**南开大学**

**实习实训漏洞复现报告**

**2022年XX月XX日**

目录

[1.漏洞复现结论（15分） 1](#_Toc28487)

[1.1风险等级分布 1](#_Toc7481)

[2.工作计划（25分） 1](#_Toc24528)

[2.1工作人员 1](#_Toc13939)

[2.2漏洞对象 1](#_Toc3137)

[2.3漏洞复现阶段 1](#_Toc7909)

[2.4风险等级 2](#_Toc1860)

[3.漏洞复现过程（35分） 2](#_Toc6133)

[3.1 风险管理及规避 2](#_Toc18532)

[3.2测试方法 2](#_Toc4033)

[3.3测试中所用的工具 2](#_Toc28445)

[4. 漏洞复现结果（25分） 3](#_Toc12892)

[4.1 POC插件编写 3](#_Toc32666)

[4.2 漏洞信息 3](#_Toc25120)

# 1.漏洞复现结论（15分）

XXX的安全人员采用科学的漏洞复现步骤于2XXX年XX月XX日至2XXX年XX月XX日对XXX进行了全面深入的漏洞复现。

本次共发现漏洞X个，其高危漏洞X个，中危漏洞X个,低危漏洞X个。

|  |  |  |
| --- | --- | --- |
| **序号** | **漏洞名称** | **风险值** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

## 1.1风险等级分布

本次评估漏洞的详细风险等级分布如下：

# 2.工作计划（25分）

## 2.1工作人员

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 职务 | 姓名 | 联系方式 |
| 1 | 组长 |  |  |
| 2 | 组员 |  |  |
| 3 | 组员 |  |  |
| 4 | 组员 |  |  |
| 5 | 组员 |  |  |

## 2.2漏洞对象

测试对象应为渗透测试授权书明确表明的对象。

## 2.3漏洞复现阶段

|  |  |
| --- | --- |
| 项目阶段 | 工作内容 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## 2.4风险等级

|  |  |  |
| --- | --- | --- |
| 编号 | 风险等级 | 风险描述 |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

# 3.漏洞复现过程（35分）

漏洞复现过程是通过本地测试利用目标网站安全漏洞，模拟恶意攻击者的攻击方法。以人工渗透为主，以漏洞扫描工具为辅，在保证整个渗透测试过程都在可以控制和调整的范围之内尽可能的获取目标信息系统的管理权限以及敏感信息。

## 3.1 风险管理及规避

如何保障客户系统在测试过程中稳定、安全的运转。

## 3.2测试方法

根据具体项目具体分析测试方法，例如信息收集等。

## 3.3测试中所用的工具

详细描述本次测试过程中使用的工具，以及工具版本。

# 漏洞复现结果（25分）

## 4.1 POC插件编写

参考POC模板、SQL注入案例模板、命令执行漏洞案例模板、任意文件读取下载案例模板、文件上传案例模板，进行poc插件编写。

## 4.2 漏洞信息

根据原始报告、漏洞报告以及OWASP TOP 10漏洞信息描述，填写如下表格。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **UVD-ID** |  | **漏洞类别** |  | **CVE-ID** |  |
| **披露/发现时间** |  | **bugtraq编号** |  | **CNNVD-ID：** |  |
| **提交时间** |  | **漏洞发现者** |  | **CNVD-ID：** |  |
| **漏洞等级** |  | **提交者** |  | **搜索关键词** |  |
| **影响范围** |  | | | | |
| **来源** |  | | | | |
| **漏洞简介** |  | | | | |
| **漏洞详情** |  | | | | |
| **参考链接** |  | | | | |
| **靶场信息** |  | | | | |
| **POC** |  | | | | |
| **修复方案** |  | | | | |

备注：蓝色字体均为提示内容，正式报告内容中，应当删除。