**文档名称**：邯郸市生态环境局渗透测试报告

**文档属性**：受控文件

**邯郸市生态环境局在线监测**

**渗透测试报告**



**河北赛克普泰计算机咨询服务有限公司**

**二零二零年八月**

**文档信息**

|  |  |  |  |
| --- | --- | --- | --- |
| 文档名称 | 邯郸市生态环境局渗透测试报告 | | |
| 版本编号 | V 2.0 | 保密级别 | 受控 |
| 制 作 人 | 徐奇隆 | 复 审 人 | 张维峰 |
| 适用范围 | 本文档为**河北赛克普泰计算机咨询服务有限公司**(以下简称**赛克普泰**)为邯郸市生态环境局渗透测试项目制作的文档,供项目组专家和领导决策参考。 | | |
| 扩散范围 | 赛克普泰公司管理层  邯郸市生态环境局管理层 | | |

**分发控制**

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 读者 | 权限 | 与文档主要关系 |
| 1 | 赛克普泰项目组 | 创建、修改、读取 | 项目组成员负责编制、修改、审核本文档 |
| 2 | 项目经理 | 批准 | 项目经理,负责本文档的批准程序 |
| 3 | 邯郸市生态环境局项目组 | 读取、建议 | 最终用户 |

**版本历史**

|  |  |  |  |
| --- | --- | --- | --- |
| 版本编号 | 创建日期 | 制作人 | 说明 |
| V 1.0 | 2020.8.10 | 徐奇隆 | 编写渗透测试报告 |
| V1.1 | 2020.8.10 | 郭杰 | 修改渗透测试报告 |
| V2.0 | 2020.8.10 | 张维峰 | 审核渗透测试报告 |

目录

[一．摘要 3](#_Toc48916598)

[二. 项目概述 4](#_Toc48916599)

[2.1 测试流程 4](#_Toc48916600)

[2.2 风险管理及规避 4](#_Toc48916601)

[2.3 参考依据 5](#_Toc48916602)

[2.4 客户收益 5](#_Toc48916603)

[三. 测试服务说明 6](#_Toc48916604)

[3.1 测试对象与环境 6](#_Toc48916605)

[3.2 测试时间与人员 6](#_Toc48916606)

[3.3 工具及相关资源 6](#_Toc48916607)

[四、测试过程详述 9](#_Toc48916608)

[4.1 重点污染源自动监控与基础数据库系统 9](#_Toc48916609)

[1）IIS短文件名泄露 9](#_Toc48916610)

[2）敏感信息泄露 11](#_Toc48916611)

[3）目录遍历 12](#_Toc48916612)

[4）弱口令 13](#_Toc48916613)

[5）Redis未授权访问 14](#_Toc48916614)

[4.2 邯郸市环境保护局污染源自动监控系统 15](#_Toc48916615)

[1）未授权访问 15](#_Toc48916616)

[2）敏感信息明文传输 16](#_Toc48916617)

[3）用户名枚举 17](#_Toc48916618)

[4）敏感信息泄露 18](#_Toc48916619)

[附录A 安全等级评定 20](#_Toc48916620)

[附录B 风险程度分级 21](#_Toc48916621)

# 一．摘要

我司针对邯郸市生态环境局《重点污染源自动监控与基础数据库系统》、《邯郸市环境保护局污染源自动监控系统》进行了渗透测试工作,通过Web漏洞扫描器扫描及验证的同时结合本地通信抓包、数据包分析、模糊测试、重放分析等多种渗透手段对本系统进行渗透测试分析，以发现系统中的安全漏洞和风险点,并提供测试报告、提出系统整改意见。

