****

渗透测试报告

|  |  |
| --- | --- |
| 客户名称 | {{report\_center}} |
| 报告时间 | {{ report\_end\_time }} |

**文档说明**

|  |  |  |  |
| --- | --- | --- | --- |
| 文档名称 | {{report\_center}}渗透测试报告 | | |
| 文档管理编号 | SFSS-PT-R0101 | | |
| 保密级别 | 商密 | 文档版本号 | V1.0 |
| 制作人 | 深信服安全服务团队 | 制作日期 | {{ report\_end\_time }} |
| 复审人 | 深信服安全服务团队 | 复审日期 | {{ report\_end\_time }} |
| 扩散范围 | 限“深信服科技股份有限公司项目组”、{{report\_center}} | | |
| 分发控制 | 深信服：创建、修改、读取。{{report\_center}}项目组：读取。 | | |

**版本变更记录**

| 修改日期 | 版本 | 说明 | 修改人 |
| --- | --- | --- | --- |
| {{ report\_end\_time }} | V1.0 | 正式版本 | 深信服安全服务团队 |

**适用范围**

本次渗透测试是由{{report\_center}}授权，由深信服科技股份有限公司（以下简称“深信服”）对{{report\_center}}进行的安全风险深度评估，根据评估结果提交技术报告，用于对该网站系统的安全状况做出安全评估和加固建议，仅限于“深信服”、{{report\_center}}内部人员传阅。

本报告结论的有效性建立在被测试单位提供相关证据的真实性基础之上。本报告中给出的评估结论仅对被评估的信息系统当时的安全状态有效，当信息系统发生涉及到的系统构成组件（或子系统）变更时本报告不再适用。

**版权声明**

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属深信服所有，受到有关产权及版权法保护。任何个人、机构未经深信服的书面授权许可，不得以任何方式复制或引用本文的任何片段。

目录

[摘要 1](#_Toc2632)

[1渗透测试说明 3](#_Toc9557)

[1.1 测试时间 3](#_Toc23378)

[1.2 测试人员 3](#_Toc27355)

[1.3 测试范围与账户使用情况 3](#_Toc4846)

[2 问题总览 3](#_Toc5407)

[2.1 风险总览 3](#_Toc25600)

[2.2 漏洞概况 4](#_Toc26866)

[3 渗透测试漏洞详情 4](#_Toc28557)

[3.1 {{report\_systemname}} 4](#_Toc7382)

[4 渗透测试依据和参考 5](#_Toc3417)

[5 渗透测试工作说明 6](#_Toc24485)

[5.1 测试方法 6](#_Toc5748)

[5.2 漏洞评级标准 6](#_Toc23903)

[5.3 综合风险评级标准 7](#_Toc10563)

[5.4 测试工具 7](#_Toc31640)

[5.5 修复建议说明 8](#_Toc23242)

[6 致谢 8](#_Toc4629)

[7 意见反馈 8](#_Toc10045)

[8 了解更多 9](#_Toc18846)

# 摘要

应{{report\_center}}邀请，深信服安全服务团队于{{ report\_start\_time }}至{{ report\_end\_time }}，对本单位部分系统进行了全面的渗透测试。测试手段主要通过模拟黑客攻击手法对{{report\_systemname}}开展测试并发现安全隐患；本次安全测试共发现了{{vuls|length}}个安全漏洞，按漏洞风险分布为：高风险**{{vuls|vul\_statistics(3)}}**个，中风险**{{vuls|vul\_statistics(2)}}**个，低风险**{{vuls|vul\_statistics(1)}}**个。

深信服安全服务团队发现存在的安全漏洞主要为：{% set index\_space=namespace(value=1) %}{% if vuls|vul\_statistics(3) !=0 %}

发现存在的**高风险**的安全漏洞主要为：{% for item in vuls %}{% if item.vul\_level=='3'%}

{{ index\_space.value }}) {{report\_systemname}}存在**{{ item. vul\_name}}**漏洞的问题，{{ item.vul\_desc}}。{%set index\_space.value = index\_space.value +1%}{% endif %}{% endfor %}{% endif %} {% set index\_space=namespace(value=1) %}{% if vuls|vul\_statistics(2) !=0 %}

发现存在的**中风险**的安全漏洞主要为：{% for item in vuls %}{% if item.vul\_level=='2'%}

{{index\_space.value }}) {{report\_systemname}}存在**{{ item. vul\_name}}**漏洞的问题，{{ item.vul\_desc}}。{%set index\_space.value=index\_space.value+1%}{% endif %}{% endfor %}{% endif %} {% set index\_space=namespace(value=1) %}{% if vuls|vul\_statistics(1) !=0 %}

发现存在的**低风险**的安全漏洞主要为：{% for item in vuls %}{% if item.vul\_level=='1'%}

{{index\_space.value }}) {{report\_systemname}}存在**{{ item. vul\_name}}**漏洞的问题，{{ item.vul\_desc}}。{%set index\_space.value=index\_space.value+1%}{% endif %}{% endfor %}{% endif %}

