**{{Company\_A}}**

**渗透测试报告**

{{Test\_Type}}

**{{Company\_B}}**

{{Report\_Date}}

**适用性声明**

本报告仅适用于此次在{{Company\_A}}开展渗透测试时的状况。渗透测试结束之后，因内部环境或不可预知的国内国际政治、经济、法律等社会环境的变化，可能会影响评估结论的有效性。再者，任何控制系统都存在固有的局限性，错误、违反内部控制的情况仍然有可能发生及不被发现。

**版权声明**

本文中的所有信息均为单位内部信息，务请妥善保管，未经{{Company\_A}}作出的书面许可，不得为任何目的、以任何形式或手段（包括电子、机械、复印、录音或其他形式）对本文档的任何部分进行复制、存储、引入检索系统或者传播。

**版本变更记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本号 | 拟制／修改日期 | 拟制／修改人 | 修改记录 | 批准人 |
| V1.0 | {{Report\_Date}} | {{Author}} | 创建文档 | {{Project\_Manager}} |

# 项目概述

## 服务背景

{{Company\_A}}授权{{Company\_B}}对信息系统进行渗透测试。{{Company\_B}}的渗透测试工作按照事前制定的渗透测试实施方案进行。

本次渗透测试是由测试人员以黑盒或白盒的形式完成对指定信息系统的测试工作。渗透测试涉及的范围仅包括{{Company\_A}}授权指定的域名或系统，不对任何超于授权范围内的网站域名和IP进行评估。

## 项目目标

对客户信息系统渗透测试的主要目标是：直观体现信息业务安全风险现状了解当前降低安全风险的初始任务；检验信息系统安全基础设施的有效性，针对渗透成果获得有效处理方案；防止系统入侵安全隐患再次被黑客利用，避免业务经济损失数量持续增加；维护客户业务公众形象与声誉，增强对客户可靠业务环境的信心；最大限度的降低客户安全运营成本，提高信息业务发展安全竞争力。

# 服务概述

## 测试对象

此次渗透测试是根据{{Company\_A}}要求，针对业务系统所进行的一次渗透测试，具体测试对象如下：

|  |  |  |
| --- | --- | --- |
| **序号** | **系统名称** | **域名或URL** |
|  |  |  |
|  |  |  |

## 测试人员

此次项目的渗透测试小组由{{Company\_B}}资深安全服务工程师主要参与，工作人员配合。项目组成人员如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **项目角色** | **姓名** | **手机号** | **邮箱** |
|  |  |  |  |  |
|  |  |  |  |  |

## 测试流程



## 测试方法

基于本次安全测试的性质（合规性验证/风险评估/漏洞发现）及目的（提升系统安全性/满足监管要求/保障业务连续性），为确保测试过程不对目标系统、网络或业务造成破坏、损害或数据篡改，测试团队严格遵循非破坏性测试原则，主动规避以下高风险攻击手段：

不通过欺骗、诱导等手段获取非公开信息或权限（如伪装身份、钓鱼邮件、电话诈骗等）。不模拟大流量洪泛或资源耗尽攻击，避免影响目标系统正常运行。不散布病毒、木马、勒索软件、蠕虫等恶意程序，不利用零日漏洞（0day）进行未授权植入。不针对企业微信、钉钉、Slack等工具的漏洞进行利用或窃取会话信息。不通过伪造网站、邮件或链接诱导用户泄露敏感信息（如账号密码、验证码等）。若测试目标为防御体系验证（如抗DDoS能力），需提前与客户签署授权书并明确攻击范围。

## 安全测试流程

**（1）信息收集阶段**

主动信息收集：

通过端口扫描（如Nmap）、协议识别（如Banner抓取）获取开放服务及版本信息。利用工具（如Sublist3r）或DNS查询（如Dig、Nslookup）挖掘隐藏的子域名。检测Web应用目录结构（如Dirsearch、Gobuster），识别未授权访问的敏感文件（如备份文件、配置文件）。

被动信息收集：

从Google Hacking、Shodan、Censys等平台获取历史漏洞、技术文档或暴露的IP段。通过LinkedIn、GitHub等渠道收集目标组织的技术栈、人员信息（需遵守隐私政策）。最终形成《信息收集报告》，包含IP地址范围、开放端口、服务版本、潜在漏洞点等。