总体安全情况为：邯郸市生态环境局《重点污染源自动监控与基础数据库系统》、《邯郸市环境保护局污染源自动监控系统》均为高危状态。

测试结果如下：

高风险漏洞：3个

中风险漏洞：8个

低风险漏洞：2个

详细安全问题汇总：

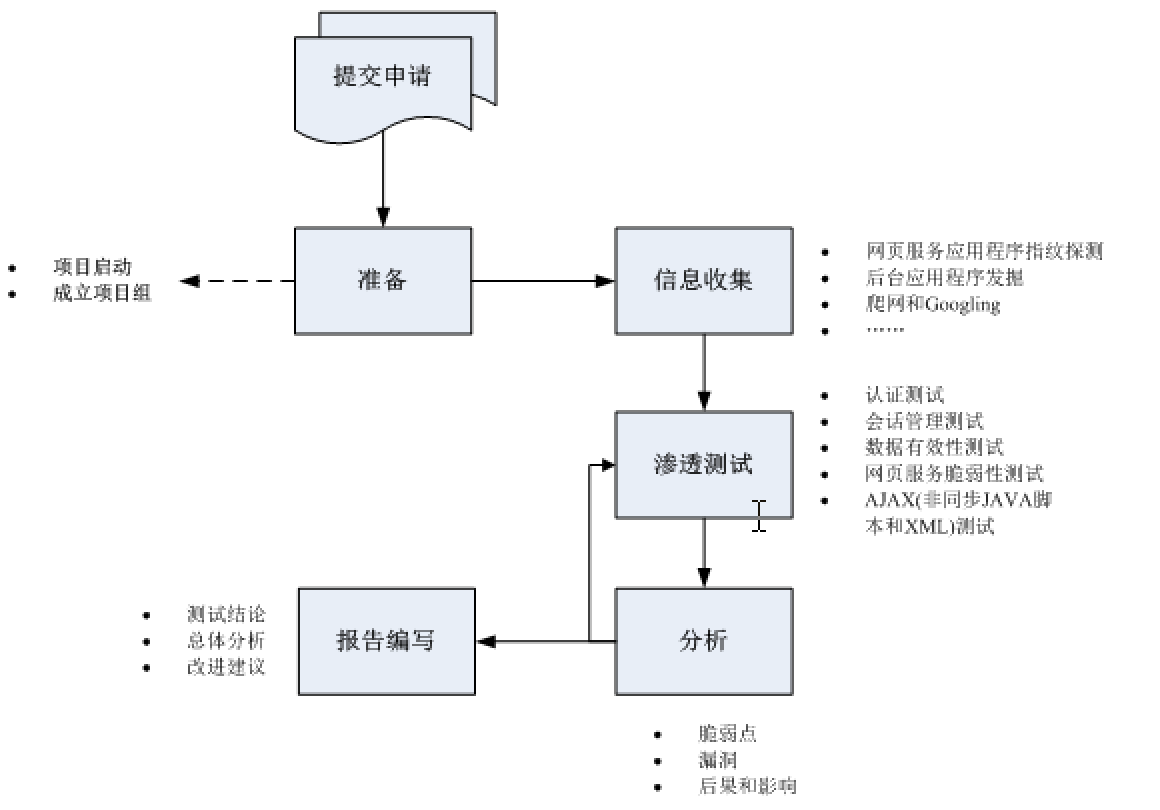
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **重点污染源自动监控与基础数据库系统漏洞名称** | **存在数量** | **风险等级** | **说明** |
| 1 | 弱口令 | 1 | 高风险 | 口令可猜解 |
| 2 | Redis未授权访问 | 1 | 高风险 | 可连接redis数据库 |
| 3 | 敏感信息泄露 | 2 | 中风险 | 页面泄露敏感信息 |
| 4 | 目录遍历 | 1 | 中风险 | 数据传输未加密 |
| 5 | IIS短文件名泄露 | 3 | 中风险 | 获取网站服务器文件名 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **邯郸市环境保护局污染源自动监控系统漏洞名称** | **存在数量** | **风险等级** | **说明** |
| 1 | 未授权访问 | 1 | 高风险 | 不需要账号密码进入后台 |
| 2 | 敏感信息泄露 | 2 | 中风险 | 配置不当 |
| 3 | 敏感信息明文传输 | 1 | 低风险 | 敏感信息传输未加密 |
| 4 | 用户名枚举 | 1 | 低风险 | 登录失败时响应不同 |

# 二. 项目概述

## 2.1 测试流程

渗透测试为五个工作阶段：



## 2.2 风险管理及规避

为保障客户系统在渗透测试中稳定、安全地运转，我们将提供以下多种方式来进行风险规避。

**对象的选择**

为更大程度地避免风险的产生，渗透测试还可选择对备份系统进行测试，因为备份系统与在线系统所安装的应用和承载的数据差异较小，而其稳定性要求又比在线系统低，因此，选择对备份系统进行测试也是规避风险的一种常见方式。

**时间的控制**

从时间安排上，测试人员将尽量避免在数据高峰时进行测试，以此来减小测试工作对被测系统带来的压力。另外，测试人员每次测试前期也将通过电话、邮件等方式告知相关人员，以防止测试过程中出现意外情况。

**技术手段**

我司的渗透测试人员都具有丰富的经验和技能，在每一步测试前期都会预估可能带来的后果，对于可能产生影响的测试（如：溢出攻击）将被记录并跳过，并随后与客户协商决定是否进行测试及测试方法。

**监控措施**

针对每一系统进行测试前，测试人员都会告知被测试系统管理员，并且在测试过程中会随时关注目标系统的负荷等信息，一旦出现异常，将会停止测试。

**工具使用**

在使用工具测试的过程中，测试人员会通过设置线程、插件数量等参数来减少对系统的压力，同时还会去除任何可能对目标系统带来危害的插件，如：远程攻击溢出类插件、拒绝服务攻击类插件等等。

## 2.3 参考依据

渗透测试参考的标准包括但不限于：

* 国际OWASP组织发布的最新版OWASP TOP10
* 《信息安全技术 web应用安全扫描产品安全技术要求》
* 《信息安全技术 web应用防火墙产品安全技术要求》

## 2.4 客户收益

通过进行渗透测试，可对贵方的信息化系统起到如下推进作用：

**明确安全隐患**

渗透测试是一个从空间到面再到点的过程，测试人员模拟黑客的入侵，从外部整体切入，最终落至某个威胁点并加以利用，最终对整个网络产生威胁，以此明确整体系统中的安全隐患点。

**提高安全意识**

如上所述，任何的隐患在渗透测试服务中都可能造成“千里之堤溃于蚁穴”的效果，因此渗透测试服务可有效督促管理人员杜绝任何一处小的缺陷，从而降低整体风险。

**提高安全技能**

在测试人员与用户的交互过程中，可提升用户的技能。另外，通过专业的渗透测试报告，也能为用户提供当前流行安全问题的参考。

# 三. 测试服务说明

## 3.1 测试对象与环境

|  |  |  |
| --- | --- | --- |
| **序号** | **系统名称** | **地址** |
| 1 | 重点污染源自动监控与基础数据库系统 | http://10.122.65.67:9031/monitor-web/index.html |
| 2 | 污染源在线数据智能分析系统 | http://10.122.65.103:8080/jointframe/app/AppMain!index.page |

