

**xx系统**

**渗透测试报告**

x年x月x日

目录

[一. 项目概述 3](#_Toc28332807)

[1.1 评估范围 3](#_Toc28332808)

[1.2 漏洞综述 3](#_Toc28332809)

[二. 漏洞说明 4](#_Toc28332810)

[2.1 XXX漏洞 4](#_Toc28332811)

[2.1.1 漏洞概要 4](#_Toc28332812)

[2.1.2 漏洞详情 4](#_Toc28332813)

[2.1.3 修复建议 4](#_Toc28332814)

[三. 测试总结及建议 4](#_Toc28332815)

[四. 附录：XX漏洞等级表 4](#_Toc28332816)

# 项目概述

## 评估范围

|  |  |  |
| --- | --- | --- |
| **项目** | **内容** | **备注** |
| 授权渗透范围 | xxx.xx.com | 该域名下不限协议及服务，不得改动旁站内容。 |
| 授权时间 | x年x月x日~x月x日 | 包含报告编写时间及复测时间 |
| 授权客户 | xx公司xx部xxx | 联系方式xxx |
| 测试机IP | xx.xx.x.xx | 测试地址报备 |
| 测试方法 | 手工+工具 |  |
| 测试工具 | BurpSuite、kalilinux、Wappalyzer、御剑、中国菜刀、Subdomain Brute |  |
| 遗留文件 | 渗透过程中产生了几个重要文件用作漏洞证明，需要甲方后期清除 | /var/www/html/shell.php |
| 注意事项 | 渗透测试前客户需备份网站所有程序及数据，保证网站在渗透测试过程中被技术性破坏的情况下仍能通过备份恢复。  不得在渗透测试期间提供业务服务，避免产生的新数据丢失。 |  |

## 漏洞综述

本次渗透测试共发现漏洞xx个，其中严重漏洞xx个，高危漏洞xx个，中危xx个，低位xx个，目标总体安全评价为xx。研判标准参考文末附件。

本次测试主要漏洞列表见下。

# 漏洞说明

## XXX漏洞

### 漏洞概要

|  |  |  |
| --- | --- | --- |
| **类目** | **内容** | **备注** |
| 漏洞位置 |  |  |
| 漏洞类型 |  |  |
| 严重性 |  |  |
| 主要危害 |  |  |
| 其他信息 |  |  |

### 漏洞详情

### 修复建议

# 测试总结及建议

# 附录：[漏洞等级评判标准](https://security.360.cn/News/news/id/252)

【严重】

1、直接获取核心服务器权限的漏洞，包括但不限于上传Webshell、任意代码执行、远程命令执行等。

2、直接导致严重的信息泄露漏洞，包括但不限于重要数据库的SQL注入、系统权限控制不严格等导致的敏感数据泄露漏洞等。

3、直接导致严重影响的逻辑漏洞，包括但不限于核心账户体系的账密校验逻辑等。

【高危】

1、重要业务敏感数据信息泄露漏洞，包括但不限于重要用户信息、订单信息、数据文件信息等。

2、重要业务的逻辑漏洞，包括但不限于权限绕过等。

3、不需交互的重点业务漏洞，包括但不限于文件遍历、任意文件包含、任意文件读取等。

4、包含重要业务敏感信息的非授权访问，包括但不仅限于绕过认证直接访问管理后台、后台弱密码、可直接获取大量内网敏感信息的SSRF等。

【中危】

1、不需交互对用户产生危害的安全漏洞，包括但不限于一般页面存储型XSS等。

2、普通信息泄露漏洞，包括但不限于用户信息泄露和业务敏感信息泄露等。

3、普通的逻辑设计缺陷和流程缺陷，包括但不限于越权查看非核心系统的订单信息等。

4、其他造成中度影响的漏洞，例如：没有敏感信息的SQL注入、无回显SSRF漏洞等。

【低危】

1、在特殊条件下才能获取用户信息的安全漏洞，包括但不限于反射XSS等。

2、轻微信息泄露，包括但不限于服务器物理路径、边缘系统文件、本地日志等。

3、其他造成低危害的漏洞，例如：管理后台开放、解析漏洞、存在可被暴力破解接口等。