本次渗透测试综合风险评分：**{% if vuls|vul\_statistics(3) !=0 %}高{% elif vuls|vul\_statistics(2)!=0 %}中{% elif vuls|vul\_statistics(1)!=0 %}低{% endif %}**风险，安全漏洞的详细情况及整改方法详见：第3章渗透测试漏洞详情。

{% if vuls|vul\_statistics(3) !=0 %}**从本次渗透测试结果来看，该系统在安全防护方面存在不足，难以抵御有组织的、高级别的安全攻击。**{% endif %}

建议{{report\_center}}单位从以下三个方面进行安全整改，进一步提高网络安全防护和管理水平：

在安全防护方面，建议完善安全基线并全面进行安全加固；加强办公终端管控，完善办公网络数据安全保护措施。

在威胁发现方面，建议进一步加强APT攻击检测和威胁监测能力，加强日常安全检查力度，完善等级保护和风险评估机制，对安全加固和防护效果定期进行检查和评估，及时识别和消除风险。

在安全管理方面，建议继续加强全体系信息安全工作的整体管理和组织协调，强化人员安全意识，严格落实各项规章制度，继续加强安全开发和上线前安全测试工作，不断提升运维管理水平。

# 1渗透测试说明

## 测试时间

本次渗透测试按照事先约定规避风险的时间段开展，如下所示：

| 测试工作时间段 | | | |
| --- | --- | --- | --- |
| 开始时间 | {{ report\_start\_time }} | 结束时间 | {{ report\_end\_time }} |

## 测试人员

本次渗透测试实施人员，如下所示：

| 参测人员名单 | | | | | |
| --- | --- | --- | --- | --- | --- |
| 姓名 | 深信服安全服务团队 | 测试IP | - | 联系方式 | - |

## 测试范围与账户使用情况

本次渗透测试范围如下图所示：

| 渗透测试范围 | | | | |
| --- | --- | --- | --- | --- |
| 编号 | 应用系统名称 | 应用系统URL/IP | 应用系统版本 | 测试账号 |
| 1 | {{report\_systemname}} | {{report\_test\_url}} | - | - |

# 问题总览

## 风险总览

| 风险总览 | | |
| --- | --- | --- |
| 编号 | 应用系统名称 | 渗透结果 |
| 1 | {{report\_systemname}} | 高危{{vuls|vul\_statistics(3)}}个  中危{{vuls|vul\_statistics(2)}}个  低危{{vuls|vul\_statistics(1)}}个 |

## 漏洞概况

本次渗透测试发现的漏洞摘要如下表所示：

| 渗透测试漏洞清单 | | | | |
| --- | --- | --- | --- | --- |
| 编号 | 系统名称 | 漏洞名称 | 漏洞影响 | 漏洞级别 |
| {%tr for item in vuls %} | | | | |
| {{ loop.index }} | {{report\_systemname}} | {{item. vul\_name}} | {{item.vul\_desc}} | {% if item. vul\_level=='3'%}高{% elif item.vul\_level=='2'%}中{% elif item.vul\_level=='1' %}低{% endif %} |
| {%tr endfor %} | | | | |

所有发现漏洞的详细说明和建议请参见第3章渗透测试漏洞详情。

# 渗透测试漏洞详情

## {{report\_systemname}}{% for item in vuls %}

### {{ item.vul\_name}}

|  |  |
| --- | --- |
| 漏洞级别 | {% if item.vul\_level=='3'%}高{% elif item.vul\_level=='2'%}中{% elif item.vul\_level=='1' %}低{% endif %} |
| URL/IP | {{ item.vul\_url}} |
| 漏洞及风险描述 | {{ item.vul\_desc}} |
| 漏洞举证：  {{item.vul\_content}} | |
| 修复建议 | {{ item.vul\_repair }} |

{% endfor %}

# 渗透测试依据和参考

深信服科技将参考下列国内、国际及深信服科技制定的相关标准或规范指导渗透测试工作。

国内标准、指南或规范：

* 《计算机信息系统 安全保护等级划分准则》GB17859-1999
* 《信息安全技术 信息安全风险评估规范》GB/T 20984-2007
* 《信息安全技术 信息系统灾难恢复规范》GB/T 20988-2007
* 《信息安全技术 安全漏洞等级划分指南》GB/T 30279-2020
* 《信息安全技术 信息安全风险评估实施指南》GB/T 31509-2015
* 《信息安全技术 网络安全等级保护实施指南》GB/T 25058-2019
* 《信息安全技术 网络安全等级保护基本要求》GB/T 22239-2019
* 《信息安全技术 网络安全等级保护测评要求》GB/T 28448-2019

国际标准、指南或规范：

* 《信息技术 安全技术 安全保证框架 第1部分：介绍和概念》ISO/IEC TR 15443-1:2012
* 《信息技术 安全技术 安全保证框架 第2部分：分析》ISO/IEC TR 15443-2:2012
* 《信息技术 安全技术 运行系统安全评估》ISO/IEC TR 19791:2010
* 《信息技术 安全技术 信息安全风险管理》ISO/IEC 27005:2018
* OWASP OWASP\_Testing\_Guide\_v4
* OWASP OWASP\_Development\_Guide\_2005
* OWASP OWASP\_Top\_10\_2021\_Chinese