## 3.2 测试时间与人员

|  |  |
| --- | --- |
| **测试时间** | 2020-08-05 ~ 2020-08-10 |
| **测试负责人员** | 郭杰、徐奇隆 |

## 3.3 工具及相关资源

测试人员模拟黑客入侵常用工具对目标进行渗透测试。例如，操作系统自带网络应用、管理和诊断工具、免费安全扫描器、远程入侵代码和本地提升权限代码等。

这些工具经过全球数以万计的程序员、网络管理员、安全专家以及黑客的测试和实际应用，在技术上已经非常成熟，实现了网络检查和安全测试的高度可控性，能够根据使用者的实际要求进行有针对性的测试。

主要对系统和应用的错误配置进行检查和信息收集，加快了进行系统脆弱性检查的速度和准确度，并避免了大量手工操作可能带来的操作失误或者遗漏。

以下列出了渗透测试中常用的网络扫描、网络管理等工具，这些工具都是网络上的免费软件。测试人员将可能利用到，但不限于以下工具。由于种类繁杂，在这里不会一一列出。

* 1. **信息探测与收集**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **工具名称** | **说明** | **备注** |
| 1 | Whois | 用来查询域名的IP以及所有者等信息的传输协议 | http://ewhois.cnnic.net.cn/  http://www.whois-search.com/  http://whois.webhosting.info/  http://whois.chinaz.com/ |
| 2 | nslookup | 用于查询DNS信息 | 系统自带 |
| 3 | Netcat | 提供交互式手工测试的网络工具 | http://joncraton.org/files/nc111nt.zip |
| 4 | Nmap | 提供对系统进行指纹的功能 | http://nmap.org/ |
| 5 | Httprecon | 针对HTTP服务器进行指纹探测的工具 | http://www.computec.ch/projekte/httprecon/ |

* 1. **扫描与检测**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **工具名称** | **说明** | **备注** |
| 1 | 绿盟 | 强大的安全漏洞扫描工具 | https://www.nsfocus.com.cn/ |
| 2 | Nikto | 针对HTTP服务器的开源扫描工具 | http://cirt.net/nikto2 |
| 3 | 绿盟 | 针对web程序的开源扫描工具 | https://www.nsfocus.com.cn/ |
| 4 | 安华金和数据库漏扫系统 | 数据库系统专业漏洞扫描工具 | https://www.nsfocus.com.cn/ |

* 1. **漏洞利用**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **工具名称** | **说明** | **备注** |
| 1 | Metasploit | 综合漏洞利用平台 | http://www.metasploit.com/ |
| 2 | Exploit-db | 常见可用漏洞的发布平台 | http://www.exploit-db.com/ |
| 3 | Hydra | 多功能口令破解工具 | http://freeworld.thc.org/thc-hydra/ |
| 4 | Smbcrack | SMB口令破解工具 | N/A |
| 5 | SQLMap | SQL注入利用工具 | http://sqlmap.sourceforge.net/ |

* 1. **手工测试**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **工具名称** | **说明** | **备注** |
| 1 | BurpSuite | 综合检测工具，用于分析、修改提交的HTTP数据包内容。 | https://portswigger.net/burp/ |
| 2 | Fiddler | 用于修改提交的HTTP数据包内容的工具 | http://www.fiddler2.com/fiddler2/ |
| 3 | Perl | Perl程序运行环境，用于测试人员定制编写测试代码 | http://www.perl.org/ |
| 4 | Python | Python程序运行环境，用于测试人员定制编写测试代码 | http://python.org/ |

# 四、测试过程详述

## 4.1 重点污染源自动监控与基础数据库系统

### 1）IIS短文件名泄露

**【风险等级】**中风险

**【漏洞地址】**

http://10.122.65.103:800/

<http://10.122.65.103:809/>

http://10.122.65.103:81/

**【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，攻击者可利用此漏洞枚举网络服务器根目录中的文件。危害：攻击者可以利用“~”字符猜解或遍历服务器1中的文件名，或对IIS服务器中的.Net Framework进行拒绝服务攻击。

