四维创智

猎奇
移动应用安全风险检测报告

- 检测时间：2018-10-16 09:04:41
- 引擎版本： 3.猎奇0.0
- 适用系统： Android

目录

1 检测依据

《信息安全技术移动智能终端个人信息保护技术要求》

《YD/T 1438-2006 数字移动台应用层软件功能要求和测试方法》

《YD/T 2307-2011 数字移动通信终端通用功能技术要求和测试方法》

《电子银行业务管理办法》

《电子银行安全评估指引》

《中国金融移动支付客户端技术规范》

《中国金融移动支付应用安全规范》

《移动互联网应用软件安全评估大纲》

《中华人民共和国网络安全法》

《移动互联网应用程序信息服务管理规定》

2 检测结果

84

应用名：恶意程序示例　　包名：com.hijack_activity　　大小：1.94MB

MD5值：51f44f8f8edb7b69dcfde50f68e35226

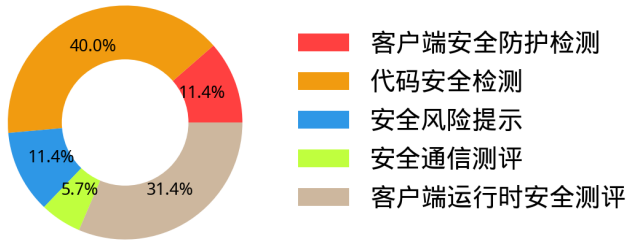
Sha1值：536cafdf30f37d8d6e099595229c9a9258894439

2.1 检测结果综述

漏洞级别

高危漏洞	3
中危漏洞	7
低危漏洞	1
检测项总数	74

漏洞类型



2.2 检测项汇总

序号	检测项	检测结果
1	开启单元测试	安全
2	可被导出的Service组件	高危
3	可被导出的Content Provider组件	安全
4	服务器证书校验	安全
5	隐藏的启动代码	安全
6	使用反射调用	安全
7	使用加密函数	安全
8	加载dex文件	安全
9	Webview 密码明文保存	安全
10	打印调试日志	安全
11	Email扫描	安全
12	初始化IvParameterSpec漏洞	安全
13	应用可被调试风险	安全
14	Content Provider目录遍历漏洞	安全

15	可被导出的Activity组件	安全
16	全局可写的内部文件（运行时）	安全
17	联系人查询	安全
18	允许任意调试	中危
19	加载远端jar文件	安全
20	对外暴露的Content Provider接口（可被攻击）	安全
21	模拟器检测	安全
22	使用混淆保护	中危
23	URL扫描	中危
24	使用SQLite数据库	安全
25	使用进程间通信（IPC）	低危
26	Webview远程代码执行	安全
27	冗余权限引用	中危
28	html页面感染检测	安全
29	第三方sdk密钥泄漏	安全
30	Activity组件劫持检测	安全
31	使用udp通信	安全
32	本地动态加载	安全
33	可被导出的Broadcast Recevier组件	安全
34	调试检测	安全
35	应用内授权信息	安全
36	不安全地载入任务栈	安全
37	寄生推高风险SDK	安全
38	指定的Activity加载模式	安全
39	可被导出的Activity组件	安全
40	intent scheme url漏洞	安全
41	篡改检测	安全
42	客户端证书绑定	安全
43	Webview禁用SSL错误	安全
44	短信操作	安全
45	执行系统命令	安全
46	Webview远程调试开启	安全
47	对外部存储卡进行读写	安全
48	应用克隆漏洞	安全
49	Janus签名机制绕过漏洞	高危
50	拥有较高优先级的组件	安全

51	so注入检测	安全
52	Zip文件目录遍历漏洞	安全
53	获得SIM卡信息	安全
54	安全加固检测	中危
55	代码硬编码敏感信息	安全
56	自定义短信接收端口	安全
57	使用堆栈保护技术	安全
58	获得手机信息	安全
59	通讯安全测试	高危
60	使用原生层代码	安全
61	Pending Intent 劫持风险	中危
62	使用Webview控件加载HTTP内容	安全
63	二次打包检测	安全
64	应用信任所有证书	安全
65	全局可读写的内部文件	安全
66	本地SQL注入	安全
67	编译时使用PIE标记	安全
68	设备root检测	安全
69	获得手机位置	安全
70	调用内部或隐藏api	安全
71	特定敏感词汇检测	安全
72	允许任意备份	中危
73	处于测试模式	安全
74	使用不安全的随机函数	安全

3 检测详情

3.1 APP基础信息

3.1.1、应用签名信息

所有者	C=US, O=Android, CN=Android Debug
发布者	C=US, O=Android, CN=Android Debug
序列号	[01]

起始日期	19 CST 2017,
截至日志	19 CST 2047]
证书内容	['0000: 94 DC 58 B6 49 6E 3D 35 41 42 64 F4 2D 25 CE C1 ..X.In=5ABd.-%..', '0010: D4 2E BA 87 B9 FB FA A1 D3 25 59 D0 F9 32 EF 3D .....%Y..2.=', '0020: 95 9D B0 00 6A 13 D8 FB 92 F0 28 20 BB 06 C3 62 ....j.....(...b', '0030: 5A 78 94 84 19 FE DE 17 C9 2F 6E 41 6A 9E 62 BA Zx...../nAj.b.', '0040: 30 47 C2 A7 48 20 C1 3F 55 51 C8 31 1E 7A 6B A3 0G..H .?UQ.1.zk.', '0050: 77 89 65 AD 4D 57 22 DF 0F 69 BD FE 6C B7 86 94 w.e.MW"..i..l...', '0060: 8E 76 B3 BC 2E 2D A8 31 3A 6A 8D 63 35 16 48 A6 .v...-.1:j.c5.H.', '0070: E8 39 F8 75 1F 7E 4A A1 9B 53 FB B2 FD 57 56 12 .9.u..J..S...WV.']
签名算法及名称	SHA1withRSA, OID = 1.2.840.113549.1.1.5
版本	V1

3.1.2、应用权限信息

权限	描述	等级
GET_TASKS	获取正在运行的应用程序	危险
RECEIVE_BOOT_COMPLETED	开机自启动	常规

3.1.3、第三方sdk信息

图标	名称	类型	评估
未检测到应用集成第三方sdk			

3.2 安全通信测评

3.2.1、服务器证书校验

检测目的	检测客户端是否对通信的服务端进行证书校验。
威胁描述	服务器和客户端使用HTTPS协议进行连接时，客户端必须对服务器证书进行强校验，如签名CA是否合法、证书是否是自签名、主机域名是否匹配、证书是否过期等，以验证服务器是真实合法的目标服务器。如果未校验，客户端可能与仿冒的服务器建立通信链接，同时服务端也可能与仿冒的客户端建立通信链接，即“中间人攻击”。攻击者可以冒充中间人，在客户端和服务端中间转发信息，窃取账号、密码等敏感信息。
检测结果	安全
结果描述	经检测,代码中包含服务端证书校验相关代码
检测详情	无
修复建议	无

3.2.2、客户端证书绑定

检测目的	检测客户端是否绑定证书。

威胁描述	若客户端证书没有直接绑定，则会使用系统信任的证书颁发机构颁发的证书。只要攻击者将自己的证书导入到被攻击者的手机中，即可窃取篡改被攻击者与服务端的通信数据
检测结果	安全
结果描述	经检测,代码中包含客户端证书绑定
检测详情	无
修复建议	无

3.2.3、通讯安全测试

检测目的	检测客户端是否使用安全的加密信道传输数据。
威胁描述	若应用直接使用HTTP协议或者SSL v3以下版本通信，进行登录账户或交换数据等业务操作，可能会引发数据信息泄露。建议使用TLS v1.2以上版本协议通信。
检测结果	高危
结果描述	经检测，应用未使用https安全的加密信道
检测详情	未检测到应用采用https安全信道
修复建议	建议使用SSL v3以上版本进行通信

3.2.4、应用信任所有证书

检测目的	检测应用是否信任所有证书
威胁描述	使用HTTPS协议进行通信时，客户端必须对服务端证书的完整性进行校验，防止攻击者通过伪造证书窃取和篡改通信数据
检测结果	安全
结果描述	经检测，应用不存在信任所有证书漏洞
检测详情	无
修复建议	无

3.3 客户端运行时安全测评

3.3.1、可被导出的Service组件

检测目的	检测应用的 Service 组件是否能被第三方程序调用
威胁描述	Service执行的操作比较敏感，比如更新数据库、提供事件通知等，如果设置了导出权限，可能被系统或者第三方的App直接调出并使用。暴露的Service组件可能导致权限提升，service劫持，消息伪造，拒绝服务攻击等风险。
检测结果	高危
结果描述	经检测，应用有可被导出的service组件

检测详情	com.hijack_activity.MyService
修复建议	只被应用本身使用的service应设置为私有;service接收到的数据需谨慎处理等

