**保密级别：商业机密**

**中韩人寿渗透测试报告**



**深信服科技股份有限公司**

* **文档说明**

|  |  |  |  |
| --- | --- | --- | --- |
| 文档名称 | 中韩人寿渗透测试报告 | | |
| 保密级别 | 商密 | 文档版本号 | V1.0 |
| 制作人 | 尹普 | 制作日期 | 2018-12-15 |
| 复审人 | 欧阳思裕 | 复审日期 | 2018-12-17 |
| 扩散范围 | 限“深信服”、中韩人寿保险有限公司 | | |

* **适用范围**

本次渗透测试是由中韩人寿保险有限公司授权，由深信服科技股份有限公司（以下简称“深信服”）对中韩人寿保险有限公司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”、中韩人寿保险有限公司内部人员传阅。

* **版本变更记录**

|  |  |  |  |
| --- | --- | --- | --- |
| 修改日期 | 版本 | 说明 | 修改人 |
|  |  |  |  |
|  |  |  |  |

目 录

[目 录 3](#_Toc531809705)

[报告摘要 4](#_Toc531809706)

[1. 渗透测试说明 6](#_Toc531809707)

[1.1 测试时间与人员 6](#_Toc531809708)

[1.2 测试范围 6](#_Toc531809709)

[1.3 风险级别 6](#_Toc531809710)

[2. 问题总览 7](#_Toc531809711)

[2.1 风险总览 7](#_Toc531809712)

[2.2 关键漏洞概况 8](#_Toc531809713)

[3. 渗透测试工作内容 9](#_Toc531809714)

[3.1 测试步骤 9](#_Toc531809715)

[3.2 测试工具 9](#_Toc531809716)

[3.3 测试漏洞种类 10](#_Toc531809717)

[4. 渗透测试漏洞细节 11](#_Toc531809718)

[4.1 xx系统 11](#_Toc531809719)

[4.1.1 XXXX漏洞 11](#_Toc531809720)

[4.1.2 任意帐号密码重置漏洞 12](#_Toc531809721)

[4.2 xx系统 14](#_Toc531809722)

[4.2.1 XXXX漏洞 14](#_Toc531809723)

[4.2.2 XXXX漏洞 14](#_Toc531809724)

[5. 致谢 15](#_Toc531809725)

[6. 了解更多 15](#_Toc531809726)

报告摘要

应XX单位邀请，深信服安全服务团队于2018年12月12日至2018年12月14日，对中国人寿有限公司应用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XX系统开展测试并发现安全隐患；本次安全测试共发现了10个安全漏洞，按漏洞风险分布为：高风险4个，中风险4个，低风险2个。

深信服安全服务团队发现存在的高风险的安全漏洞主要为：

1) 网站存在超级管理员设置过于简单的问题，安全人员攻破并获取系统较高管理员权限，包括：查看修改删除应用应用交付，可以导致用户业务大面积瘫痪，影响用户对外的应用服务。

2) 网站存在系统用户密码重置的逻辑绕过漏洞问题，安全人员可以利用泄露的敏感接口数据，结合网站的密码重置逻辑，可以通过数据撞库的方式重置用户的密码，从而获取到合理用户的登录权限，登录进入系统，获取到内部的敏感信息，对数据进行删除修改等操作，给网站带来不可挽回的损失。

3) 网站后台管理页面存在SQL注入漏洞，恶意攻击者可以注入SQL代码来检索存储在数据库中的敏感数据，找出数据库结构，创建、修改、利用或破坏数据库中的数据，给网站带来极大风险。

4） XXXXXXXX

本次安全测试综合风险评分：高风险

从本次渗透测试结果来看，XX单位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。**

建议XX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：

1. 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。
2. 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。
3. 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。

# 渗透测试说明

1.1 测试时间与人员

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** | | | |
| 起始时间 | 2018年12月12日 | 结束时间 | 2018年12月14日 |

本次渗透测试实施人员，如下所示：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **参测人员名单** | | | | | |
| 姓名 | 尹普 | 所属部门 | 深信服安全服务团队 | 联系方式 | 13437291936 |

1.2 测试范围

本次渗透测试范围，如下所示：

|  |  |  |  |
| --- | --- | --- | --- |
| **渗透测试范围** | | | |
| 编号 | 应用系统名称 | 应用系统URL | 应用系统IP |
| 1 | 官网门户网站 | www.sinokorealife.com.cn | 101.71.248.243 |
| 2 | 自主服务中心网站 | eservice.sinokorealife.com.cn | 183.129.157.228 |
| 3 | 办公管理系统 | casserver.sinokorealife.com.cn | 218.75.72.220 |
| 4 | 营销员管理系统 | newagent.sinokorealife.com.cn | 218.75.72.214 |