攻击者可通过该漏洞尝试获取网站服务器文件的文件名，达到获取更多信息来入侵服务器的目的。

**【修复建议】**

修改Windows配置，关闭短文件名功能。

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。

**【漏洞验证】**

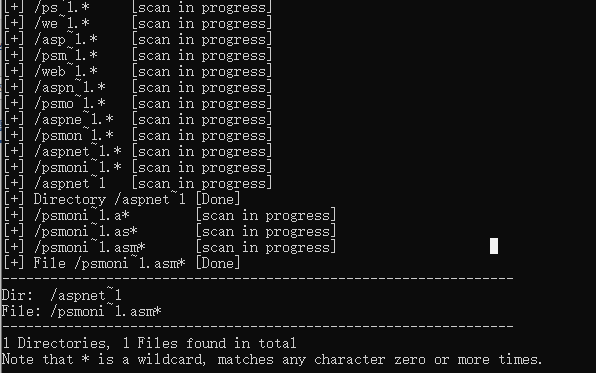


图4.1.1-1

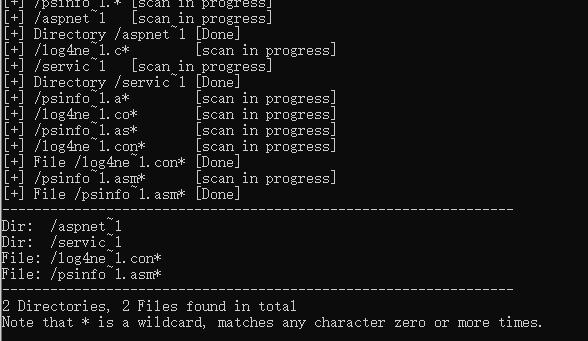


图4.1.1-2

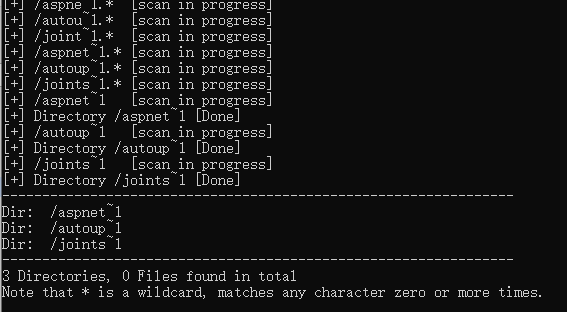


图4.1.1-3

### 2）敏感信息泄露

**【风险等级】**中风险

**【漏洞地址】**

<http://10.122.65.103:8080/jointframe/app/sso/login?service=http%3A%2F%2F10.122.65.103%3A8080%2Fjointframe%2Fapp%2Fsso%2Fj_sso_spring_security_check>