3.3.2、可被导出的Content Provider组件

检测目的	检测登录状态下的 Provider 组件能否被第三方程序调用,且出现文件下载、权限提升或者敏感信息泄露等安全风险。
威胁描述	Content Provider组件设置为可导出会允许攻击者在外部调用Content Provider组件时，可能会导致敏感信息泄漏，sql注入，目录遍历漏洞等
检测结果	安全
结果描述	经测试,对外暴露的 Content URI 接口不能进行查询操作
检测详情	无
修复建议	无

3.3.3、加载dex文件

检测目的	检测应用是否运行时加载了dex文件
威胁描述	应用利用类加载机制在运行时加载dex文件。攻击者可以针对dex文件进行伪造和替换，向应用植入恶意代码，窃取信息或盗用计算资源
检测结果	安全
结果描述	经检测,应用未动态加载dex
检测详情	无
修复建议	无

3.3.4、应用可被调试风险

检测目的	检测 APK 是否能够利用 GDB、IDA 等调试器对应用程序进行动态调试。
威胁描述	调试通常是恶意攻击者针对应用发起攻击时信息收集的重要手段，恶意程序或者人工可以通过动态调试技术，对程序进行内存调试跟踪，可以窃取目标进程的数据信息，从而获取用户的隐私数据信息
检测结果	安全
结果描述	应用不存在可被调试风险
检测详情	无
修复建议	无

3.3.5、Content Provider目录遍历漏洞

检测目的	检测应用是否存在Content Provider目录遍历漏洞
威胁描述	对外暴露的Content Provider组件实现了openFile()接口，并且没有对Content Provider组件的访问进行权限控制，也没有对访问的目标文件的Uri进行有效判断，第三方应用程序可以利用该接口进行文件目录遍历，访问任意可读

	文件
检测结果	安全
结果描述	应用不存在Content Provider目录遍历漏洞
检测详情	无
修复建议	无

3.3.6、可被导出的Activity组件

检测目的	检测可导出Activity组件安全问题
威胁描述	攻击者向Intent中传入其自定义的序列化类对象，当调用组件收到此Extra序列化类对象时，应用开发者没有对传入的数据做异常判断，导致应用崩溃。本地拒绝服务漏洞不仅可以导致防护应用的防护功能被绕过或失效（如杀毒应用、安全卫士、防盗锁屏等），也可以导致应用被大面积攻击而崩溃，造成不同程度的经济利益损失。
检测结果	安全
结果描述	未发现可导出组件存在安全问题
检测详情	无
修复建议	无

3.3.7、加载远端jar文件

检测目的	检测应用是否远程调用了jar文件
威胁描述	应用可以通过JarURLConnection远程调用jar文件，但是当这个过程被攻击者劫持，或jar文件被攻击者替换为恶意文件时，将会导致攻击者在本地插入恶意代码，获取本地权限和任意代码执行。
检测结果	安全
结果描述	经检测,应用未远程调用jar
检测详情	无
修复建议	无

3.3.8、对外暴露的Content Provider接口（可被攻击）

检测目的	检测登录状态下的 Provider 组件能否被第三方程序调用。
威胁描述	Content Provider被用于在不同应用程序或者进程之间共享数据，而应用程序的不同数据内容应该具有严格的访问权限。如果权限设置不当，应用程序的Content Provider数据可能被其他程序直接访问或者修改，导致用户的敏感数据泄露，或者应用数据被恶意篡改，例如盗取账号信息，修改支付金额等。
检测结果	安全
结果描述	应用不存在可被攻击的Content Provider接口
检测详情	无
修复建议	无

3.3.9、使用SQLite数据库

检测目的	检测应用是否使用SQLite数据库
威胁描述	在sqlite数据库中明文存储的敏感信息可能被恶意软件轻易读取
检测结果	安全
结果描述	经检测，应用不存在使用SQLite数据库风险
检测详情	无
修复建议	无

3.3.10、使用进程间通信（IPC）

检测目的	检测应用是否使用了进程间通信
威胁描述	Android系统为每个应用分配了一个独立的虚拟机，或者说为每一个进程都分配一个独立的虚拟机，不同的虚拟机在内存分配上有不同的地址空间，这就导致在不同的虚拟机中访问同一个对象会产生多分副本。此时进行进程间通信将可能导致沙箱机制失效、应用拒绝服务等风险。
检测结果	低危
结果描述	经检测，应用进程间通信存在一定风险
检测详情	/android/support/v4/app/ShareCompat$ShareCompatImpl.java 6, ' * android.support.v4.app.ShareCompat$IntentBuilder' 15, ' public void configureMenuItem(MenuItem var1, ShareCompat.IntentBuilder var2);' /android/support/v4/app/TaskStackBuilder$SupportParentable.java 5, ' * android.content.Intent' 9, 'import android.content.Intent;' 12, ' public Intent getSupportParentActivityIntent();' /android/support/v4/app/TaskStackBuilder$TaskStackBuilderImpl.java 5, ' * android.app.PendingIntent' 7, ' * android.content.Intent' 12, 'import android.app.PendingIntent;' 14, 'import android.content.Intent;' 18, ' public PendingIntent getPendingIntent(Context var1, Intent[] var2, int var3, int var4, Bundle var5);' /android/support/v4/app/NavUtils$NavUtilsImpl.java 7, ' * android.content.Intent' 14, 'import android.content.Intent;' 18, ' public Intent getParentActivityIntent(Activity var1);' 22, ' public void navigateUpTo(Activity var1, Intent var2);' 24, ' public boolean shouldUpRecreateTask(Activity var1, Intent var2);' /android/support/v4/content/IntentCompat$IntentCompatImpl.java 6, ' * android.content.Intent' 11, 'import android.content.Intent;' 13, 'interface IntentCompat$IntentCompatImpl {' 14, ' public Intent makeMainActivity(ComponentName var1);' 16, ' public Intent makeMainSelectorActivity(String var1, String var2);' 18, ' public Intent makeRestartActivityTask(ComponentName var1);'
修复建议	在进行进程间通信时严格校验身份与参数

3.3.11、第三方sdk密钥泄漏

检测目的	检测应用是否明文泄漏了第三方sdk密钥
威胁描述	开发者经常会使用第三方sdk来加速应用的开发，但有时在与第三方sdk进行认证时，可能会泄漏sdk的认证密钥
检测结果	安全
结果描述	经检测,应用不存在第三方sdk密钥泄漏
检测详情	无
修复建议	无

3.3.12、本地动态加载

检测目的	测试应用是否动态加载dex文件
威胁描述	Anroid4.1之前的系统版本容许Android应用将动态加载的DEX文件存储在被其他应用任意读写的目录中(如sdcard)，这样只要攻击者指定加载一个恶意的dex，或将原有的dex替换为恶意的dex，即可达到恶意代码注入的目的，产生安全风险。
检测结果	安全
结果描述	经检测,代码中未使用本地动态加载
检测详情	无
修复建议	无

3.3.13、可被导出的Broadcast Recevier组件

检测目的	检测 Receiver 组件是否能被第三方程序调用
威胁描述	从全局考虑Broadcast Receiver可以方便应用程序和系统、应用程序之间、应用程序内的通信，对单个应用程序而言Broadcast Receiver是存在安全性问题的，比如恶意程序可以不断的去发送你所接收的广播，这样会造成敏感信息泄漏，权限绕过，消息伪造，拒绝服务等风险。
检测结果	安全
结果描述	经检测，应用没有可被导出的Broadcast Receiver组件
检测详情	无
修复建议	无

3.3.14、调试检测

检测目的	检测应用是否采取了防护应用被调试的措施
威胁描述	调试检测机制可以阻止攻击者利用GDB、Ptrace等调试器跟踪运行程序，查看、修改内存中的代码和数据等行为。保护客户的关键数据以及服务器的信息安全，增加攻击者的攻击成本。
检测结果	安全
结果描述	经检测，应用具备防护应用被调试的能力
检测详情	无

修复建议	无

3.3.15、可被导出的Activity组件

检测目的	检测应用的 Activity 组件能否被第三方程序调用
威胁描述	Activity组件设置导出权限，则该组件能够被外部的其他组件直接调用，这样就可能导致泄露隐私数据或者应用程序崩溃等风险。Activity被恶意应用调用，可能有以下威胁描述：修改程序的状态或者数据；被调用的Activity可能返回隐私信息给恶意应用，造成数据泄露；可能使应用程序崩溃，造成拒绝服务等漏洞。
检测结果	安全
结果描述	经检测，应用没有可被导出的Activity组件
检测详情	无
修复建议	无

