安全检测评估报告

移动管培

文件状态： 【√】正式发稿	**公司名称**	深圳爱加密科技有限公司	**文档名称**	安全检测评估报告
	检测时间	2020-06-08	**密级**	中

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》

2 检测结果概览

应用检测结果如表 2-1 和图 2-2 所示，各检测项检测结果如表 2-2 所示。

应用名称	移动管培
检测分数	53
检测项总数	24 (包括 18 项风险检测、6 项基本信息检测)

表1.1 检测得分

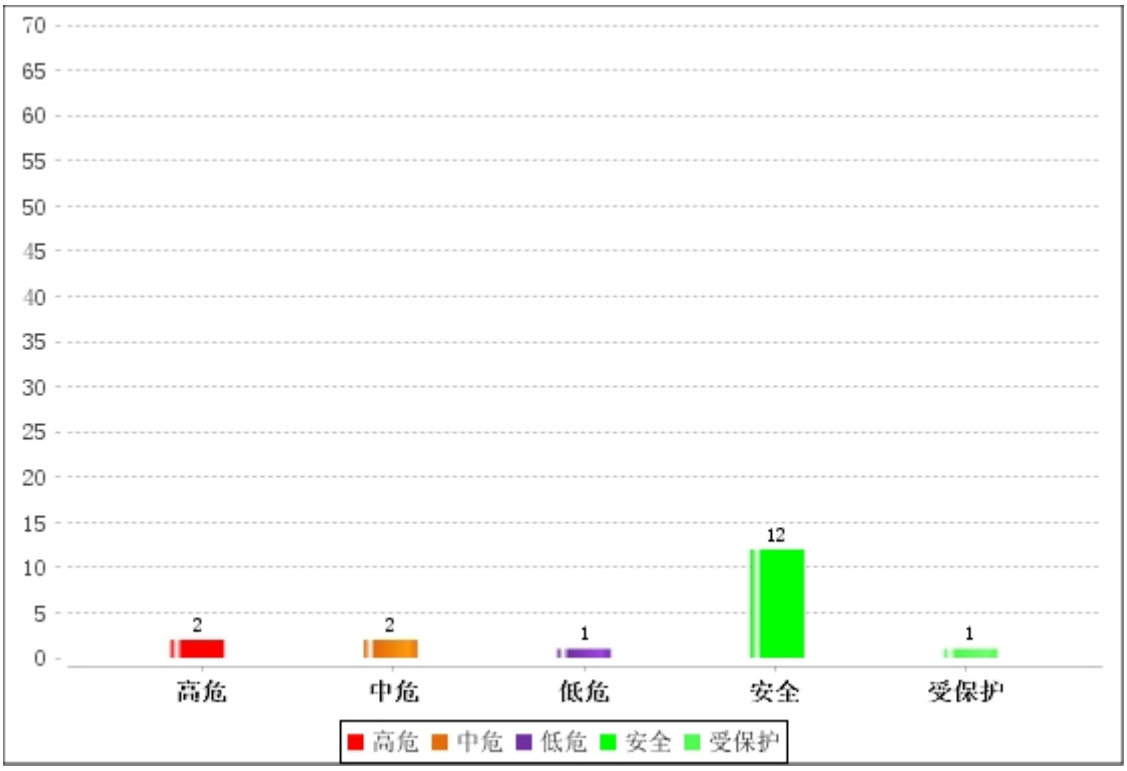

图1.2 检测结果汇总

序号	检测项目	检测结果
1	应用包信息检测	--
2	应用签名信息检测	--
3	应用行为信息检测	--
4	应用权限信息检测	--
5	应用加固壳识别	--
6	第三方 SDK 检测	--

序号	检测项目	检测结果
7	敏感行为检测	安全
8	敏感函数检测	安全
9	敏感词汇检测	安全
10	动态加载 DEX 行为检测	安全
11	代码混淆检测	中危
12	DEX 保护检测	受保护
13	DEX 加花保护检测	中危
14	重要函数逻辑安全	安全
15	权限滥用检测	安全
16	Activity 最小化特权检测	高危
17	Service 最小化特权检测	安全
18	Broadcast Receiver 最小化特权检测	高危
19	Intent 检测	安全
20	调试信息检测	安全
21	测试数据移除检测	安全
22	异常处理检测	低危
23	跨域访问漏洞	安全
24	硬编码检测	安全

