

**pikachu系统**

**渗透测试报告**

2022年10月22日

目录

[一. 项目概述 3](#_Toc117368627)

[1.1 评估范围 3](#_Toc117368628)

[1.2 漏洞综述 3](#_Toc117368629)

[二. 漏洞说明 4](#_Toc117368630)

[2.1 XSS漏洞 4](#_Toc117368631)

[2.1.1 漏洞概要 4](#_Toc117368632)

[2.1.2 漏洞详情 5](#_Toc117368633)

[2.1.3 修复建议 5](#_Toc117368634)

[2.2 SQLi漏洞 5](#_Toc117368635)

[2.2.1 漏洞概要 5](#_Toc117368636)

[2.2.2 漏洞详情 6](#_Toc117368637)

[2.2.3 修复建议 6](#_Toc117368638)

[2.3 任意文件上传漏洞 6](#_Toc117368639)

[2.3.1 漏洞概要 6](#_Toc117368640)

[2.3.2 漏洞详情 7](#_Toc117368641)

[2.3.3 修复建议 8](#_Toc117368642)

[三. 测试总结及建议 8](#_Toc117368643)

[四. 附录：漏洞等级评判标准 8](#_Toc117368644)

# 项目概述

## 评估范围

|  |  |  |
| --- | --- | --- |
| **项目** | **内容** | **备注** |
| 授权渗透范围 | 192.168.96.135/pikachu/ | 该域名下不限协议及服务，不得改动旁站内容。 |
| 授权时间 | 2022年10月21日~10月22日 | 包含报告编写时间及复测时间 |
| 授权客户 | pikachu公司 系统安全部 张三 | 联系方式13877887788 |
| 测试机IP | 192.168.1.37 | 测试地址报备 |
| 测试方法 | 手工+工具 |  |
| 测试工具 | BurpSuite、kalilinux、Wappalyzer、御剑、蚁剑、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 | C:\phpStudy\WWW\pikachu\vul\unsafeupload\  uploads\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 3个，其中严重漏洞 2个，高危漏洞 0 个，中危漏洞 0个，低危 1个，目标总体安全评价为 差 。研判标准参考文末附件。

本次测试主要漏洞列表见下。

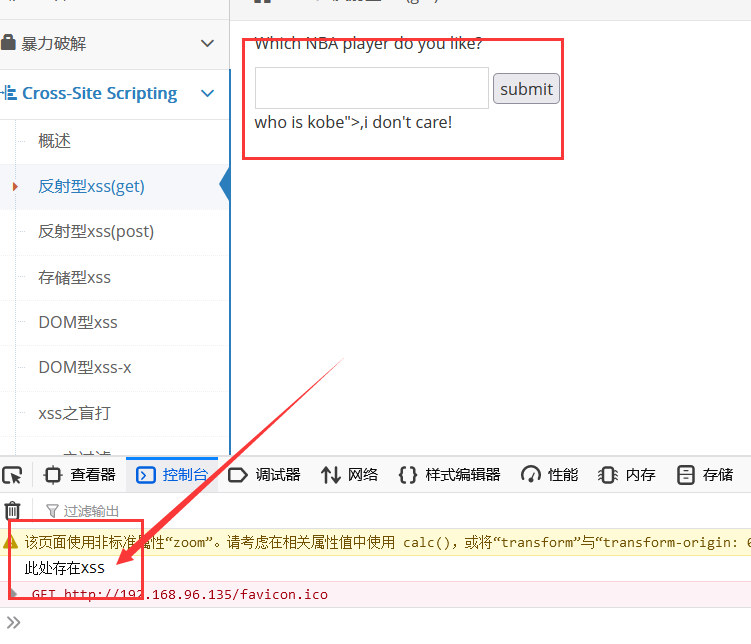
# 漏洞说明

## XSS漏洞

### 漏洞概要

|  |  |  |
| --- | --- | --- |
| **类目** | **内容** | **备注** |
| 漏洞位置 | http://192.168.96.135/pikachu/vul/xss/xss\_reflected\_get.php |  |
| 漏洞类型 | 反射型XSS |  |
| 严重性 | 低危 |  |
| 主要危害 | 获取用户IP、cookie、浏览记录、个人信息等；在网页显示广告、垃圾信息等 |  |
| 其他信息 |  |  |

### 漏洞详情



### 修复建议

1. 将网站所有输入点输入的内容进行实体化编码，对输入了href属性值的地方进行严格的格式验证

2. 如果有富文本输入场景，使用既有的富文本输入框架

## SQLi漏洞

### 漏洞概要

|  |  |  |
| --- | --- | --- |
| **类目** | **内容** | **备注** |
| 漏洞位置 | http://192.168.96.135/pikachu/vul/sqli/sqli\_search.php |  |
| 漏洞类型 | SQL注入 |  |
| 严重性 | 严重 |  |
| 主要危害 | 拖库、写入文件、执行系统命令等。 |  |
| 其他信息 |  |  |

### 漏洞详情



### 修复建议

1. 使用安全的数据库连接方式如PDO、MySQLi

2. 不直接拼接前端提交的参数查询

3. 将查询语句进行预编译；

3. 对前端提交的特殊字符进行转义、使用成熟的防注入框架

## 任意文件上传漏洞

### 漏洞概要

|  |  |  |
| --- | --- | --- |
| **类目** | **内容** | **备注** |
| 漏洞位置 | http://192.168.96.135/pikachu/vul/unsafeupload/servercheck.php |  |
| 漏洞类型 | 任意文件上传导致getShell |  |
| 严重性 | 高危 |  |
| 主要危害 | 执行系统命令，读取系统文件、控制服务器 |  |
| 其他信息 | shell文件在网站服务器路径：C:\phpStudy\WWW\pikachu\vul\unsafeupload\  uploads\shell.php，请手动删除该文件 |  |

### 漏洞详情





### 修复建议

1. 使用文件类型白名单

2. 对白名单内的文件进行内容检查：检测文件特征是否与后缀一致、检测文件内容是否包含恶意代码执行的关键函数，脚本代码的标签<?php等内容

3. 将上传的文件随机重命名

4. 对于只需要用户上传不需要用户访问的文件，不返回文件保存路径

# 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。