3.3.16、对外部存储卡进行读写

检测目的	检测应用是否存在对外部存储卡进行读写
威胁描述	使用外部存储实现数据持久化，这里的外部存储一般就是指SD卡。使用SD卡存储的数据，不仅本应用访问，任何有访问SD卡权限的应用均可以访问。如果在SD卡上存储账号、密码等敏感信息，容易导致信息泄漏。
检测结果	安全
结果描述	经检测，应用不存在对外部存储卡进行读写风险
检测详情	无
修复建议	无

3.3.17、Janus签名机制绕过漏洞

检测目的	检测应用是否存在Janus签名机制绕过漏洞
威胁描述	由于安卓的signature scheme V1签名机制并未考虑ART运行环境下直接安装dex的情况，使得攻击者可以通过将dex附在原安装包后面的方式绕过安卓自身的签名校验，任意安装恶意程序。 如果应用使用1.0版签名，则在安卓5.0以上的环境下存在应用签名被绕过，应用被恶意替换的安全风险。
检测结果	高危
结果描述	检测到应用存在Janus签名机制绕过漏洞
检测详情	Signature-Version: 1.0
修复建议	使用V2.0或以上的模式对APP进行签名

3.3.18、so注入检测

检测目的	检测应用是否可以so注入
威胁描述	Android动态代码注入是不修改源程序只修改目标进程的寄存器、内存值等就能控制程序实现既定目标的一种方法。通过动态注入，攻击者可以劫持目标进程函数、窃取目标进程数据、篡改目标进程数据等，从而监控程序运

	行、获取敏感信息等。常见的动态注入，可以获取登录账号、密码等。
检测结果	安全
结果描述	应用对so注入做了防护
检测详情	无
修复建议	无

3.3.19、使用Webview控件加载HTTP内容

检测目的	检测应用是否使用Webview加载HTTP内容
威胁描述	使用Webview组件的应用通常调用系统自身的HTML解析器，在面临跨站点脚本攻击、远程代码执行等攻击方式时具有明显的弱势。
检测结果	安全
结果描述	经检测,应用未使用Webview加载HTTP内容
检测详情	无
修复建议	无

3.3.20、全局可读写的内部文件

检测目的	检测应用是否存在可被其它程序任意读取和修改的文件
威胁描述	为了实现不同软件之间的数据共享，设置内部文件为全局可读或全局可写，导致其他应用可以读取和修改该文件。攻击者可以读取此文件内容，获取文件中关键配置信息、账户信息数据等敏感信息，可能会被盗取或者恶意篡改，导致程序无法运行、业务逻辑被修改等问题。
检测结果	安全
结果描述	经检测，应用不存在可被其它程序任意读取和修改的文件
检测详情	无
修复建议	无

3.3.21、本地SQL注入

检测目的	检测应用是否存在本地sql注入。
威胁描述	由于Content Provider组件读写权限设置不当，并且未对SQL查询语句的字段参数作过滤判断，应用本地数据库可能被注入攻击。可能导致存储的敏感数据信息被查询泄露，例如用户名、密码等，或者产生查询异常导致应用崩溃。
检测结果	安全
结果描述	应用不存在本地SQL注入风险
检测详情	无
修复建议	无

3.3.22、调用内部或隐藏api

检测目的	检测应用是否存在调用内部或隐藏的api风险
威胁描述	应用调用了安卓系统内部的或隐藏的api，这些api一般由于权限过高或未开发完成而没有开放给应用直接调用，调用这些api可能降低应用稳定性
检测结果	安全
结果描述	经检测，应用未调用内部或隐藏的api
检测详情	无
修复建议	无

3.4 代码安全检测

3.4.1、开启单元测试

检测目的	检测应用是否关闭单元测试
威胁描述	应用未关闭AndroidManifest中的单元测试选项，可能导致泄露敏感信息，客户端功能暴露，使得攻击者可以轻易获得应用的执行逻辑。
检测结果	安全
结果描述	经检测，应用不正常关闭单元测试
检测详情	无
修复建议	无

3.4.2、隐藏的启动代码

检测目的	检测应用是否存在隐藏的启动代码风险
威胁描述	在data标签中使用 android_secret_code 来处理Android的隐形字符串（形如输入#*800800*#开启超级用户模式等）。而隐形字符串的泄漏可能导致大面积的信息泄露或权限控制失效
检测结果	安全
结果描述	经检测，应用不存在隐藏的启动代码风险
检测详情	无
修复建议	无

3.4.3、使用反射调用

检测目的	检测应用代码是否使用反射调用
威胁描述	应用若使用反射调用运行机制，则可能存在调用数据不可控的原因而造成的远程代码执行漏洞。

检测结果	安全
结果描述	经检测,代码中未使用反射调用
检测详情	无
修复建议	无

3.4.4、使用加密函数

检测目的	检测应用使用加密函数
威胁描述	检测应用是否对敏感数据加密后再进行存储。在客户端中对需要传输和存储的数据进行加密，可以很好的保护敏感数据的机密性，极大增加攻击者获取敏感数据的攻击成本。
检测结果	安全
结果描述	经检测,代码中使用了加密函数
检测详情	无
修复建议	无

3.4.5、Webview 密码明文保存

检测目的	检测应用是否存在Webview密码明文保存漏洞
威胁描述	WebView组件默认开启了密码保存功能，会提示用户是否保存密码，当用户选择保存在WebView中输入的用户名和密码，则会被明文保存到应用数据目录的databases/webview.db中。攻击者可能通过root的方式访问该应用的WebView数据库，从而窃取本地明文存储的用户名和密码。
检测结果	安全
结果描述	经检测，应用不存在Webview密码明文保存风险
检测详情	无
修复建议	无

3.4.6、打印调试日志

检测目的	检测应用是否打印调试日志
威胁描述	调试信息函数可能输出重要的调试信息，其中包含的信息可能导致用户信息泄露，泄露核心代码逻辑等，为发起攻击提供便利，例如：Activity的组件名；通信交互的日志；跟踪的变量值等。
检测结果	安全
结果描述	经检测，应用不存在打印调试日志风险
检测详情	无
修复建议	无

3.4.7、Email扫描

检测目的	检测应用是否存在测试时留存的email信息
威胁描述	开发人员有时会在开发时将email信息硬编码到代码中方便使用，而在发布时未删除这部分email信息可能导致开发人员信息泄漏，或导致应用运行逻辑外泄。
检测结果	安全
结果描述	经检测,应用中未发现email信息
检测详情	无
修复建议	无

3.4.8、初始化IvParameterSpec漏洞

检测目的	检测应用是否存在初始化IvParameterSpec漏洞
威胁描述	使用固定初始化向量，结果密码文本可预测性会高得多，容易受到字典式攻击。
检测结果	安全
结果描述	经检测，应用不存在初始化IvParameterSpec漏洞
检测详情	无
修复建议	无

3.4.9、允许任意调试

检测目的	检测应用是否允许任意调试。
威胁描述	允许任意调试的应用程序可以给攻击者提供很方便的调试接口，授予其访问、修改运行时的敏感数据的权限，对业务和个人信息带来安全隐患。此属性由AndroidManifest.xml中debuggable属性控制。应用配置文件AndroidManifest.xml中的调试标记开启，可被Java调试工具如JDB进行调试，获取和篡改用户敏感信息，甚至可以分析并且修改代码实现的业务逻辑，例如窃取用户密码、绕过验证码防护等。
检测结果	中危
结果描述	经检测，客户端配置文件中开启了任意调试模式
检测详情	[b'']
修复建议	建议将AndroidManifest.xml文件中的debugable属性置为False

3.4.10、URL扫描

检测目的	扫描应用中出现的url
威胁描述	扫描应用中出现url信息。
检测结果	中危
结果描述	检测到应用泄漏url信息
	data:landroid/os/bundle;

检测详情	data:ljava/lang/object; data:z
修复建议	无

3.4.11、Webview远程代码执行

检测目的	检测应用是否存在WebView远程代码执行漏洞。
威胁描述	Android API level 17以及之前的版本，由于程序没有正确限制使用addJavascriptInterface方法，远程攻击者可通过使用Java Reflection API利用该漏洞执行任意Java对象的方法。通过addJavascriptInterface给WebView加入一个 JavaScript桥接接口，JavaScript通过调用这个接口可以直接与本地的Java接口进行交互。导致手机被安装木马程序，发送扣费短信，通信录或者短信被窃取，甚至手机被远程控制。
检测结果	安全
结果描述	经检测，应用不存在Webview远程代码执行
检测详情	无
修复建议	无

3.4.12、冗余权限引用

检测目的	检测应用是否存在声明权限未被使用的风险。
威胁描述	应用程序引用了不必要的权限
检测结果	中危
结果描述	检测到应用存在声明权限未被使用的问题
检测详情	android.permission.RECEIVE_BOOT_COMPLETED
修复建议	依据最小权限原则，不需要的权限不再声明

3.4.13、应用内授权信息

检测目的	检测应用是否存在应用内授权信息
威胁描述	应用内定义了涉及付费的操作以及可能涉及到用户隐私的操作，具有较高的风险系数
检测结果	安全
结果描述	经检测，应用不存在应用内授权信息风险
检测详情	无
修复建议	无