深信服工作规范：

* 深信服科技安全服务工作规范、渗透测试实施规范

# 渗透测试工作说明

## 测试方法

深信服安全服务团队的攻击和渗透方法是对测试范围内的资产进行全面，可重复和可审计的评估。这种测试方法通过模拟黑客入侵的方式识别Web应用程序相关的安全漏洞，并提供解决此类漏洞的建议。渗透测试通过以下七个步骤进行：

| 编号 | 测试步骤 |
| --- | --- |
|  | 确定有关目标Web应用程序的详细信息 |
|  | 抓取目标Web应用程序并识别用户输入字段 |
|  | 了解正在运行的应用程序和服务 |
|  | 识别应用程序/操作系统的漏洞 |
|  | 验证漏洞，并且确定漏洞的风险 |
|  | 总结单个漏洞的风险和评级 |
|  | 总结整体系统的风险评级 |

## 漏洞评级标准

深信服安全服务团队的漏洞评级依照《信息安全技术-网络安全漏洞分类分级指南 GB/T 30279-2020》进行，从访问路径、触发要求、权限需求、交互条件、保密性影响程度、完整性影响程度、可用性影响程度七个维度进行技术赋值，按照标准要求计算出漏洞技术分级结果，共包含：超危、高危、中危、低危四个漏洞评级。

漏洞评级详情请参考《信息安全技术-网络安全漏洞分类分级指南 GB/T 30279-2020》。

## 综合风险评级标准

| 综合风险评级标准 | |
| --- | --- |
| 风险级别 | 说明 |
| 高风险 | 存在1个及以上高危漏洞，或3个以上中危漏洞的系统 |
| 中风险 | 存在1个到3个中危漏洞，或5个以上低危漏洞的系统 |
| 低风险 | 存在5个及以内低危漏洞，或未检测到漏洞的系统 |

## 测试工具

我们的测试方法需要使用商业扫描工具和开源/免费软件渗透测试工具。用于测试的工具（包括且不限）如下所示：

| 类型 | 名称 | 功能 | 作用 |
| --- | --- | --- | --- |
| 端口扫描工具 | TSS（自研） | 1. 网站WEB漏洞扫描 2. 主机系统漏洞扫描 3. 开放的端口扫描 4. 开放的服务识别 | 1. 扫描并发现业务系统的WEB漏洞、主机漏洞； 2. 输出扫描报告，报告中包含业务系统的基本信息如IP地址、服务类型、漏洞描述、漏洞危害等。 |
| NMAP | 1. 开放的端口扫描 2. 开放的服务识别 | 检测服务器开放的端口与服务。 |
| Goby |
| 域名资产分析工具 | Dig | 域名及资产发现搜集工具 | 基础资产收集、互联网信息泄露搜集、指纹识别、业务系统功能收集、接口信息收集。 |
| Nslookup |
| 北极星（自研） |
| 渗透工具 | Metasploit | 漏洞利用、溢出攻击 | 进行漏洞利用、溢出攻击、暴力破解等渗透测试。 |
| Kali | 渗透测试工具集 |
| SQLMAP | SQL注入渗透测试 |
| Burp Suite | 协议分析 |
| Tcpdump | 协议分析 |
| Wireshark | 协议分析 |
| 北极星（自研） | 应用缺陷分析及情报搜集 |
| gorailgun（自研） | 应用缺陷分析 |

备注：在实施渗透的过程中，深信服安全服务团队会根据业务系统场景的不同，使用符合场景的脚本用于自动化测试。

## 修复建议说明

深信服在本文档中提供的各项修复建议均为基于漏洞的原理性分析修复方案或应用厂商提供的通用性方案，深信服无法完全了解系统研发详情，无法判断实际修复动作可能对业务造成的影响，对应建议仅供漏洞修复参考。

深信服建议客户在测试环境中进行漏洞修复的验证工作或在修复前做好备份，避免修复过程中因非预期的问题导致业务受到影响。

# 致谢

深信服安全服务团队由衷感谢{{report\_center}}相关部门与人员在渗透测试过程中进行沟通、协调的部门和人员，是你们的大力配合，使得我们的工作能够顺利完成。

# 意见反馈

请您点击下方链接或扫码进行服务评价以及意见反馈，您的宝贵意见将是我们改善工作的方向和服务的动力，我们定会认真对待，切实改进，在此对您的支持和帮助表示感谢！

链接评价：<https://www.wjx.cn/vm/YfrNigW.aspx>

二维码评价：



# 了解更多

了解更多安全信息，或关于本文出现的漏洞、攻击方式等详细介绍与建议，可查看深信服安全中心的威胁维基或关注深信服科技公众号了解最新的安全情报。

威胁维基：http://sec.sangfor.com.cn/vulns/lst.html

公众号：

