



移动 APP 安全检测报告

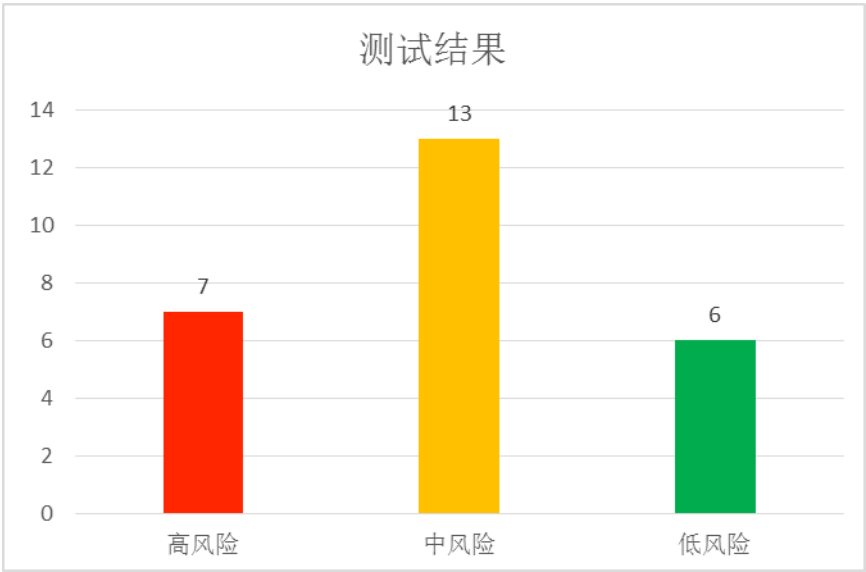
项目名称	xxxxAPP-安全测试-Android
项目编号	Testin_xxxx_20160714
送测单位	xxxx 有限公司
测试类型	安全测试

2016 年 7 月

报告摘要

本次 xxxxAPP Android 版的安全检测分别从七个方向进行，包括运行环境安全、应用安全、用户操作安全、数据安全、通信安全、业务安全、服务器端安全等，共 27 个安全检测用例。经检测发现：高风险问题 7 个，中风险问题 13 个，低风险问题 6 个，其中 1 个未测试项。如下图。

风险等级	数量
高安全风险问题	7
中安全风险问题	13
低安全风险问题	6



“xxxx” Android APP 安全检测结果汇总

测试用例	用例名称	测试项	测试结果	风险等级
4.1	环境安全检测	系统 root 检测	被测 APP 没有进行 Android 终端的 root 环境检测。	中
		网络代理安全检测	被测 APP 没有防网络代理操作。	中
4.2	应用安全检测	安装包逆向分析	被测 APP 能被实现反编译，代码没有进行混淆。在代码中发现大量的 URL 信息，并且在代码中发现有支付相关的密钥和邮箱信息。	高
		重打包检测	经检测发现被测 APP 可进行重打包处理。重打包后的 APP 可安装可运行。	高
		组件安全检测	经检测发现该 APP 的可攻击面为 7 个。其中有 2 个 Activity, 3 个 Broadcast Receiver, 2 个 service 可导出。	中
		软件运行日志检测	被测 APP 开启了日志调试功能，发现被测 APP 含有用户名、收货人名称、手机号、地址等敏感信息输出。	高
4.3	用户操作安全检测	弱口令检测	被测 APP 注册界面可输入纯六位的弱口令密码注册。被测 APP 没有严格的密码校验机制。	高
		密码找回安全检测	经检测发现被测 APP 找回密码过程中不存在任意密码重置风险。	低
		登录限制检测	经检测发现被测 APP 没有错误密码登录限制机制，攻击者可对系统存在的账户进行暴力破解攻击。	高
		密码保护机制检测	经检测发现被测 APP 登录页面切换到后台再切换回到登录页面时，密码输入框中的内容没有及时清空。	中
		验证码安全检测	被测 APP 的图形验证码是由客户端生成，在注册操作中，未经过服务端验证，存在验证绕过风险。	中
4.4	数据安全检测	键盘劫持检测	在被测 APP 界面上可以捕获到点击屏幕的坐标事件。	中
		防屏幕录制检测	被测 APP 在用户密码输入页面没有做防屏幕截屏操作，被测 APP 存在屏幕录制风险。	中
		信息显示安全	被测 APP 用户个人资料信息字符未经过隐蔽处理。	中
		本地存储安全检测	发现本地存储目录下的数据库文件中信息进行了加密处理。	中
		本地文件权限检测	发现本地存储有明文的用户的用户名、手机号码和用户 Id 等信息。	低