3.4.14、不安全地载入任务栈

检测目的	检测应用是否指定了Activity加载模式

威胁描述	攻击者精心设计恶意Activity覆盖原有的Activity
检测结果	安全
结果描述	经检测，应用指定了Activity加载模式
检测详情	无
修复建议	无

3.4.15、指定的Activity加载模式

检测目的	检测应用是否直接调用启动activity
威胁描述	直接调用启动activity
检测结果	安全
结果描述	经检测，应用没有直接调用启动activity
检测详情	无
修复建议	无

3.4.16、intent scheme url漏洞

检测目的	检测应用是否存在intent scheme url 漏洞
威胁描述	Intent Scheme URL是一种特殊的URL格式，用来通过Web页面启动已安装应用的Activity组件。如果过滤规则缺失，攻击者利用Intent scheme URLs可以通过web js代码进行一些恶意行为，比如盗取cookie、启动应用等等。攻击者也可以构造特殊格式的URL直接向系统发送意图，启动应用的Activity组件或者发送异常数据，导致应用的敏感信息泄露或者应用崩溃。
检测结果	安全
结果描述	经检测，应用不存在intent scheme url 漏洞
检测详情	无
修复建议	无

3.4.17、Webview禁用SSL错误

检测目的	检测应用是否存在Webview忽略SSL证书错误漏洞。
威胁描述	Android WebView组件加载使用HTTPS协议加密的网页时，如果服务端校验证书错误，客户端应该拒绝加载网页。但是如果发生证书认证错误时，调用WebViewClient类的onReceivedSslError方法，并在该方法实现中调用了handler.proceed()来忽略该证书错误，则客户端会绕过证书校验错误继续加载此网页。这样会导致“中间人攻击”，攻击者可以冒充中间人，在客户端和服务端中间转发信息，窃取账号、密码等敏感信息。
检测结果	安全
结果描述	经检测，应用不存在Webview忽略SSL证书错误
检测详情	无

修复建议	无

3.4.18、执行系统命令

检测目的	检测应用是否存在执行系统命令风险
威胁描述	直接在java层执行系统命令将有可能被恶意软件利用，帮助攻击者打通攻击链，获取更高权限，进行更有破坏力的操作
检测结果	安全
结果描述	经检测，应用不存在执行系统命令风险
检测详情	无
修复建议	无

3.4.19、Webview远程调试开启

检测目的	检测应用是否存在WebView远程调试开启漏洞。
威胁描述	远程调试设置为开启状态，恶意攻击者将可以远程对webview及相关的h5文件进行调试，造成信息泄露或远程控制
检测结果	安全
结果描述	经检测，应用不存在Webview远程调试开启风险
检测详情	无
修复建议	无

3.4.20、应用克隆漏洞

检测目的	检测是应用否存在应用克隆风险
威胁描述	该漏洞主要对使用了webview控件，开启file域访问且未按安全策略开发的Android应用app造成影响
检测结果	安全
结果描述	检测到应用不存在应用克隆漏洞
检测详情	无
修复建议	无

3.4.21、拥有较高优先级的组件

检测目的	检测应用是否存在拥有较高优先级的组件
威胁描述	组件设置了一个较高优先级的过滤器，而这个组件可能被恶意程序利用，达到提权的目的
检测结果	安全

结果描述	经检测，应用不存在拥有较高优先级的组件风险
检测详情	无
修复建议	无

3.4.22、Zip文件目录遍历漏洞

检测目的	检测应用编译时是否具有zip文件目录遍历漏洞
威胁描述	使用ZipEntry.getName()解压zip文件，没有对上级目录字符串(../)进行过滤校验，可能会导致被解压的文件发生目录跳转，解压到其他目录，并且覆盖相应的文件，最终导致任意代码执行
检测结果	安全
结果描述	应用不存在zip文件目录遍历风险
检测详情	无
修复建议	无

3.4.23、代码硬编码敏感信息

检测目的	检测应用是否存在代码硬编码敏感信息
威胁描述	应用的加密密钥、邮箱、内网地址路径等应该被单独加密的信息直接在代码中用其他编码转码处理，当攻击者对应用进行反编译后将会轻易地获得这部分敏感信息，为攻击者的后续渗透工作提供便利
检测结果	安全
结果描述	经检测，应用不存在代码硬编码敏感信息
检测详情	无
修复建议	无

3.4.24、获得手机信息

检测目的	检测应用是否获得手机信息
威胁描述	部分恶意应用通过获得手机信息来对机主信息进行收集和识别
检测结果	安全
结果描述	经检测,应用中未发现收集收集信息
检测详情	无
修复建议	无

3.4.25、Pending Intent 劫持风险

检测目的	检测应用是否存在Pending Intent调用风险

威胁描述	隐式调用Intent能够在不同应用间传递数据，但并未对Intent消息接收端进行限制，可能存在该消息被第三方应用劫持的风险。可能造成的风险包括：恶意调用，恶意接收数据；仿冒应用，例如（恶意钓鱼，启动登录界面）；恶意发送广播；启动应用服务；调用组件，接受组件返回的数据；拦截有序广播。
检测结果	中危
结果描述	经检测，应用存在Pending Intent 劫持风险
检测详情	[{'path': '/android/support/v4/app/TaskStackBuilder$TaskStackBuilderImpl.java', 'lines': [(5, ' * android.app.PendingIntent'), (12, 'import android.app.PendingIntent;'), (18, ' public PendingIntent getPendingIntent(Context var1, Intent[] var2, int var3, int var4, Bundle var5);')]}]
修复建议	建议移除应用的Pending Intent对象

3.4.26、允许任意备份

检测目的	检测应用是否允许任意备份
威胁描述	Android系统提供了为应用程序数据的备份和恢复功能，该功能由AndroidMainfest.xml文件中的allowBackup属性值控制，其默认值为true。当该属性没有显式设置为false时，恶意攻击者可以通过adb的restore命令备份应用程序，进而获得用户的敏感信息。
检测结果	中危
结果描述	经检测，应用存在允许任意备份风险
检测详情	[b'']
修复建议	在AndroidManifest.xml中显式地将AllowBackup属性设置为False

3.4.27、处于测试模式

检测目的	检测应用是否处于测试模式下
威胁描述	AndroidManifest.xml文件中的testOnly属性被置为True，使得应用程序处于测试模式，可能会暴露一些不属于自己的功能或数据，这将引发安全漏洞。且这种应用程序只能通过adb进行安装。
检测结果	安全
结果描述	经检测,客户端配置文件中未指定开启测试模式。
检测详情	无
修复建议	无

3.4.28、使用不安全的随机函数

检测目的	检测应用是否存在不安全的随机函数漏洞
威胁描述	在SecureRandom生成随机数时，如果我们不调用setSeed方法，SecureRandom会从系统中找到一个默认随机源。每次生成随机数时都会从这个随机源中取seed。不安全的使用方式会导致SecureRandom使用相同的种子生成随机数，每次生成随机数时也是相同的。该漏洞存在于Android系统随机生成数字串安全密钥的环节中。这会导致使用的随机数或加密算法被破解
检测结果	安全
结果描述	经检测，应用不存在不安全的随机函数使用

检测详情	无
修复建议	无

3.5 客户端安全防护检测

3.5.1、模拟器检测

检测目的	检测 APK 是否能够在模拟器中运行
威胁描述	对于运行在模拟器中的应用程序，攻击者可以从里到外地分析该应用的行为特征、流量数据、代码逻辑等。而除了部分游戏应用外，大部分的应用在正常使用时都不会运行在模拟器环境中。因此建议增加模拟器检测，增加攻击者的攻击成本。
检测结果	安全
结果描述	经检测，应用对在模拟器上运行进行了有效防护
检测详情	无
修复建议	无