**（2）渗透测试阶段**

使用自动化工具（如Burp Suite、Nessus）检测常见漏洞（如SQL注入、XSS、CSRF、文件上传漏洞）。对高风险漏洞进行人工复现，排除误报并确认影响范围（如越权访问、信息泄露）。若存在漏洞，尝试获取普通用户权限（如Webshell上传、数据库弱口令登录）。仅在授权范围内测试，不扩展至关联系统或生产环境。形成《渗透测试初步报告》，记录发现的漏洞、利用方式及风险等级。

**（3）缺陷利用阶段**

尝试通过内核漏洞（如Dirty Cow）、配置错误（如SUID提权）或密码破解（如John the Ripper）获取管理员权限。模拟攻击者建立后门（如添加SSH密钥、计划任务），测试系统日志监测与响应能力。测试完成后彻底清除测试痕迹（如删除测试账号、关闭后门），避免残留风险。若首次未成功提权，可结合新发现的信息重新规划攻击路径（如从信息收集阶段补充数据）。更新《渗透测试报告》，补充权限提升路径及系统防御弱点分析。

**（4）成果收集与威胁分析阶段**

按类型（如OWASP Top 10）、严重程度（高危/中危/低危）及影响范围（如数据泄露、服务中断）进行归类。结合业务场景分析漏洞利用可能性（如金融系统更关注数据窃取，工业控制系统更关注设备停机）。量化漏洞对机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）的破坏程度。形成《威胁分析矩阵表》，明确每个漏洞的CVSS评分、修复优先级及建议措施。

**（5）输出报告阶段**

报告结构：

执行摘要：概述测试目标、范围、关键发现。

漏洞详情：按威胁等级排序，包含漏洞描述、复现步骤、截图/日志证据。

修复建议：提供代码级修复方案（如输入校验）、配置优化建议（如关闭不必要的端口）或管理措施（如权限分离）。

附录：测试工具列表、授权书扫描件、免责声明。

可视化呈现：使用图表（如漏洞分布饼图、修复进度甘特图）增强报告可读性。

报告交付：通过加密渠道（如PGP邮件）发送报告，并安排现场解读会议解答客户疑问。

## 风险管理及规避

为保障客户系统在渗透测试过程中稳定、安全的运转，我们将提供以下多种方式来进行风险规避。

**（1）对象的选择**

为更大程度的避免风险的产生，渗透测试还可选择对备份系统进行测试。因为备份系统与在线系统所安装的应用和承载的数据差异较小，而其稳定性要求又比在线系统低，因此，选择对备份系统进行测试也是规避风险的一种常见方式。

**（2）时间的控制**

从时间安排上，测试人员将将尽量避免在数据高峰时进行测试，以此来减小测试工作对被测试系统带来的压力。

另外，测试人员在每次测试前也将通过电话、邮件等方式告知相关人员，以防止测试过程中出现意外情况。

**（3）技术手段**

{{Company\_B}}的渗透测试人员都具有丰富的经验和技能，在每一步测试前都会预估可能带来的后果，对于可能产生影响的测试（如：溢出攻击）将被记录并跳过，并在随后与客户协商决定是否进行测试及测试方法。

**（4）监控措施**

针对每一系统进行测试前，测试人员都会告知被测试系统管理员，并且在测试过程中会随时关注目标系统的负荷等信息，一旦出现任何异常，将会停止测试。

**（5）工具的使用**

在使用工具测试的过程中，测试人员会通过设置线程、插件数量等参数来减少其对系统的压力，同时还会去除任何可能对目标系统带来危害的插件，如：远程溢出攻击类插件、拒绝服务攻击类插件等等。

# 漏洞统计

我公司依据本次测试内容安排资深安全工程师采用科学的渗透测试手段于{{Test\_Date}}至{{End\_Date}}对{{Company\_A}}进行了全面深入的漏洞检测。共计发现{{VULN\_TOTAL}}个漏洞，包括{{VULN\_CRITICAL}}个严重漏洞，{{VULN\_HIGH}}个高危漏洞，{{VULN\_MEDIUM}}个中危漏洞，{{VULN\_LOW}}个低危漏洞，各系统漏洞情况统计如下：

{{VULN\_STATS\_TABLE}}

{{VULN\_DETAILS\_LIST}}