http://10.122.65.103:7080/jointframe/app

**【漏洞描述】**

在页面中或者返回的响应包中泄露了敏感信息，给攻击者渗透提供了非常多的有用信息。

**【修复建议】**

1、如果是探针或测试页面等无用的程序建议删除，或者修改成难以猜解的名字。

　　2、不影响业务或功能的情况下删除或禁止访问泄露敏感信息页面。

　　3、在服务器端对相关敏感信息进行模糊化处理。

　　4、对服务器端返回的数据进行严格的检查，满足查询数据与页面显示数据一致。

**【漏洞验证】**

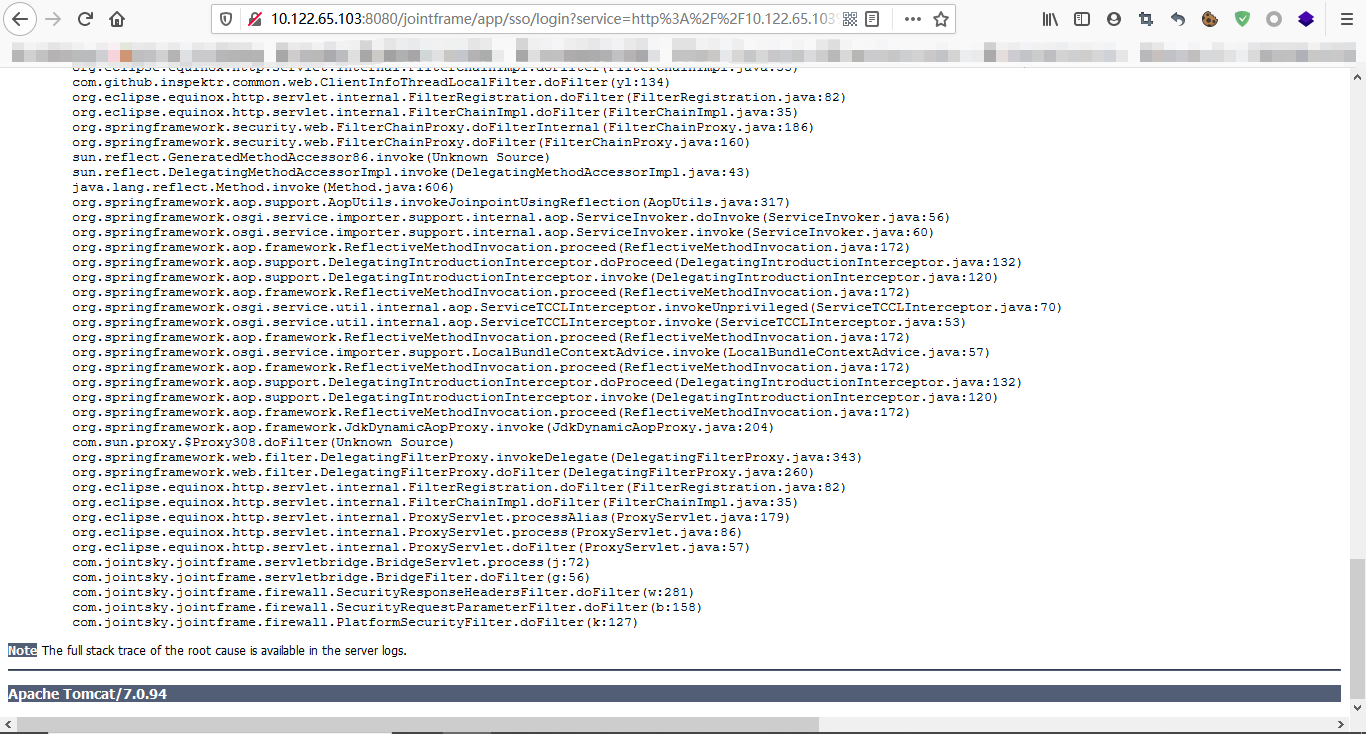


图4.1.2-1

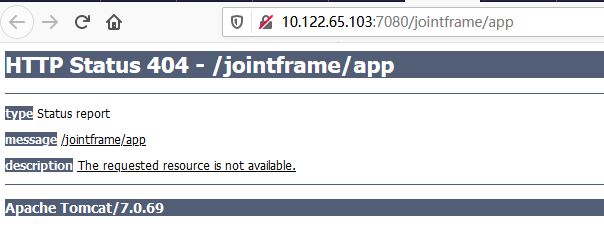


图4.1.2-2

### 3）目录遍历

**【风险等级】**中风险

**【漏洞地址】**

http://10.122.65.103:800/

**【漏洞描述】**

网站存在目录遍历漏洞，泄露网站源码信息。通过利用目录遍历漏洞，攻击者得到根目录和访问文件所在其他目录。

**【修复建议】**

配置中间件关闭目录遍历。

**【漏洞验证】**

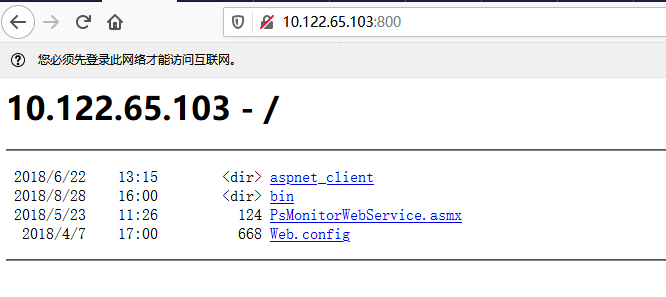


图4.1.3-1

### 4）弱口令

**【风险等级】**高风险

**【漏洞地址】**

http://10.122.65.103:8161/admin/

**【漏洞描述】**

由于网站用户帐号存在弱口令，导致攻击者通过弱口令可轻松登录到网站中，从而进行下一步的攻击，如上传webshell，获取敏感数据。