3.5.2、使用混淆保护

检测目的	测试应用是否采用混淆保护
威胁描述	应用程序对代码部分的变量和运行逻辑使用混淆保护，可以防止恶意攻击者分析该应用程序，增加攻击者的攻击成本。
检测结果	中危
结果描述	经检测，应用未使用混淆保护技术
	检测到未进行混淆的文件 /summary.txt /android/support/v4/media/TransportMediatorCallback.java /android/support/v4/accessibilityservice/AccessibilityServiceInfoCompat$AccessibilityServiceInfoVersionImpl.java /android/support/v4/os/ParcelableCompatCreatorCallbacks.java /android/support/v4/app/ShareCompat$ShareCompatImpl.java /android/support/v4/app/FragmentContainer.java /android/support/v4/app/TaskStackBuilder$SupportParentable.java /android/support/v4/app/FragmentManager$OnBackStackChangedListener.java /android/support/v4/app/FragmentManager$BackStackEntry.java /android/support/v4/app/ActionBarDrawerToggle$Delegate.java /android/support/v4/app/ActionBarDrawerToggle$ActionBarDrawerToggleImpl.java /android/support/v4/app/NotificationCompat$NotificationCompatImpl.java /android/support/v4/app/ActionBarDrawerToggle$DelegateProvider.java /android/support/v4/app/TaskStackBuilder$TaskStackBuilderImpl.java /android/support/v4/app/FragmentTabHost$1.java /android/support/v4/app/NavUtils$NavUtilsImpl.java /android/support/v4/app/LoaderManager$LoaderCallbacks.java /android/support/v4/app/ActionBarDrawerToggle$1.java /android/support/v4/internal/view/SupportMenu.java /android/support/v4/internal/view/SupportMenuItem.java /android/support/v4/internal/view/SupportSubMenu.java /android/support/v4/text/TextDirectionHeuristicsCompat$TextDirectionAlgorithm.java /android/support/v4/text/ICUCompat$ICUCompatImpl.java /android/support/v4/text/BidiFormatter$1.java /android/support/v4/text/TextDirectionHeuristicCompat.java /android/support/v4/text/TextDirectionHeuristicsCompat$1.java /android/support/v4/graphics/drawable/DrawableCompat$DrawableImpl.java /android/support/v4/widget/CursorFilter$CursorFilterClient.java /android/support/v4/widget/SearchViewCompatHoneycomb$OnCloseListenerCompatBridge.java /android/support/v4/widget/SimpleCursorAdapter$ViewBinder.java

检测详情	/android/support/v4/widget/EdgeEffectCompat$EdgeEffectImpl.java /android/support/v4/widget/ExploreByTouchHelper$1.java /android/support/v4/widget/SlidingPaneLayout$PanelSlideListener.java /android/support/v4/widget/SearchViewCompatHoneycomb$OnQueryTextListenerCompatBridge.java /android/support/v4/widget/SearchViewCompat$SearchViewCompatImpl.java /android/support/v4/widget/ScrollerCompat$ScrollerCompatImpl.java /android/support/v4/widget/CursorAdapter$1.java /android/support/v4/widget/DrawerLayout$DrawerListener.java /android/support/v4/widget/SimpleCursorAdapter$CursorToStringConverter.java /android/support/v4/widget/SlidingPaneLayout$SlidingPanelLayoutImpl.java /android/support/v4/widget/SlidingPaneLayout$1.java /android/support/v4/view/ViewGroupCompat$ViewGroupCompatImpl.java /android/support/v4/view/ActionProvider$VisibilityListener.java /android/support/v4/view/ViewConfigurationCompat$ViewConfigurationVersionImpl.java /android/support/v4/view/AccessibilityDelegateCompat$AccessibilityDelegateImpl.java /android/support/v4/view/GestureDetectorCompat$GestureDetectorCompatImpl.java /android/support/v4/view/GravityCompat$GravityCompatImpl.java /android/support/v4/view/MotionEventCompat$MotionEventVersionImpl.java /android/support/v4/view/ViewPager$OnAdapterChangeListener.java /android/support/v4/view/MarginLayoutParamsCompat$MarginLayoutParamsCompatImpl.java /android/support/v4/view/VelocityTrackerCompat$VelocityTrackerVersionImpl.java /android/support/v4/view/ViewPager$OnPageChangeListener.java /android/support/v4/view/PagerTitleStrip$PagerTitleStripImpl.java /android/support/v4/view/MenuItemCompat$MenuVersionImpl.java /android/support/v4/view/ViewParentCompat$ViewParentCompatImpl.java /android/support/v4/view/PagerTitleStrip$1.java /android/support/v4/view/ViewCompat$ViewCompatImpl.java /android/support/v4/view/MenuItemCompat$OnActionExpandListener.java /android/support/v4/view/AccessibilityDelegateCompatJellyBean$AccessibilityDelegateBridgeJellyBean.java /android/support/v4/view/MenuItemCompatIcs$SupportActionExpandProxy.java /android/support/v4/view/ViewPager$Decor.java /android/support/v4/view/accessibility/AccessibilityRecordCompat$AccessibilityRecordImpl.java /android/support/v4/view/accessibility/AccessibilityManagerCompat$AccessibilityManagerVersionImpl.java /android/support/v4/view/accessibility/AccessibilityManagerCompatIcs$AccessibilityStateChangeListenerBridge.java /android/support/v4/view/accessibility/AccessibilityEventCompat$AccessibilityEventVersionImpl.java /android/support/v4/view/accessibility/AccessibilityNodeInfoCompat$AccessibilityNodeInfoImpl.java /android/support/v4/view/accessibility/AccessibilityNodeProviderCompat$AccessibilityNodeProviderImpl.java /android/support/v4/view/accessibility/AccessibilityNodeProviderCompatJellyBean$AccessibilityNodeInfoBridge.java /android/support/v4/view/ViewPager$PageTransformer.java /android/support/v4/view/ActionProvider$SubUiVisibilityListener.java /android/support/v4/view/KeyEventCompat$KeyEventVersionImpl.java /android/support/v4/view/AccessibilityDelegateCompatIcs$AccessibilityDelegateBridge.java /android/support/v4/content/IntentCompat$IntentCompatImpl.java /android/support/v4/content/FileProvider$PathStrategy.java /android/support/v4/content/Loader$OnLoadCompleteListener.java /android/support/v4/net/TrafficStatsCompat$1.java /android/support/v4/net/ConnectivityManagerCompat$ConnectivityManagerCompatImpl.java /android/support/v4/net/TrafficStatsCompat$TrafficStatsCompatImpl.java
修复建议	建议开发者对代码进行混淆处理

3.5.3、Activity组件劫持检测

检测目的	检测关键组件在进入后台时是否具备防止进入后台或者提示用户等的相关功能。
威胁描述	界面劫持是指当应用打开一个应用界面时，操作已被恶意应用监听，恶意应用立即启动自己的仿冒界面并覆盖在应用的真实界面之上。用户在未察觉的在仿冒的界面中输入账号、密码等，导致用户关键信息被窃取。重要的Activity组件在进入后台时应该具备提醒用户或者防止进入后台的相关功能，否则恶意应用可以伪造相同的界面来劫持用户的输入信息，造成账号密码等敏感信息的泄露
检测结果	安全
结果描述	应用不存在Activity组件被劫持的问题
检测详情	无
修复建议	无

3.5.4、篡改检测

检测目的	检测应用是否具备防护应用篡改的能力
威胁描述	恶意攻击者经常使用向正常的应用程序中植入恶意代码或修改资源文件后二次打包的方式来构造恶意应用，仿冒原应用诱使用户进行安装，对原应用造成不良影响。应用程序应对自身是否被篡改应进行检测，防止恶意攻击者二次打包分析应用，增加攻击者的攻击成本。
检测结果	安全
结果描述	经检测，应用具备防护应用被篡改的能力
检测详情	无
修复建议	无

3.5.5、安全加固检测

检测目的	检测应用是否进行安全加固
威胁描述	检测应用是否进行了安全的加固方式,进行了安全加固可以对二次打包，软件调试等进行有效的防护
检测结果	中危
结果描述	未检测到应用采用安全加固
检测详情	
修复建议	建议对应用进行安全加固

3.5.6、使用原生层代码

检测目的	检测应用是否采用原生层代码
威胁描述	应用如果未使用原生层代码实现自身的敏感函数（如加解密、存储、通信、敏感数据生成等），可能导致相关代码的被攻击者轻易破解获取源代码，分析出逻辑流程，进而进行仿冒和破坏。同时使用原生层代码能够隐藏Android Framework层的API调用，提高APP运行的效率，增加攻击者逆向应用的门槛，实现大多数安全相关的防护功能。
检测结果	安全
结果描述	经检测,应用使用了原生层代码
检测详情	无
修复建议	无

3.5.7、二次打包检测

检测目的	检测应用是否可以进行二次打包
威胁描述	APK篡改后二次打包不仅严重威胁应用开发者的版权和经济利益，而且也使APP用户遭受到不法应用的恶意侵害。对客户端程序添加或修改代码，修改客户端资源图片，配置信息、图标，添加广告，推广自己的产品，再生成新的客户端程序，可导致大量盗版应用的出现减少开发者的收入；恶意的二次打包还能实现应用钓鱼、添加病毒代码、添加恶意代码，从而窃取登录账号密码、支付密码，拦截验证码短信，修改转账目标账号、金额等等。
检测结果	安全
结果描述	应用对二次打包做了防护
检测详情	无

修复建议	无

3.5.8、设备root检测

检测目的	检测应用是否对root后的设备采取防护措施
威胁描述	root后的设备将会导致恶意程序拿到非常高的权限，原有的沙箱机制等安全策略将会遭到破坏，严重威胁应用安全，攻击者获取了ROOT权限可以随意访问任意应用储存的任何数据，造成数据泄露、数据非法篡改等风险。应用应针对处于ROOT环境下的各项风险进行防御，或向用户做出提示
检测结果	安全
结果描述	经检测，应用对在root设备上的运行进行了防护
检测详情	无
修复建议	无

