

受控： C级

文档编号：CSCEC8B-PT-#DATA#-01

#SYSTEM#系统

渗透测试报告

中国建筑第八工程局有限公司

#DATA#

修订记录

| **日期** | **修订版本** | **修改描述** | **作者** |
| --- | --- | --- | --- |
| #DATA# | V1.0 | 初稿编写 |  |
| #DATA# | V1.1 | 文档审核 |  |

**目 录**

[一、 任务概述 4](#_Toc8503)

[二、 测试范围 4](#_Toc5559)

[三、 测试准备 4](#_Toc2180)

[3.1 人员安排 4](#_Toc3750)

[3.2 测试时间 5](#_Toc12885)

[3.3 测试账号 5](#_Toc28661)

[3.4 测试工具 5](#_Toc7227)

[四、 结果汇总 6](#_Toc2664)

[4.1 漏洞统计 6](#_Toc16279)

[4.2 数量分布 6](#_Toc22235)

[4.3 风险分析 6](#_Toc2760)

[五、 漏洞详细描述及加固建议 7](#_Toc26434)

[5.1 #SYSTEM#系统 7](#_Toc30916)

[5.1.1 【#POCRISK#】#POCNAME# 7](#_Toc24670)

[5.1.2 【#POCRISK#】#POCNAME# 7](#_Toc25180)

[5.1.3 【#POCRISK#】#POCNAME# 7](#_Toc19055)

# 任务概述

渗透测试是模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统的安全作深入的探测，发现系统最脆弱的环节，能够让管理人员直观了解信息系统漏洞被利用过程，并导致的后果。

本次安全测试已获得相关授权，渗透测试团队利用各种主流的攻击技术对目标系统做模拟攻击测试，以发现系统中的安全漏洞和风险点，并提出系统安全加固意见。本报告仅用于内部参考，最终结果以第三方专业机构渗透测试报告为准。

# 测试范围

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **访问域名/IP地址** | **信息系统名称** | **测试日期范围** |
| 1 | #IP# | #SYSTEM# | #DATARANGE# |

# 测试准备

## 人员安排

测试对接人员：#DJNAME#

渗透测试人员：#CSNAME#

实施具体分工如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **职责分工** | **人员姓名** | **联系方式** |
|  | 测试对接 | #DJNAME# | #DJPHONE# |
|  | 渗透测试 | #CSNAME# | #CSPHONE# |

## 

## 测试时间

测试日期范围：#DATARANGE#

## 测试账号

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **信息系统名称** | **测试账号/认证设施** | **测试人员访问地址** |
| 1 | #SYSTEM# | #CSACCOUNT# | #IP# |

## 测试工具

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **工具名称** | **版本** | **功能描述** |
| 1 | AWVS | v14 | 针对主机的80（HTTP）或443（HTTPS），进行漏洞扫描，以达到发现漏洞的目的。 |
| 2 | APPscan | v9.0.3.6 | 是一款非常好用且功能强大的Web 应用安全测试工具，曾以 Watchfire AppScan 的名称享誉业界，Rational AppScan 可自动化 Web 应用的安全漏洞评估工作，能扫描和检测所有常见的 Web 应用安全漏洞。 |
| 3 | Burpsuite | v1.7 | Proxy是一个拦截HTTP/S的代理模块，可以拦截，查看，修改在两个方向上的原始数据流，同时BP还有其他模块，可以实现暴力破解、重放等功能。 |
| 4 | wireshark | v2.0.4 | 抓包，显示出最为详细的网络封包资料 |
| 5 | NMAP | v7.70 | 扫描端口，以及端口上开放的服务。 |
| 6 | hydra | v8.1 | 针对各种服务进行爆破，如RDP、SSH、telnet、mysql等。 |
| 7 | sqlmap | v1.2.8 | 是一款SQL 注入的工具，只是把我们手工注入的一些方法，自动化实现了，所应用的原理，与常见的SQL 注入手法一致。通过程序自动化实现SQL 注入s，加快注入的速度。以提高渗透测试工作的效率。 |
| 8 | Nessus | v8.0.3 | 主要是用来扫描系统漏洞的一款开源工具。 |
| 9 | 其余工具 | / | 安全团队编写的脚本、测试软件等。 |

# 结果汇总

## **漏洞统计**

|  |  |  |
| --- | --- | --- |
| **危害级别** | **漏洞数量** | **安全状况评价** |
| **高危** |  | **/** |
| **中危** |  | **/** |
| **低危** |  | **/** |

## **数量分布**

## **风险分析**

| **序号** | **系统名称** | **漏洞名称** | **风险级别** | **风险描述** |
| --- | --- | --- | --- | --- |
| 1 | #SYSTEM# | #POCNAME# | #POCRISK# | #POCDISCRIBE# |

# 漏洞详细描述及加固建议

## #SYSTEM#系统

### 5.1.1 【#VULNERABILITIES\_SECTION#】#VULNERABILITIES\_SECTION#

|  |  |
| --- | --- |
| **风险描述** | #VULNERABILITIES\_SECTION# |
| **测试过程** | #VULNERABILITIES\_SECTION# |
| **整改建议** | #VULNERABILITIES\_SECTION# |