另外攻击者利用弱口令登录网站管理后台，可执行任意管理员的操作。

**【修复建议】**

1、强制用户首次登录时修改默认口令，或是使用用户自定义初始密码的策略；

2、完善密码策略，信息安全最佳实践的密码策略为8位（包括）以上字符，包含数字、大小写字母、特殊字符中的至少3种；

3、增加人机验证机制，限制ip访问次数。

**【漏洞验证】**

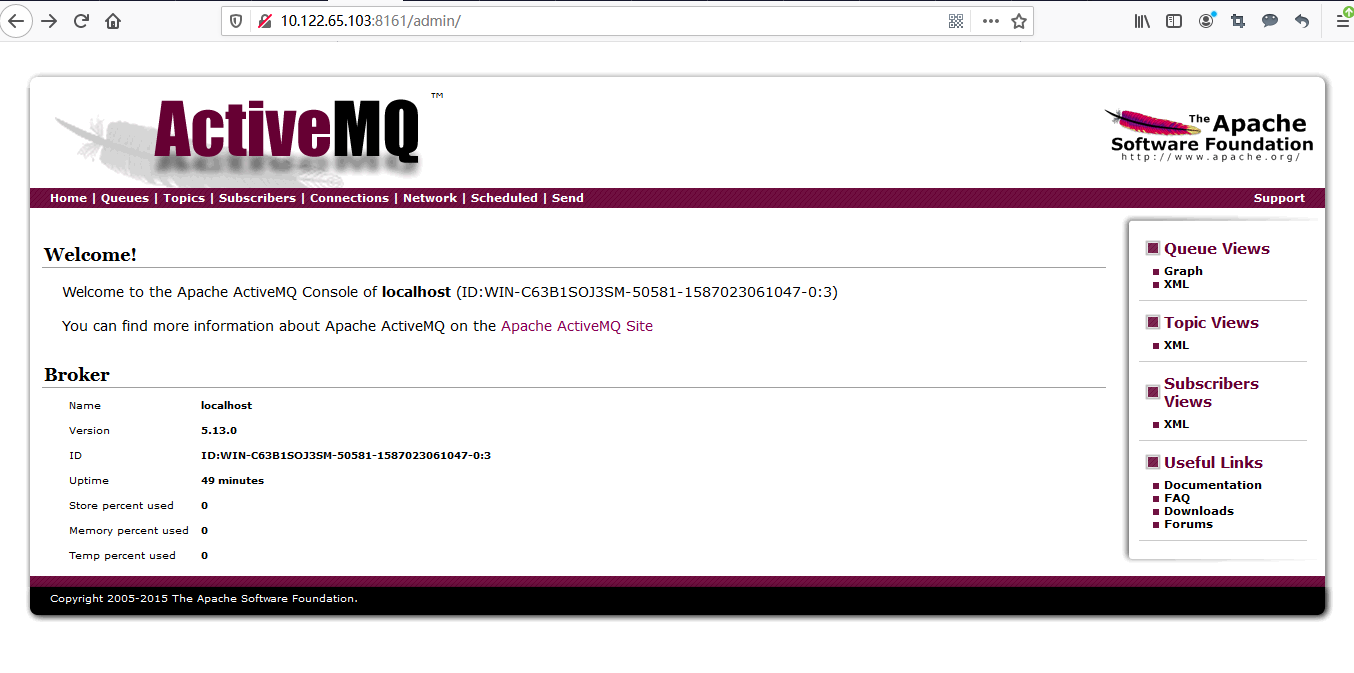


图4.1.4-1（admin/admin）

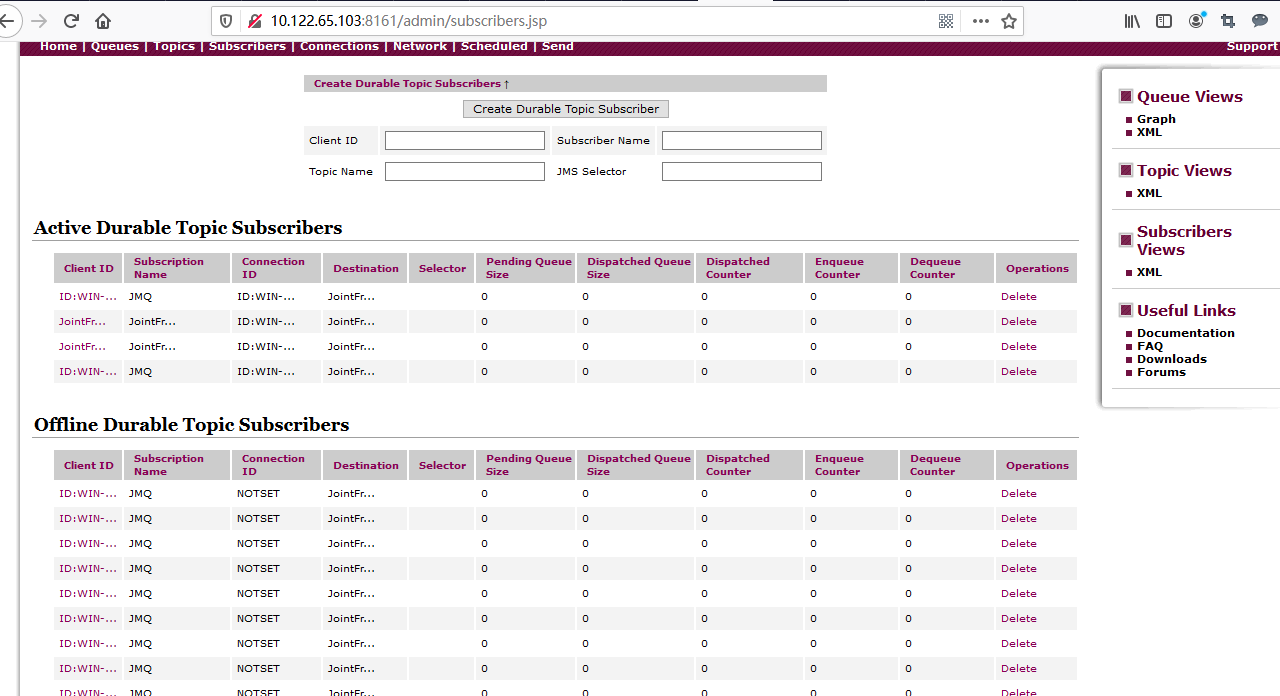


图4.1.4-2

### 5）Redis未授权访问

**【风险等级】**高风险

**【漏洞地址】**

10.122.65.102:6379

**【漏洞描述】**

Redis 默认情况下，会绑定在 0.0.0.0:6379，，如果没有进行采用相关的策略，比如添加防火墙规则避免其他非信任来源 ip 访问等，这样将会将 Redis 服务暴露到公网上，如果在没有设置密码认证（一般为空）的情况下，会导致任意用户在可以访问目标服务器的情况下未授权访问 Redis 以及读取 Redis 的数据。攻击者在未授权访问 Redis 的情况下，利用 Redis 自身的提供的config 命令，可以进行写文件操作，攻击者可以成功将自己的ssh公钥写入目标服务器的 /root/.ssh 文件夹的authotrized\_keys 文件中，进而可以使用对应私钥直接使用ssh服务登录目标服务器。