表2.1 检测结果详情

3 检测详情

3.1 移动应用基本信息检测

3.1.1 应用信息检测

应用名称	移动管培
包名	com.gaotai.ydxygwjs
文件大小	13.5MB
版本信息	1.0.12
文件 MD5	75bb527175d3cb30ae8a39e8036fe9ee

3.1.2 应用签名信息检测

所有者	CN=jxt
发布者	CN=jxt
序列号	4f857fad
有效期开始日期	Wed Apr 11 20:57:17 CST 2012
截止日期	Fri Mar 18 20:57:17 CST 2112
证书指纹	MD5: 20:EA:95:4E:36:A3:5F:4C:E5:9E:34:A9:69:5C:CC:DA SHA1: A5:1E:96:47:C0:F9:B7:02:D2:E5:26:FB:EF:BA:BA:3E:5F:CC:67:E3 SHA256: 5F:23:AD:BA:60:AA:ED:65:C7:91:5F:9C:C7:92:89:DB:2A:A7:5E:5A:DC:4D:74:E9:28:FC:19:26:86:E2:D3:2B 签名算法名称: SHA1withRSA 版本: 3

3.1.3 应用行为信息检测

允许应用程序控制闪光灯。
允许应用程序控制振动器。
允许应用程序写入 SD 卡。
允许应用程序查看所有网络的状态。

允许应用程序发送顽固广播，这些广播在结束后仍会保留。恶意应用程序可能会借此使手机耗用太多内存，从而降低其速度或稳定性。
允许应用程序使用相机拍照，这样应用程序可随时收集进入相机镜头的图像。
允许应用程序访问录音路径。
允许应用程序防止手机进入休眠状态。
允许应用程序装载和卸载可移动存储器的文件系统。
允许应用程序查看有关 WLAN 状态的信息。
允许应用程序连接到 WLAN 接入点以及与 WLAN 接入点断开连接，并对配置的 WLAN 网络进行更改。
允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
允许程序访问网络。
允许应用程序修改整个系统的音频设置，如音量和路由。
允许应用程序查看本地蓝牙手机的配置，以及建立或接受与配对设备的连接。

3.1.4 应用权限信息检测

权限名称	权限检测
"android.permission.FLASHLIGHT"	控制闪光灯
"android.permission.VIBRATE"	控制振动器
"android.permission.WRITE_EXTERNAL_STORAGE"	修改/删除 SD 卡中的内容
"android.permission.ACCESS_NETWORK_STATE"	查看网络状态
"android.permission.BROADCAST_STICKY"	发送置顶广播
"android.permission.CAMERA"	拍照
"android.permission.RECORD_AUDIO"	录音
"android.permission.WAKE_LOCK"	防止手机休眠
"android.permission.MOUNT_UNMOUNT_FILESYSTEMS"	装载和卸载文件系统
"android.permission.ACCESS_WIFI_STATE"	查看 WLAN 状态
"android.permission.CHANGE_WIFI_STATE"	更改 WLAN 状态
"android.permission.GET_TASKS"	检索当前运行的应用程序
"android.permission.WRITE_SETTINGS"	修改全局系统设置
"android.permission.READ_PHONE_STATE"	读取手机状态和身份

"android.permission.RECEIVE_BOOT_COMPLETED"	开机时自动启动
"android.permission.INTERNET"	访问网络
"android.permission.MODIFY_AUDIO_SETTINGS"	更改您的音频设置
"android.permission.BLUETOOTH"	创建蓝牙连接