3.6 安全风险提示

3.6.1、联系人查询

检测目的	检测应用是否存在联系人查询风险
威胁描述	第三方应用可能正在通过非法手段获取联系人信息
检测结果	安全
结果描述	经检测，应用不存在联系人查询风险
检测详情	无
修复建议	无

3.6.2、使用udp通信

检测目的	检测应用是否存在使用UDP套接字通信风险
威胁描述	可能会受到UDP淹没攻击。当受害系统接收到一个 UDP 数据包的时候，它会确定目的端口正在等待中的应用程序。当它发现该端口中并不存在正在等待的应用程序，它就会产生一个目的地址无法连接的 ICMP数据包发送给该伪造的源地址。如果向受害者计算机端口发送了足够多的 UDP 数据包的时候，整个系统就会瘫痪。
检测结果	安全
结果描述	经检测，应用不存在使用UDP套接字通信风险
检测详情	无
修复建议	无

3.6.3、寄生推高风险SDK

检测目的	检测应用是否使用了感染寄生推的SDK

威胁描述	应用使用感染寄生推的SDK后会联网获取恶意jar包并加载，在未获得用户授权的情况下对用户手机进行ROOT，并通过恶意推送广告牟利。
检测结果	安全
结果描述	经检测,应用未使用具有相关风险的SDK
检测详情	无
修复建议	无

3.6.4、短信操作

检测目的	检测应用是否存在短信操作风险
威胁描述	第三方应用对短信进行操作，恶意应用可以利用本操作在用户无感的情况下进行短信收发，恶意消耗资费或盗窃用户敏感信息
检测结果	安全
结果描述	经检测，应用不存在短信操作风险
检测详情	无
修复建议	无

3.6.5、获得SIM卡信息

检测目的	检测应用是否存在获得获得SIM卡信息风险
威胁描述	应用通过查询SIM卡信息可以获得如用户手机号码、SIM卡序号、SIM卡国家代码、SIM用户识别号等信息，恶意应用通常会采集这些信息来对感染用户进行标识和分类，或通过对SIM卡进行补卡操作来伪造身份。
检测结果	安全
结果描述	经检测，应用不存在获得SIM卡信息风险
检测详情	无
修复建议	无

3.6.6、自定义短信接收端口

检测目的	检测应用是否存在自定义消息接收端口风险
威胁描述	在data标签中使用 android:port 属性来处理Android的URI消息信息,而这个端口可能被恶意程序利用来产生或者接收垃圾信息或者骚扰信息。
检测结果	安全
结果描述	经检测，应用不存在自定义消息接收端口风险
检测详情	无
修复建议	无

3.6.7、获得手机位置

检测目的	检测应用是否存在获得手机位置信息风险
威胁描述	通过网络或GPS获取用户所在位置的经纬度信息，恶意应用可以凭借此操作窃取用户所在位置，侵犯用户隐私
检测结果	安全
结果描述	经检测，应用不存在获得手机位置信息风险
检测详情	无
修复建议	无

3.6.8、特定敏感词汇检测

检测目的	扫描应用文本中的特定敏感词汇
威胁描述	应用中含有暴力、黄赌毒、政治、宗教等敏感词汇，会给应用拥有者带来法律、声誉等方面的负面影响。
检测结果	安全
结果描述	未检测到特定敏感词汇
检测详情	无
修复建议	无

4 应用服务端安全测评

4.1 http://192.168.0.41

4.1.1 服务端信息收集

操作系统	Windows Server
编程语言	PHP
cms	fckeditor
web服务器	未知
waf	未知

4.1.2 服务端漏洞测试

4.1.2.1 文件上传漏洞检测

检测目的	检测服务端文件上传漏洞
漏洞描述	文件上传漏洞是指网络攻击者上传了一个可执行的文件到服务器并执行,这里上传的文件可以是木马，病毒，恶意

	脚本或者WebShell等。
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.2 不安全eval函数使用检测

检测目的	寻找不安全eval()函数的使用
漏洞描述	因为eval函数可以执行传给它的任何字符串，所以对eval函数是否安全使用进行检测是很有必要的
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.3 不安全ssl使用检测

检测目的	检测使用了HTTPS提供的URL是否能通过不安全的HTTP协议使用
漏洞描述	可以使用不安全的HTTP协议访问安全内容
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.4 命令行执行

检测目的	检测服务器端命令行执行漏洞
漏洞描述	用户通过浏览器提交执行命令，由于服务器端没有针对执行函数做过滤，导致在没有指定绝对路径的情况下就执行命令，可能会允许攻击者通过改变 $PATH 或程序执行环境的其他方面来执行一个恶意构造的代码
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.5 本地包含漏洞

检测目的	检测服务端是否有本地包含漏洞
漏洞描述	本地包含漏洞（也被称为LFI）,是通过网络浏览器上的服务器包含文件的一个过程，当页面的文件来源过滤不严时，就会出现这种漏洞，而且还能允许注入目录遍历字符
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.6 sql注入漏洞检测

检测目的	查找服务端sql注入漏洞
漏洞描述	SQL注入就是通过构建特殊的具有SQL语法的语句，绕到数据库中进而执行相应的操作的漏洞。
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.7 preg_replace漏洞检测

检测目的	检测服务端是否存在preg_replace漏洞
漏洞描述	当用户可以控制正则表达式或正在分析的字符串的内容并且正则表达式具有'e'修饰符时，此PHP函数易受攻击。
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.8 格式字符串错误

检测目的	检测服务端中是否存在格式字符串错误
漏洞描述	只有在服务器配置为返回错误时才能检测格式字符串漏洞，并且应用程序是以cgi-c或其他语言开发的，这些语言允许程序员执行此类错误。
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.9 LDAP注入

检测目的	检测服务端是否存在ldapi注入漏洞
漏洞描述	LDAP注入攻击和SQL注入攻击相似，是利用用户引入的参数生成LDAP查询。一个安全的Web应用在构造和将查询发送给服务器前应该净化用户传入的参数。在有漏洞的环境中，这些参数没有得到合适的过滤，因而攻击者可以注入任意恶意代码。
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.10 缓冲区溢出漏洞

检测目的	查找缓冲区溢出漏洞
漏洞描述	缓冲区溢出是一种非常普遍、非常危险的漏洞，在各种操作系统、应用软件中广泛存在。利用缓冲区溢出攻击，可以导致程序运行失败、系统宕机、重新启动等后果。更为严重的是，可以利用它执行非授权指令，甚至可以取得系统特权，进而进行各种非法操作。
漏洞等级	安全
漏洞url	无

修复建议	无

4.1.2.11 ReDoS漏洞

检测目的	检测服务端是否存在正则表达式拒绝服务漏洞
漏洞描述	正则表达式拒绝服务攻击。开发人员使用了正则表达式来对用户输入的数据进行有效性校验, 当编写校验的正则表达式存在缺陷或者不严谨时, 攻击者可以构造特殊的字符串来大量消耗服务器的系统资源，造成服务器的服务中断或停止。
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.12 XPATH注入

检测目的	查找XPATH注入
漏洞描述	XPath注入攻击是指利用XPath 解析器的松散输入和容错特性，能够在 URL、表单或其它信息上附带恶意的XPath查询代码，以获得权限信息的访问权并更改这些信息。XPath注入攻击是针对Web服务应用新的攻击方法，它允许攻击者在事先不知道XPath查询相关知 识的情况下，通过XPath查询得到一个XML文档的完整内容。
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.13 xss漏洞

检测目的	查找服务器是否存在xss漏洞
漏洞描述	xss漏洞允许恶意web用户将代码植入到提供给其它用户使用的页面中。比如这些代码包括HTML代码和客户端脚本。攻击者利用XSS漏洞旁路掉访问控制——例如同源策略。
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.14 htaccess配置错误

检测目的	查找htaccess配置错误
漏洞描述	.htaccess文件是Apache服务器中的一个配置文件，它负责相关目录下的网页配置。通过.htaccess文件，调用php的解析器解析一个文件名只要包含“cimer”这个字符串的任意文件。这个“cimer”的内容如果是一句话木马.即可利用中国菜刀进行连接。
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.15 服务器端包含漏洞

检测目的	检测服务器端包含（SSI）漏洞

漏洞描述	服务器端包含提供了一种对现有HTML文档增加动态内容的方法。apache和iis都可以通过配置支持SSI，在网页内容被返回给用户之前，服务器会执行网页内容中的SSI标签。在很多场景中，用户输入的内容可以显示在页面中，比如一个存在反射XSS漏洞的页面，如果输入的payload不是xss代码而是ssi的标签，服务器又开启了ssi支持的话就会存在SSI漏洞
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.16 跨站请求伪造漏洞