		数据清除检测	手机上卸载 APP 后，未发现残留有关于该 APP 的相关信息。	低
4.5	通信安全检测	传输协议分析	经检测发现被测 APP 使用了 HTTP 协议进行网络传输数据。且传输数据为明文传输。	高
		实体身份认证	发现被测 APP 使用的是 HTTP 协议，有使用安全协议进行认证。	中
		重放攻击检测	被测 APP 不存在短信模块，测试条件不足。	N/A
		会话超时检测	经检测发现被测 APP 没有严格的会话超时检测验证机制。	中
		断网会话检测	经检测发现被测 APP 在断网时没有相关提示。	中
4.6	业务安全检测	越权访问检测	被测 APP 在明显的越权访问风险。攻击者可通过修改数据包中的 UserId 字段非法获取他人的收货地址信息。	高
		信息提示检测	被测 APP 输入账户信息后进入主界面再切换到后台，发现被测 APP 没有相关提示。	中
		数据有效性检测	被测 APP 有相应的数据有效性校验。	低
4.7	服务器端安全检测	漏洞扫描检测	对服务器端 IP（115.xxx.xxx.xxx）使用工具进行漏洞扫描，未发现有高危漏洞。	低
		敏感信息泄露检测	查看从服务器端响应的数据未发现有关敏感信息泄露。	低

目 录

报告摘要.....	2
“XXXX” ANDROID APP 安全检测结果汇总	3
1 项目概述	7
1.1 项目背景	7
1.2 参考标准和规范	7
2 测试目标和内容	8
2.1 测试目标	8
2.2 测试内容	8
3 测试环境	9
3.1 网络环境	9
3.2 软硬件环境	9
3.3 测试工具平台	9
3.4 测试对象	9
4 检测过程	11
4.1 运行环境安全检测	11
4.1.1 系统 root 检测	11
4.1.2 网络代理安全检测	12
4.2 软件自身安全检测	13
4.2.1 安装包逆向分析	13
4.2.2 重打包检测	13
4.2.3 组件安全检测	14
4.2.4 软件运行日志检测	14
4.3 用户操作安全检测	14
4.3.1 弱口令检测	14
4.3.2 密码找回安全检测	14
4.3.3 登录限制检测	14
4.3.4 密码保护机制检测	14
4.3.5 验证码安全检测	14
4.4 数据安全检测	15
4.4.1 键盘劫持检测	15
4.4.2 防屏幕录制检测	15
4.4.3 信息显示安全检测	15
4.4.4 本地存储安全检测	15
4.4.5 本地文件权限检测	15
4.4.6 数据清除检测	15

4.5	通信安全检测	15
4.5.1	传输协议分析	15
4.5.2	实体身份认证	15
4.5.3	重放攻击检测	16
4.5.4	会话超时检测	16
4.5.5	断网会话检测	16
4.6	业务安全检测	16
4.6.1	越权访问检测	16
4.6.2	信息提示检测	16
4.6.3	数据有效性检测	16
4.7	服务器端安全检测	16
4.7.1	漏洞扫描检测	16
4.7.2	敏感信息泄露检测	16
5	附件	17
5.1	安全风险等级评定标准	17