1.3 风险级别

|  |  |
| --- | --- |
| **风险级别** | |
| 级别 | 依据 |
| **高危** | 1. 获取服务器权限的漏洞 2. 严重的信息泄漏漏洞 3. 敏感信息越权访问 4. 严重的逻辑设计缺陷和流程缺陷 5. 任意文件操作漏洞 6. 存储型跨站脚本漏洞、XXE漏洞 |
| **中危** | 1. 需交互方可影响用户的漏洞 2. 普通的逻辑设计缺陷和流程缺陷 3. 比较严重的信息泄漏漏洞 |
| **低危** | 1. 普通信息泄漏漏洞 2. 难以利用但存在安全隐患的漏洞、只能造成轻微影响的漏洞 |

# 问题总览

2.1 风险总览

本次渗透测试总计发现漏洞40个，整体风险分布如下图所示：

|  |  |
| --- | --- |
| 安全级别 | 漏洞数量 |
| 高危 | 18 |
| 中危 | 10 |
| 低危 | 12 |

2.2 关键漏洞概况

本次渗透测试发现的高危漏洞摘要如下表所示：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **编号** | **系统名称** | **漏洞名称** | **漏洞影响** | **漏洞级别** |
| 1 |  | SQL注入漏洞 | 由于缺乏输入验证，攻击者可以将修改原始SQL查询的SQL代码，从而导致数据库服务器执行任意的SQL查询。恶意攻击者可以注入SQL代码来检索存储在数据库中的敏感数据，找出数据库结构，或者创建，修改或删除数据库中的数据。恶意攻击者甚至可能在数据库服务器上执行任意操作系统命令。 | **高** |
| 2 |  | 管理员弱口令 | 恶意攻击者一旦获得管理员账号密码，可以对后台数据进行收集和篡改。比如，获取所有用户的账号信息；重置所有用户的账号密码；对商城所有的商品进行管理；对网站模板进行编辑；查看交易数据等。 | **高** |

**所有发现漏洞的详细说明和建议请参见第4章节渗透测试漏洞细节。**

# 渗透测试工作内容

## 3.1 测试步骤

深信服安全服务团队对测试范围内的资产进行全面的评估。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 |
| 1 | 前期交互阶段：与客户进行交流、讨论，来确定渗透测试的范围与目标 |
| 2 | 情报搜集阶段：对目标客户的系统进行一系列踩点工作 |
| 3 | 威胁建模阶段：主要使用在情报搜集阶段所获取的信息，来标识出目标系统上可能存在的安全漏洞与弱点 |
| 4 | 漏洞分析阶段：主要是从前面几个环节获取的信息，并从中分析和理解哪些攻击途径可行 |
| 5 | 渗透攻击阶段：主要是针对目标系统实施已经经过了深入研究和测试的渗透攻击，进行针对性的安全测试 |
| 6 | 后渗透攻击阶段：从已经攻陷了客户的一些系统开始，将以特定业务系统为目标，标识出关键的基础设施，并寻找客户组织最具价值的信息和资产，并需要演示出能够对客户组织造成最重要业务影响的攻击途径 |
| 7 | 报告阶段：提交渗透测试报告，阐明客户系统中存在的安全隐患以及专业的修复建议 |

