石家庄市水生态环境系统渗透测试报告

[CNDJBH-PT-LYK-20221123-01]



**河北华测信息技术有限公司**

**2022-11**

|  |  |
| --- | --- |
| 密级 | 商密 |

文档信息

|  |  |
| --- | --- |
| 修订时间 | 20221123 |
| 文档名称 | 石家庄市水生态环境系统渗透测试报告 |
| 文档编号 | CNDJBH-PT-LYK-20221123-01 |
| 保密级别  | 商密 |
| 扩散范围 | 公司内部，石家庄市电子政务中心 |

文档说明

此文档作为河北华测信息技术有限公司的正式文档编写规范，用于公司对外发布的各种系统说明书、系统白皮书、技术手册等文档。

版权声明

本文件中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属河北华测信息技术有限公司所有，受到有关产权及版权法保护。任何个人、机构未经河北华测信息技术有限公司的书面授权许可，不得以任何方式复制或引用本文件的任何片断。

目录

[1. 摘要 4](#_Toc120090550)

[2. 项目概述 5](#_Toc120090551)

[2.1. 渗透测试目的 5](#_Toc120090552)

[2.2. 渗透测试范围 5](#_Toc120090553)

[2.3. 渗透测试依据 6](#_Toc120090554)

[2.4. 渗透测试工具 6](#_Toc120090555)

[3. 渗透测试详情 6](#_Toc120090556)

[3.1. 高危漏洞 6](#_Toc120090557)

[3.1.1. 垂直越权访问 6](#_Toc120090558)

[4. 安全风险总结 8](#_Toc120090559)

[5. 附录 8](#_Toc120090560)

1. 摘要

2022年11月19日，受石家庄市电子政务中心委托，河北华测信息技术有限公司对石家庄市水生态环境系统进行了网站安全渗透测试。

在渗透测试过程中发现石家庄市水生态环境系统存在1种安全漏洞。现对渗透测试结果进行说明，并提出漏洞修复建议。

|  |  |  |
| --- | --- | --- |
| **威胁级别** | **漏洞名称** | **数量** |
| **高危漏洞** | 垂直越权访问 | 1 |

|  |  |  |
| --- | --- | --- |
| **测试分类** | **测试项** | **测试结果** |
| **WEB安全** | SQL注入 | **通过** |
| 跨站脚本攻击（XSS） | **通过** |
| XML外部实体（XXE）注入 | **通过** |
| 跨站点伪造请求（CSRF） | **通过** |
| 服务器端请求伪造（SSRF） | **通过** |
| 任意文件上传 | **通过** |
| 任意文件下载或读取 | **通过** |
| 任意目录遍历 | **通过** |
| .svn/.git源代码泄露 | **通过** |
| 敏感信息泄露 | **通过** |
| CRLF注入 | **通过** |
| 命令执行注入 | **通过** |
| URL重定向 | **通过** |
| Json劫持 | **通过** |
| 第三方组件安全 | **通过** |
| 本地/远程文件包含 | **通过** |
| 任意代码执行 | **通过** |
| Struts2远程命令执行 | **通过** |
| Spring远程命令执行 | **通过** |
| 反序列化命令执行 | **通过** |
| **业务逻辑安全** | 用户名枚举 | **通过** |
| 用户密码枚举 | **通过** |
| 明文密码传输 | **通过** |
| 用户密码重置 | **通过** |
| 用户弱口令 | **通过** |
| 会话标志固定攻击 | **通过** |
| 平行越权访问 | **通过** |
| 垂直越权访问 | **存在** |
| 未授权访问 | **通过** |
| 验证码缺陷 | **通过** |
| 登录短信验证码泄漏 | **通过** |
| **中间件安全** | 中间件配置缺陷 | **通过** |
| 中间件弱口令 | **通过** |
| Webloigc反序列化命令执行 | **通过** |
| Jboss反序列化命令执行 | **通过** |
| Websphere反序列化命令执行 | **通过** |
| Jenkins反序列命令执行 | **通过** |
| JBoss远程代码执行 | **通过** |
| 文件解析代码执行 | **通过** |
| **服务器安全** | 域传送漏洞 | **通过** |
| Redis未授权访问 | **通过** |
| MangoDB未授权访问 | **通过** |
| 操作系统弱口令 | **通过** |
| 数据库弱口令 | **通过** |
| 本地权限提升 | **通过** |
| 已存在的脚本木马 | **通过** |
| 应用防护软硬件缺陷 | **通过** |

1. 项目概述
	1. 渗透测试目的

通过本项目的成功实施，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，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。

● 发现授权渗透测试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

* 1. 渗透测试范围

本次授权渗透测试范围如下：

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **备注** |
| 1 | 石家庄市水生态环境系统 | http://124.239.186.82:38008/ShiJiaZhuangSHJ/index.html |

* 1. 渗透测试依据

● 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

* 1. 渗透测试工具

● 自动化扫描：为保障业务正常运行，通过人工进行扫描

● 自动化扫描：Nessus等

● 端口扫描、服务检测：Nmap等

● 网络数据分析：Wireshark等

● 漏洞分析利用：Metasploit、SQLMAP等

1. 渗透测试详情
	1. 高危漏洞
		1. 垂直越权访问

**漏洞概述：**

用系统在处理各个角色业务功能时，并未对当前用户角色与该业务功能的权限标志进行判断，导致用户可越权访问非自身权限范围内的业务功能，造成越权操作。常见如：越权添加、修改、删除用户以及权限、越权访问系统管理功能等。

**测试方法：**

1. 登录高权限用户；
2. 记录高权限菜单的URL地址；
3. 切换登录，登录低权限用户；
4. 低权限用户直接访问高权限菜单URL，查看是否可成功访问。

**测试结果与过程：**

当前用户无添加用户权限，权限如下图：



通过查看接口找到添加用户接口，构造参数，成功添加用户





**修复建议：**

合理验证用户权限。

1. 安全风险总结

石家庄市水生态环境系统运行在当前网络体系下发现存在可利用的安全风险漏洞。因此，我们认为石家庄市水生态环境系统当前的总体安全状态为**预警状态**。

1. 附录

|  |
| --- |
| **安全风险状况等级说明** |
| **良好状态** | 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。 |
| **预警状态** | 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。 |
| **严重状态** | 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。 |
| **紧急状态** | 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。 |

|  |
| --- |
| **漏洞等级状况说明** |
| **低危漏洞** | 对系统造成较小的影响，攻击难度高，攻击场景较为苛刻，不会直接影响到系统的正常运行，攻击者可能无法通过该漏洞获得权限。 |
| **中危漏洞** | 对系统造成一般的影响，攻击难度一般，在特定场景下将可影响系统的正常运行，攻击者需要配合其他安全漏洞方可间接获得权限。 |
| **高危漏洞** | 对系统造成严重的影响，攻击难度低，一般情况下可直接利用而无需特定场景和要求，攻击者可直接利用该漏洞获得权限。 |