1 项目概述

1.1 项目背景

随着移动互联网的发展，移动终端安全也越来越受到关注。特别是 Android 系统的崛起，互联网上的各类手机软件数量迅速上升。因 Android 系统是开源的，导致各种 Android 恶意软件迅猛增加，成为手机系统的最大受害者。与此同时，手机操作系统和软件本身的漏洞也进一步危害到用户的隐私安全。因此，有必要针对手机软件安全进行测评，进行常见的安全测试，评估手机软件安全的现状，为软件的安全改进提供建议，以提高手机相关软件的安全性。

1.2 参考标准和规范

- GB/T 18336-2008 信息技术 安全技术 信息技术安全性评估准则
- GB 17859-1999 计算机信息系统安全保护等级划分准则
- GB/T 20984-2007 信息安全技术 信息安全风险评估规范
- GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求
- GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求
- ISO/IEC 27001:2005 信息技术 信息安全管理体系要求

2 测试目标和内容

2.1 测试目标

利用科学的测试设计和有效的测试组织实施,分析评估和报告被测系统的整体安全保护状况,提交系统存在的安全问题,通过研发部门对于提交安全问题的修改,使系统达到一个稳定可靠的质量状态。

2.2 测试内容

测试内容包括 xxxx 移动应用客户端软件及通信链路安全性,结合当前安全漏洞与威胁现状,综合运用风险评估、技术测试等形式,对软件系统及网络安全进行检查。具体内容范围:运行环境安全、应用安全、用户操作安全、数据安全、通信安全、业务安全、服务器端安全等。

3 测试环境

3.1 网络环境

测试过程在真实网络环境下进行，测试使用到的手机和 PC 机均通过局域网连接到 Internet。

3.2 软硬件环境

Android 手机 4 台	
硬件环境	设备型号: 三星 SM-T111、华为荣耀 4A、三星 S6 Edge、魅蓝 Note、三星 note4
软件环境	操作系统: Android 4.2.2、Android5.1 应用软件: 测试工具集
PC 机 2 台	
硬件环境	设备型号: 联想 CPU: Intel Core i5-3210M 内存: 8GB DDR3 硬盘: 500GB
软件环境	操作系统: Win8.1 应用软件: 虚拟机 VMware, java 环境, 测试工具集

3.3 测试工具平台

序号	工具名称	备注
1.	移动应用安全检测平台	移动 APP 全自动化安全检测
2.	移动应用风险评估系统	结合检测规范和测试用例开发的平台

3.4 测试对象

被测对象描述表	
被测 APP 名称	xxxxx

APP 获取渠道	<p>下载地址：通过邮件获取 APK 包</p> 
APP 基本信息	



4 检测过程

4.1 运行环境安全检测

4.1.1 系统 root 检测

用例名称	系统 root 检测	执行时间	2016.07.14
测试内容	检测被测 APP 在 Android 设备 root 的环境下是否有安全检测并采取保护措施。Android 设备在 root 的情况下，系统安全性会大大的降低。		
测试过程	<p>1、将被测 APP 安装到一个已被 root 的移动设备上。</p>  <p>2、运行被测 APP，查看被测 APP 是否有 root 环境安全相关提示。发现被测 APP 操作登录的时候没有相关 root 环境安全风险提示操作。</p> 		
测试结果	被测 APP 没有进行 Android 终端的 root 环境检测。		
风险等级	中		
整改建议	在 APP 运行的时候应 xxxx，以防潜在安全漏洞。		

4.1.2 网络代理安全检测

用例名称	网络代理安全检测	执行时间	2016.07.14
测试内容	检测 APP 是否有启用手机防 HTTP 网络代理抓包机制。如果 APP 没启用防 HTTP 网络代理抓包机制，APP 在网络传输的数据包容易被中间人监听和篡改。		
测试过程	<p>1、将被测设备进行 WIFI 网络连接，设置 Android 设备 HTTP 网络代理。</p>  <p>2、使用风险评估系统的网络拦截工具代理被测 APP 所有的网络通信，发现 APP 没有相关的安全提示。</p>  <p>3、输入账号密码进行登录，通过网络抓包可以查看到传输的明文账号信息。</p> <p>图略</p>		
测试结果	被测 APP 没有防网络代理操作。		

