好运行状态，没有发现或只存在零星的低风险安全问题，此时只要保持现有安全策略就满足了本系统的安全等级要求。 |
| 2 | 预警状态<br>信息系统中存在一些漏洞或安全隐患，此时需根据评估中发现的网络、主机、应用和管理等方面的问题对进行有针对性的加固或改进。 |
| 3 | 严重状态<br>信息系统中发现存在严重漏洞或可能严重威胁到系统正常运行的安全问题，此时需要立刻采取措施，例如安装补丁或重新部署安全系统进行防护等等。 |
| 4 | 紧急状态<br>信息系统面临严峻的网络安全态势，对组织的重大经济利益或政治利益可能造成严重损害。此时需要与其他安全部门通力协作采取紧急防御措施。 |