## 3.2 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：

► Tenable Nessus

► BurpSuite

► Appscan

► Nmap

## 3.3 测试漏洞种类

|  |  |  |
| --- | --- | --- |
| 测试大类 | 测试项 | 测试目的 |
| 身份验证类 | 用户注册 | 检查用户注册功能可能涉及的安全问题 |
| 用户登录 | 检查用户登录功能可能涉及的安全问题 |
| 修改密码 | 检查用户修改密码功能可能涉及的安全问题 |
| 密码重置 | 检查忘记密码、找回密码、密码重置功能可能涉及的安全问题 |
| 验证码绕过 | 检测验证码机是否合理，是否可以被绕过 |
| 用户锁定功能 | 测试用户锁定功能相关的安全问题 |
| 会话管理类 | Cookie重放攻击 | 检测目标系统是否仅依靠cookie来确认会话身份，从而易受到cookie回放攻击 |
| 会话令牌分析 | Cookie具有明显含义，或可被预测、可逆向，可被攻击者分析出cookie结构 |
| 会话令牌泄露 | 测试会话令牌是否存在泄露的可能 |
| 会话固定攻击 | 测试目标系统是否存在固定会话的缺陷 |
| 跨站请求伪造 | 检测目标系统是否存在CSRF漏洞 |
| 访问控制类 | 功能滥用 | 测试目标系统是否由于设计不当，导致合法功能非法利用 |
| 垂直权限提升 | 测试可能出现垂直权限提升的情况 |
| 水平权限提升 | 测试可能出现水平权限提升的情况 |
| 输入处理类 | SQL注入 | 检测目标系统是否存在SQL注入漏洞 |
| 文件上传 | 检测目标系统的文件上传功能是否存在缺陷 ，导致可以上传非预期类型和内容的文件 |
| 任意文件下载 | 检测目标系统加载/下载文件功能是否可以造成任意文件下载问题 |
| XML注入 | 测试目标系统-是否存在XML注入漏洞 |
| 目录穿越 | 测试目标系统是否存在目录穿越漏洞 |
| SSRF | 检测目标系统是否存在服务端跨站请求伪造漏洞 |
| 本地文件包含 | 测试目标站点是否存在LFI漏洞 |
| 远程文件包含 | 测试目标站点是否存在RFI漏洞 |
| 远程命令/代码执行 | 测试目标系统是否存在命令/代码注入漏洞 |
| 反射型跨站脚本 | 检测目标系统是否存在反射型跨站脚本漏洞 |
| 存储型跨站脚本 | 检测目标系统是否存在存储型跨站脚本漏洞 |
| DOM-based跨站脚本 | 检测目标系统是否存在DOM-based跨站脚本漏洞 |
| 服务端URL重定向 | 检查目标系统是否存在服务端URL重定向漏洞 |
| 信息泄露类 | error code | 测试目标系统的错误处理能力，是否会输出详尽的错误信息 |
| Stack Traces | 测试目标系统是否开启了Stack Traces 调试信息 |
| 敏感信息 | 尽量收集目标系统的敏感信息 |
| 第三方应用类 | 中间件 | 测试目标系统是否存在jboss、weblogic、tomcat等中间件 |
| CMS | 测试目标系统是否存在dedecms、phpcms等CMS |

# 渗透测试漏洞细节

## 4.1 xx系统

### 4.1.1 XXXX漏洞

|  |  |
| --- | --- |
| 漏洞级别-- | |
| 漏洞名称 | |
| URL/IP |  |
| 漏洞描述 |  |
| 风险描述 |  |
| 漏洞验证过程： | |
| 处置建议 |  |
| 参考链接 | 补丁链接、漏洞介绍链接等 |

### 4.1.2 任意帐号密码重置漏洞

|  |  |
| --- | --- |
| 漏洞级别--高 | |
| 任意帐号密码重置漏洞 | |
| URL/IP | http://ecidcwc.\*\*\*\*.gov.cn/user/findPassword |
| 漏洞描述 | 在找回密码的过程中由于验证码返回，导致可重置任意用户的帐号密码 |
| 风险描述 | 恶意攻击者可重置用户密码，登录用户账户，造成信息泄露，危害个人信息安全 |
| 漏洞验证过程：  对某存在帐号进行密码找回：  截获返回数据报，查看返回的验证码信息，如下图：  输入返回验证码后即可重置该用户密码，截图如下： | |
| 处置建议 | 修改服务器实现代码，修复逻辑，验证码内容不予以回显，只返回状态信息即可 |
| 参考链接 | https://cwe.mitre.org/ |

## 4.2 xx系统

### 4.2.1 XXXX漏洞

|  |  |
| --- | --- |
| 漏洞级别-- | |
| 漏洞名称 | |
| URL/IP |  |
| 漏洞描述 |  |
| 风险描述 |  |
| 漏洞验证过程： | |
| 处置建议 |  |
| 参考链接 | 补丁链接、漏洞介绍链接等 |

### 4.2.2 XXXX漏洞

|  |  |
| --- | --- |
| 漏洞级别-- | |
| 漏洞名称 | |
| URL/IP |  |
| 漏洞描述 |  |
| 风险描述 |  |
| 漏洞验证过程： | |
| 处置建议 |  |
| 参考链接 | 补丁链接、漏洞介绍链接等 |

# 致谢

深信服安全服务团队感谢XXXXXX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。

# 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

公众号及微博：

 