风险等级	中
整改建议	APP 防网络代理操作可以从以下两个方面考虑： 1、对 APPxxxx。 2、不对 APPxxxx。

4.2 软件自身安全检测

4.2.1 安装包逆向分析

步骤省略

4.2.2 重打包检测

用例名称	重打包检测	执行时间	2016.07.14
测试内容	检测 APP 是否有防代码篡改和注入的安全问题。通过移动应用风险评估系统对 APK 反编译后进行重新签名打包然后进行安装。		
测试过程	<p>1、使用移动应用风险评估系统对被测 APP 进行重打包并签名操作，发现被测 APP 可以实现重打包。</p>  <p>2、将重打包后的 APP 安装到被测 Android 设备中，发现重打包的 APP 可安装可运行。</p> <p>图略</p>		
测试结果	经检测发现被测 APP 可进行重打包处理。重打包后的 APP 可安装可运行。		
风险等级	高		

整改建议	XXXX
------	------

4.2.3 组件安全检测

步骤省略

4.2.4 软件运行日志检测

步骤省略

4.3 用户操作安全检测

4.3.1 弱口令检测

步骤省略

4.3.2 密码找回安全检测

步骤省略

4.3.3 登录限制检测

步骤省略

4.3.4 密码保护机制检测

步骤省略

4.3.5 验证码安全检测

步骤省略

4.4 数据安全检测

4.4.1 键盘劫持检测

步骤省略

4.4.2 防屏幕录制检测

步骤省略

4.4.3 信息显示安全检测

步骤省略

4.4.4 本地存储安全检测

步骤省略

4.4.5 本地文件权限检测

步骤省略

4.4.6 数据清除检测

步骤省略

4.5 通信安全检测

4.5.1 传输协议分析

步骤省略

4.5.2 实体身份认证

步骤省略

4.5.3 重放攻击检测

步骤省略

4.5.4 会话超时检测

步骤省略

步骤省略

4.5.5 断网会话检测

步骤省略

4.6 业务安全检测

4.6.1 越权访问检测

步骤省略

4.6.2 信息提示检测

步骤省略

4.6.3 数据有效性检测

步骤省略

4.7 服务器端安全检测

4.7.1 漏洞扫描检测

步骤省略

4.7.2 敏感信息泄露检测

步骤省略

5 附件

5.1 安全风险等级评定标准

序号	风险等级	评定标准说明（符合以下条件之一）
1	低	1) 未发现明显的安全问题； 2) 未偏离相关国家行业标准规范要求； 3) 安全漏洞的利用不会对系统造成明显的安全隐患（如通过安全漏洞的利用只会获取系统组件的某些信息）； 4) 与以上相当危害程度的其他安全漏洞。
2	中	1) 偏离国家行业相关标准规范要求并且该项偏离会造成部分信息暴露等问题但不会直接引发严重问题（如读取后台数据库）； 2) 安全漏洞的利用会对系统造成一定的影响（如获得通信过程中的某些非明感信息）； 3) 安全漏洞的利用虽会对系统造成严重影响但很不容易利用； 4) 与以上相当危害程度的其他安全漏洞。
3	高	偏离国家行业相关标准规范要求并且该项偏离会直接引发严重问题（如获得程序源代码、可远程读写系统文件或操纵后台数据、可远程以普通用户身份执行命令或进行拒绝服务攻击、可远程以管理用户身份执行命令、可大量攻击用户造成恶劣影响等）； 安全漏洞的利用会对系统造成严重影响且容易利用（如获得程序源代码、可远程读写系统文件或操纵后台数据、可远程以普通用户身份执行命令或进行拒绝服务攻击、可远程以管理用户身份执行命令、可大量攻击用户造成恶劣影响等）； 与以上相当危害程度的其他安全漏洞。