检测目的	检测服务端是否存在跨站请求伪造漏洞
漏洞描述	攻击者盗用了你的身份，以你的名义发送恶意请求，对服务器来说这个请求是完全合法的，但是却完成了攻击者所期望的一个操作，比如以你的名义发送邮件、发消息，盗取你的账号，添加系统管理员，甚至于购买商品、虚拟货币转账等。
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.17 SSL证书有效性检测

检测目的	如果应用使用了https协议，检测ssl证书有效性
漏洞描述	如果使用https协议，但是使用了无效，自签名的证书，或者证书参数配置不正确，依然会产生中间人攻击等风险
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.18 跨站跟踪漏洞

检测目的	检测服务端是否存在跨站跟踪漏洞
漏洞描述	XST是利用XSS和HTTP TRACE方法的组合。
漏洞等级	低危
漏洞url	共检测到 [1] 处漏洞位置 http://192.168.0.41/
修复建议	解决方法有两个: 1,对于2.0.55以上版本的apache服务器，在httpd.conf中设置TraceEnable off 2,利用apache服务器的rewrite功能，对TRACE请求进行拦截

4.1.2.19 XML外部实体攻击

检测目的	检测XML外部实体攻击
漏洞描述	攻击者可以通过实体将他自定义的值发送给应用程序，然后让应用程序去呈现
漏洞等级	安全
漏洞url	无

修复建议	无

4.1.2.20 SQL盲注漏洞

检测目的	检测服务端中是否存在sql盲注漏洞
漏洞描述	盲注是不能通过直接显示的途径来获取数据库数据的方法。在盲注中，攻击者根据其返回页面的不同来判断信息(可能是页面内容的不同，也可以是响应时间不同)。
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.21 HTTP响应头拆分漏洞

检测目的	检测服务端中是否存在响应拆分攻击风险
漏洞描述	HTTP响应头拆分漏洞是由于web应用程序没有对用户的提交进行严格过滤，导致非法用户可以提交一些恶意字符，更具体来说，是对用户输入的CR 和LF字符没有进行严格的过滤。
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.22 远程文件包含漏洞

检测目的	检测服务端中是否存在远程文件包含漏洞
漏洞描述	远程文件包含漏洞是服务器通过PHP的特性（函数）去包含任意文件时，由于要包含的这个文件来源过滤不严格，从而可以去包含一个恶意文件，攻击者就可以远程构造一个特定的恶意文件达到攻击目的。
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.2.23 目录遍历漏洞

检测目的	检测服务端中是否存在目录遍历漏洞
漏洞描述	目录遍历（路径遍历）是由于web服务器或者web应用程序对用户输入的文件名称的安全性验证不足而导致的一种安全漏洞，使得攻击者通过利用一些特殊字符就可以绕过服务器的安全限制，访问任意的文件（可以是web根目录以外的文件），甚至执行系统命令。
漏洞等级	安全
漏洞url	无
修复建议	无

4.1.3 服务器端口扫描

端口号	对应服务

80	http
8080	http-proxy
8090	unknown
135	msrpc
8081	blackice-icecap
7001	afs3-callback
3306	mysql
139	netbios-ssn
445	microsoft-ds
8009	ajp13
3389	ms-wbt-server

4.1.4 服务器端口爆破

没有爆破结果

4.1.5 web路径爆破结果

web路径爆破地址
1 http://192.168.0.41/

四维创智

猎奇
移动应用安全检测报告

- 检测时间：2018-10-08 09:19:33
- 引擎版本： 3.0.0
- 适用系统：iOS

目录

1 检测依据

《信息安全技术移动智能终端个人信息保护技术要求》

《YD/T 1438-2006 数字移动台应用层软件功能要求和测试方法》

《YD/T 2307-2011 数字移动通信终端通用功能技术要求和测试方法》

《电子银行业务管理办法》

《电子银行安全评估指引》

《中国金融移动支付客户端技术规范》

《中国金融移动支付应用安全规范》

《移动互联网应用软件安全评估大纲》

《中华人民共和国网络安全法》

《移动互联网应用程序信息服务管理规定》

2 检测结果

10

应用名：DamnVulnerableIOSApp　　包名：None　　大小：5.53MB

MD5值：6b27b725e021afbc15c0e6574732af2a

Sha1值：7525a037f65b43891a49052091e63322ed12dd15

2.1 检测结果综述

漏洞级别

高危漏洞	0
中危漏洞	4
低危漏洞	0
检测项总数	16

漏洞类型

2.2 检测项汇总

序号	检测项	检测结果
1	弱哈希函数使用	安全
2	URL扫描	中危
3	内存分配安全	安全
4	反调试功能	中危
5	应用证书信息	安全
6	Email扫描	中危
7	使用SQLite数据库明文存储数据	安全
8	iOS运行时动态库信息	中危
9	不安全的随机函数	安全
10	弱加密函数使用	安全
11	不安全的API函数引用	安全
12	打印调试日志	安全
13	编译时使用ARC标志	安全
14	反调试功能	安全

15	编译时使用SSP标志	安全
16	编译时使用PIE标志	安全

3 检测详情

3.1 APP基础信息

3.1.1、应用权限信息

权限	描述	等级

3.2 ios应用安全检测

3.2.1、弱哈希函数使用

检测目的	检测应用是否使用弱哈希函数
威胁描述	使用弱哈希函数可能会产生哈希碰撞，或者造成哈希还原等的攻击
检测结果	安全
结果描述	经检测，应用未使用弱哈希函数
检测详情	无
修复建议	无

3.2.2、URL扫描

检测目的	扫描应用中出现的url
威胁描述	扫描应用中出现url信息。
检测结果	中危
结果描述	检测到应用泄漏url信息
	Data:(id)data; Data:(id)fileData Data:(id)formData Data:(id)data data:(id)data Data:(BOOL)data; Data:(BOOL)completeData; data:(id)data; Data:(id*)data;

检测详情	Data:(id)utf8Data; Data:(int)data http://www.w3.org/1999/02/22-rdf-syntax-ns# http://ns.adobe.com/xap/1.0/ http://ns.adobe.com/tiff/1.0/ http://damnvulnerableiosapp.com/#solutions http://highaltitudehacks.com/2013/11/08/ios-application-security-part-21-arm-and-gdb-basics http://highaltitudehacks.com/2013/08/20/ios-application-security-part-11-analyzing-network-traffic-over-http-slash-https http://google.com/ https://google.com/ https://www.google.co.uk http://highaltitudehacks.com/2014/03/07/ios-application-security-part-30-attacking-url-schemes http://highaltitudehacks.com/2013/12/17/ios-application-security-part-26-patching-ios-applications-using-ida-pro-and-hex-fiend http://highaltitudehacks.com/2014/01/17/ios-application-security-part-28-patching-ios-application-with-hopper http://highaltitudehacks.com/2013/10/26/ios-application-security-part-20-local-data-storage-nsuserdefaults http://highaltitudehacks.com/2013/06/16/ios-application-security-part-3-understanding-the-objective-c-runtime http://highaltitudehacks.com/2013/07/02/ios-aios-appllication-security-part-4-runtime-analysis-using-cycript-yahoo-weather-app http://highaltitudehacks.com/2013/07/02/ios-application-security-part-5-advanced-runtime-analysis-and-manipulation-using-cycript-yahoo-weather-app http://highaltitudehacks.com/2013/07/25/ios-application-security-part-8-method-swizzling-using-cycript http://highaltitudehacks.com/2013/09/17/ios-application-security-part-16-runtime-analysis-of-ios-applications-using-inalyzer http://highaltitudehacks.com/2013/12/17/ios-application-security-part-22-runtime-analysis-and-manipulation-using-gdb http://highaltitudehacks.com/2014/01/17/ios-application-security-part-29-insecure-or-broken-cryptography http://highaltitudehacks.com/2013/12/17/ios-application-security-part-24-jailbreak-detection-and-evasion http://damnvulnerableiosapp.com https://api.parse.com https://api.twitter.com/oauth/request_token http://twitter-oauth.callback https://api.twitter.com/oauth/access_token https://api.twitter.com/oauth/authenticate?oauth_token=%@ data:error: Data:withSettings:encryptionKey:IV:error: Data:error: Data:withSettings:password:error: Data:withSettings:password:IV:encryptionSalt:HMACSalt:error: Data:withSettings:encryptionKey:HMACKey:error: Data:withSettings:encryptionKey:HMACKey:IV:error: Data:encoding: Data:withPassword:error: Data:withEncryptionKey:HMACKey:error: Data:target:selector: Data:block: Data:options:error: Data:mimeType:fileName: Data:binary: Data:name: Data:name:fileName:mimeType: Data:totalBytesWritten:totalBytesExpectedToWrite: http://ns.adobe.com/xap/1.0/mm/ http://ns.adobe.com/xap/1.0/sType/ResourceRef# http://www.apple.com/DTDs/PropertyList-1.0.dtd http://www.apple.com/appleca/root.crl0 https://www.apple.com/appleca/0 http://www.apple.com/appleca/0M http://developer.apple.com/certificationauthority/wwdrca.crl0 http://www.apple.com/appleca/iphone.crl0 https://www.apple.com/certificateauthority/terms.html0 https://www.apple.com/certificateauthority/root.crl0U https://www.apple.com/certificateauthority/casigners.html0 www.google.co.uk0 www.google.co.uk0h http://pki.google.com/GIAG2.crt0+ http://clients1.google.com/ocsp0 http://pki.google.com/GIAG2.crl0 http://google.com.
修复建议	无