**【修复建议】**

1、禁止一些高危命令（重启redis才能生效）；

2、以低权限运行 Redis 服务（重启redis才能生效）；

3、为Redis 添加密码验证（重启redis才能生效）；

4、禁止外网访问 Redis（重启redis才能生效）；

5、修改默认端口；

6、保证 authorized\_keys 文件的安全；

7、设置防火墙策略；

**【漏洞验证】**

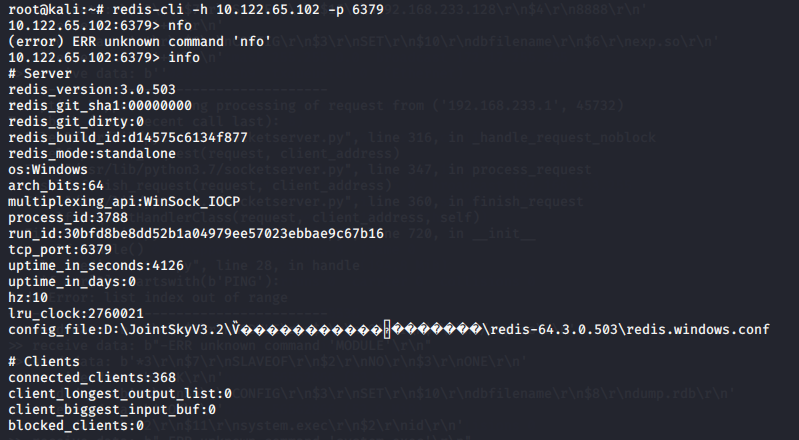


图4.1.5-1

## 4.2 邯郸市环境保护局污染源自动监控系统

### 1）未授权访问

**【风险等级】**高风险

**【漏洞地址】**

http://10.122.65.67:9031/monitor-web/pages/admin/admin.html

**【漏洞描述】**

因配置不当系统存在未授权访问漏洞，攻击者无需认证就可以访问到内部数据，其漏洞可导致敏感信息泄露，并可操控系统后台。

**【修复建议】**

合理验证访问权限。

**【漏洞验证】**



图4.2.1-1

### 2）敏感信息明文传输

**【风险等级】**低风险

**【漏洞地址】**

http://10.122.65.67:9031/monitor-web/index.html

**【漏洞描述】**

用户登录过程中使用明文传输用户登录信息，若用户遭受中间人攻击时，攻击者可直接获取该用户登录账户，从而进行进一步渗透。

**【修复建议】**

1、用户登录信息使用加密传输，如密码在传输前使用安全的算法加密后传输，可采用的算法包括：不可逆hash算法加盐（4位及以上随机数，由服务器端产生）；安全对称加密算法，如AES(128、192、256位)，且必须保证客户端密钥安全，不可被破解或读出；非对称加密算法，如RSA(不低于1024位)、SM2等。

　　2、使用https来保证传输的安全。

**【漏洞验证】**

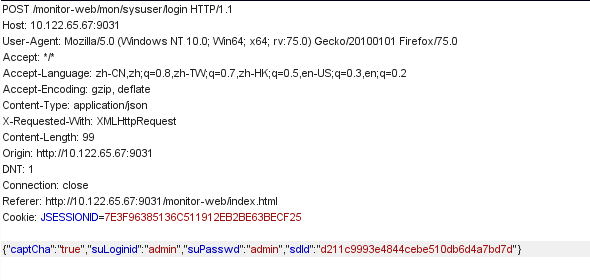


图4.2.2-1

### 3）用户名枚举

**【风险等级】**低风险

**【漏洞地址】**

http://10.122.65.67:9031/monitor-web/index.html

**【漏洞描述】**

由于错误配置或设计缺陷，当向系统提交有效账户和无效账户时，服务器会有不同的响应。利用响应的不同，攻击者可以获取到系统已经存在的账户，可用于暴力破解，进一步获取账户的登录密码。