3.2.3、内存分配安全

检测目的	检测应用内存分配安全
威胁描述	应用的可执行文件如果使用malloc函数，那么在分配内存时不会对内存进行初始化操作，从而导致应用崩溃和增加安全隐患。
检测结果	安全
结果描述	经检测，应用不存在内存分配安全风险
检测详情	无
修复建议	无

3.2.4、反调试功能

检测目的	检测应用是否使用Webview组件
威胁描述	使用Webview组件的应用通常调用系统自身的HTML解析器，在面临跨站点脚本攻击、远程代码执行等攻击方式时具有明显的弱势。
检测结果	中危
结果描述	经检测，应用使用了Webview组件
检测详情	未检测到应用采取反调试检测
修复建议	尽量不使用Webview组件或者使用具有安全配置的Webview组件。

3.2.5、应用证书信息

检测目的	检测应用中是否存在明文证书文件
威胁描述	应用中的证书文件被用来验证服务器的合法性，以及在与服务器通信的过程中对传输数据进行加密、解密，保证数据传输的保密性、完整性。明文存储的证书如果被篡改，客户端可能连接到仿冒的服务器，导致用户账号、密码等重要信息泄露。
检测结果	安全
结果描述	经检测，应用存在明文证书信息
检测详情	无
修复建议	无

3.2.6、Email扫描

检测目的	检测应用是否存在测试时留存的email信息
威胁描述	开发人员有时会在开发时将email信息硬编码到代码中方便使用，而在发布时未删除这部分email信息可能导致开发人员信息泄漏，或导致应用运行逻辑外泄。
检测结果	中危
结果描述	经检测，应用发现了硬编码的email信息

检测详情	prateek@damnvulnerableiosapp.com
修复建议	建议应用发布时将其中保存的email信息删除

3.2.7、使用SQLite数据库明文存储数据

检测目的	检测应用是否使用SQLite数据库
威胁描述	在sqlite数据库中明文存储的敏感信息可能被恶意软件轻易读取
检测结果	安全
结果描述	经检测，应用存在使用SQLite数据库风险
检测详情	无
修复建议	无

3.2.8、iOS运行时动态库信息

检测目的	检测应用运行时动态库信息
威胁描述	iOS应用运行时需要调用的系统支持文件。
检测结果	中危
结果描述	经检测，应用iOS运行时动态库信息没有风险
检测详情	DamnVulnerableIOSApp (architecture 0): /System/Library/Frameworks/SystemConfiguration.framework/SystemConfiguration /System/Library/Frameworks/StoreKit.framework/StoreKit /System/Library/Frameworks/Security.framework/Security /System/Library/Frameworks/QuartzCore.framework/QuartzCore /System/Library/Frameworks/MobileCoreServices.framework/MobileCoreServices /usr/lib/libz.1.dylib /System/Library/Frameworks/CoreLocation.framework/CoreLocation /System/Library/Frameworks/CoreGraphics.framework/CoreGraphics /System/Library/Frameworks/CFNetwork.framework/CFNetwork /System/Library/Frameworks/AudioToolbox.framework/AudioToolbox /System/Library/Frameworks/CoreData.framework/CoreData /System/Library/Frameworks/UIKit.framework/UIKit /System/Library/Frameworks/Foundation.framework/Foundation /usr/lib/libobjc.A.dylib /usr/lib/libSystem.B.dylib /System/Library/Frameworks/CoreFoundation.framework/CoreFoundation DamnVulnerableIOSApp (architecture 1): /System/Library/Frameworks/SystemConfiguration.framework/SystemConfiguration /System/Library/Frameworks/StoreKit.framework/StoreKit /System/Library/Frameworks/Security.framework/Security /System/Library/Frameworks/QuartzCore.framework/QuartzCore /System/Library/Frameworks/MobileCoreServices.framework/MobileCoreServices /usr/lib/libz.1.dylib /System/Library/Frameworks/CoreLocation.framework/CoreLocation /System/Library/Frameworks/CoreGraphics.framework/CoreGraphics /System/Library/Frameworks/CFNetwork.framework/CFNetwork /System/Library/Frameworks/AudioToolbox.framework/AudioToolbox /System/Library/Frameworks/CoreData.framework/CoreData /System/Library/Frameworks/UIKit.framework/UIKit /System/Library/Frameworks/Foundation.framework/Foundation /usr/lib/libobjc.A.dylib /usr/lib/libSystem.B.dylib /System/Library/Frameworks/CoreFoundation.framework/CoreFoundation

修复建议	尽量不要使用第三方或者自定义的动态库文件

3.2.9、不安全的随机函数

检测目的	检测应用是否存在不安全的随机函数漏洞
威胁描述	在SecureRandom生成随机数时，如果我们不调用setSeed方法，SecureRandom会从系统中找到一个默认随机源。每次 生成随机数时都会从这个随机源中取seed。不安全的使用方式会导致SecureRandom使用相同的种子生成随机数，每次 生成随机数时也是相同的。该漏洞存在于Android系统随机生成数字串安全密钥的环节中。这会导致使用的随机数或加 密算法被破解
检测结果	安全
结果描述	经检测，应用不存在不安全的随机函数使用
检测详情	无
修复建议	无

3.2.10、弱加密函数使用

检测目的	检测应用是否使用弱加密函数使用
威胁描述	AES/DES是Android程序中常用的两种对称加密算法，其工作模式有ECB、CBC、CFB和OFB。当其使用ECB或OFB工作模式或单次DES对敏感数据进行加密时，加密数据可能被选择明文攻击CPA破解。加密方法失效可能造成客户端隐私数据泄露、加密文件破解、传输数据被获取、中间人攻击等后果，导致用户敏感信息被窃取。
检测结果	安全
结果描述	经检测，应用未使用弱加密函数
检测详情	无
修复建议	无

3.2.11、不安全的API函数引用

检测目的	检测应用是否引用不安全的API函数
威胁描述	使用已经取消的/不安全的API函数，可能会造成不兼容的问题，从而导致本地拒绝服务，或者出现信息泄露和代码执行等安全问题。
检测结果	安全
结果描述	经检测，应用未使用不安全的API函数引用
检测详情	无
修复建议	无

3.2.12、打印调试日志

检测目的	检测应用是否打印调试日志

威胁描述	调试信息函数可能输出重要的调试信息，其中包含的信息可能导致用户信息泄露，泄露核心代码逻辑等，为发起攻击提供 便利，例如：Activity的组件名；通信交互的日志；跟踪的变量值等
检测结果	安全
结果描述	经检测，应用不存在打印调试日志风险
检测详情	无
修复建议	无

3.2.13、编译时使用ARC标志

检测目的	检测应用编译时是否使用ARC标志
威胁描述	如果应用在编译时使用自动化引用计数器（ARC）标签，它能够对Objective-C对象的内存进行管理，有效地防止针对内存的攻击。
检测结果	安全
结果描述	经检测，应用编译时未使用ARC标志
检测详情	无
修复建议	无

3.2.14、反调试功能

检测目的	检测应用是否采取反调试措施
威胁描述	应用程序如果使用ptrace系统调用，该调用通常用来防止软件调试和进程注入。若没有使用该系统调用可能会造成安全隐患。
检测结果	安全
结果描述	经检测，应用采取了反调试措施
检测详情	无
修复建议	无

3.2.15、编译时使用SSP标志

检测目的	检测应用编译时是否使用SSP标志
威胁描述	APP如果使用堆栈保护器（SSP）标志编译，能够有效地防止对堆栈数据的覆盖而造成的溢出攻击
检测结果	安全
结果描述	经检测，应用编译时未使用SSP标志
检测详情	无
修复建议	无

3.2.16、编译时使用PIE标志

检测目的	检测应用编译时是否使用PIE标志
威胁描述	如果应用使用位置无关的可执行（PIE）标记编译，则能够使得内存中的可执行代码随机化分步，这是一种通用的防止内存读写和代码执行的有效手段。。
检测结果	安全
结果描述	经检测，应用编译时未使用PIE标志
检测详情	无
修复建议	无