**【修复建议】**

统一身份验证失败时的响应，如：用户名或密码错误。

**【漏洞验证】**

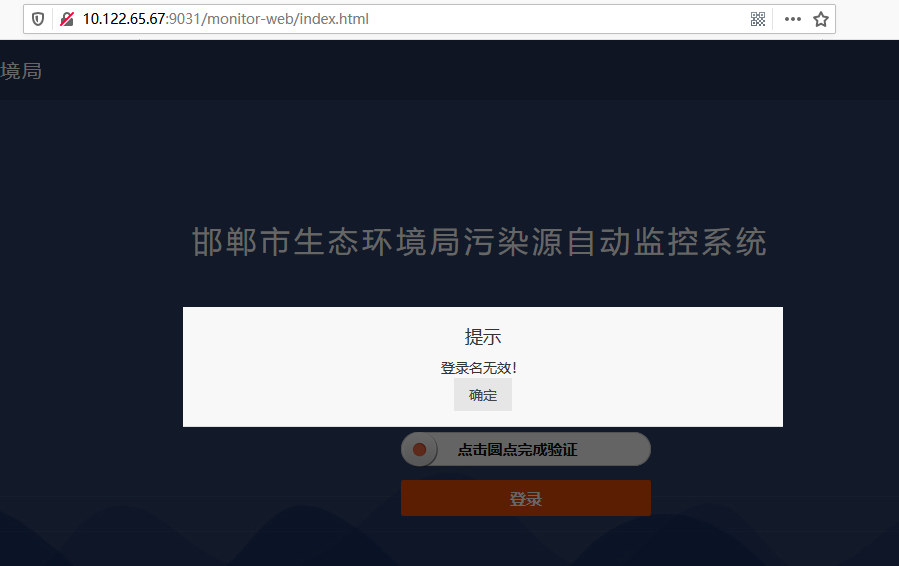


图4.2.3-1



图4.2.3-2

### 4）敏感信息泄露

**【风险等级】**中风险

**【漏洞地址】**

<http://10.122.65.67:9031/monitor-web/public/css/config.rb>

http://10.122.65.67:9031/monitor-web/services

**【漏洞描述】**

在页面中或者返回的响应包中泄露了敏感信息，通过这些信息，给攻击者渗透提供了非常多的有用信息。网站错误日志可下载，泄露网站敏感信息。

**【修复建议】**

1、如果是探针或测试页面等无用的程序建议删除，或者修改成难以猜解的名字。

　　2、不影响业务或功能的情况下删除或禁止访问泄露敏感信息页面。

　　3、在服务器端对相关敏感信息进行模糊化处理。

　　4、对服务器端返回的数据进行严格的检查，满足查询数据与页面显示数据一致。

5、禁止访问此文件。

**【漏洞验证】**

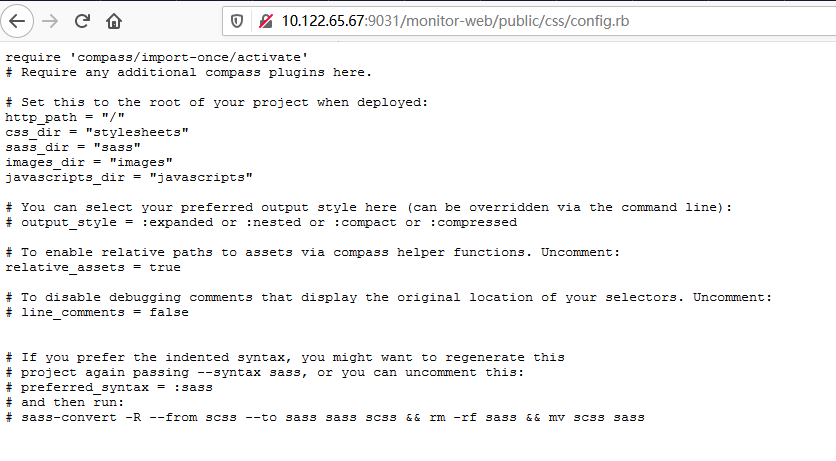


图4.2.4-1

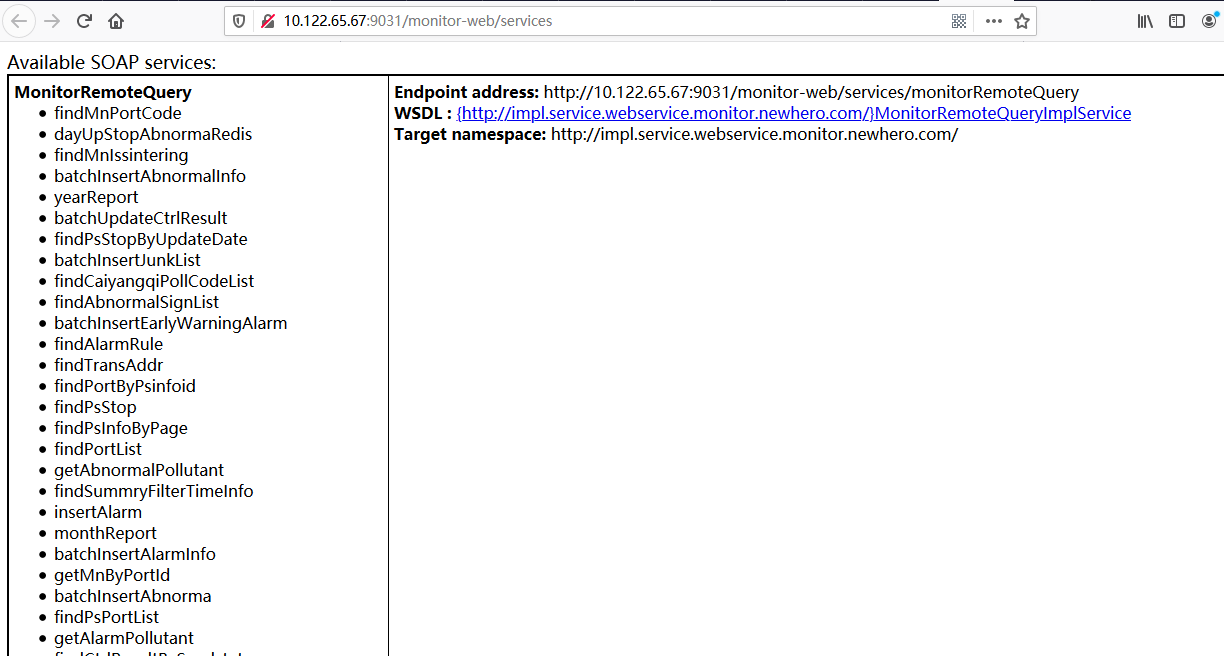


图4.2.4-2

# 附录A 安全等级评定

|  |  |
| --- | --- |
| **安全等级** | **资源内容描述** |
| 远程不安全系统  （符合任何一个条件） | 1、存在一个或一个以上严重的安全问题，可直接导致系统受到破坏；  2、与其他非安全系统连接，同时存在相互信任关系（或账号互通）的主机；  3、发现已经被人入侵且留下远程后门的主机；  4、存在3个以上中等安全问题的主机；  5、与其他非安全系统在一个共享网络中，同事远程维护明文传输口令；  6、完全不能抵抗小规模的拒绝服务攻击。 |
| 远程一般安全系统  （符合任何一个条件） | 1、存在一个或一个以上中等安全问题的主机；  2、开放过多服务，同时可能被利用来进行拒绝服务的主机；  3、与其他非安全系统直接连接，但暂时不存在直接信任（或账号互通）关系；  4、远程维护通过明文的方式传递信息；  5、存在3个以上轻度安全问题的主机；  6、只能抵抗最低级的拒绝服务攻击。 |
| 远程安全系统  （符合全部条件） | 1、最多存在1-2个轻度安全问题；  2、远程维护方式安全；  3、与不安全或一般安全系统相互对立；  4、能抵挡一定规模的拒绝服务攻击。 |

# 附录B 风险程度分级

|  |  |
| --- | --- |
| **风险等级** | **风险描述** |
| 高 | 该脆弱点若被利用，可非授权直接获得主机或设备的远程管理权限；  该脆弱点若被利用，可非授权间接获得主机或设备的本地管理用户权限；  该脆弱点若被利用，可非授权直接获得多台主机或设备的远程管理用户权限。  该脆弱点若被利用、可非授权获取其他用户信息或其他用户权限。 |
| 中 | 该脆弱点若被利用，可非授权直接获得主机或设备的远程普通用户权限；  该脆弱点若被利用，可获得主机或设备的关键信息；  该脆弱点若被利用，可造成主机或设备的服务崩溃（拒绝服务）。 |
| 低 | 该脆弱点若被利用，可获得单个主机或设备的一般信息。 |