3.1.5 应用加固壳识别

是否加壳	描述
是	该 APP 检测出使用 360 加固

3.1.6 第三方 SDK 检测

检测目的	检测应用是否包含第三方 SDK
检测详细信息	总共检测资源文件中包含第三方 SDK 数量【0】条。

3.2 移动应用恶意行为检测

3.2.1 敏感词汇检测

检测目的	检测 APP 是否具有敏感词汇
检测结果	未发现敏感词汇
检测详细信息	检测出敏感词汇共【0】条。

3.2.2 敏感函数检测

检测目的	检测 APP 程序中是否调用了敏感函数
检测结果	未发现敏感函数
检测详细信息	检测出敏感函数共【0】条。

3.2.3 敏感行为检测

检测目的	检测 APP 是否具有敏感行为
检测结果	未发现敏感行为
检测详细信息	

3.2.4 动态加载 DEX 行为检测

检测目的	检测 APP 是否具有动态加载 DEX 行为
检测结果	未发现动态加载 DEX 行为
检测详细信息	检测出动态加载 DEX 函数共【0】条：

3.3 移动应用安全规范检测

3.3.1 程序机密性规范检测

3.3.1.1 代码混淆检测

检测目的	检测 APK 程序中 Java 代码是否进行过混淆
重要等级	中
危害	代码未进行混淆会出现被反编译窃取逆向代码还原到源工程的危险
检测结果	中危
检测详情	该 APK 可以被反编译后获取源代码。
解决方案	建议使用编译器自带 proguard 混淆方案

3.3.1.2 DEX 保护检测

检测目的	检测 APK 程序中 DEX 文件是否受保护
重要等级	高
危害	DEX 未进行保护会被攻击者通过 baksmali/apktool/dex2jar 等反编译工具逆向出代码，造成核心代码逻辑泄露、重要数据加密代码逻辑泄露等等。
检测结果	受保护
检测详情	该 APP 已经过加固保护，所有的重要函数与代码都被隐藏或者类挖空保护。
解决方案	

3.3.1.3 DEX 加花保护检测

检测目的	检测 APK 程序中的 DEX 文件是否进行加花保护
重要等级	中
危害	如果程序不进行 DEX 加花保护，baksmali/apktool/dex2jar 等静态反编译工具对 DEX 文件可直接执行反编译逆向出程序的功能实现代码。

检测结果	中危
检测详情	该 APK 可以被反编译后获取源代码。
解决方案	由于大部分逆向工具都是线性读取字节码并解析，当遇到无效字节码时，就会引起反编译工具字节码解析失败。我们可以插入无效字节码到 DEX 文件，但要保证该无效字节码永远不会被执行,否则您的程序就会崩溃。

3.3.1.4 重要函数逻辑安全

检测目的	检测 APK 中实现的重要函数逻辑是否安全
重要等级	高
危害	因为 APK 本身因为未进行专业加固保护，存在被 baksmali/apktool/dex2jar 直接反编译获取程序 Java 代码，如果程序的重要函数使用 android ndk 技术通过 C/C++实现能够提高重要函数的逻辑安全强度。 Elf 格式的 SO 文件如果未进行专业的加固保护可能存在被 ipa pro 工具一键 F5 逆向出 c 代码被分析的风险。
检测结果	安全
检测详情	检测出重要函数共【0】条：
解决方案	N/A

3.3.1.5 权限滥用检测

检测目的	检测 APK 中是否存在权限滥用风险
重要等级	中
危害	权限滥用漏洞一般归类于逻辑问题，是指应用功能开放过多或权限限制不严格，导致攻击者可以通过直接或间接调用的方式达到攻击效果。有些恶意程序可以应用权限对应用造成破坏，比如利用权限滥用漏洞有时可以使用某些特殊的功能，例如：访问摄像头、利用麦克风录音、编写并植入木马、反弹 shell 等等。
检测结果	安全
检测详情	总共检测系统权限数量【21】个： 【android.permission.ACCESS_NETWORK_STATE】： 相关代码： ...Landroid/net/ConnectivityManager;-> >getActiveNetworkInfo()Landroid/net/NetworkInfo;... 【android.permission.ACCESS_WIFI_STATE】： 相关代码： ...Landroid/net/wifi/WifiManager;->isWifiEnabled()Z Landroid/net/wifi/WifiManager;->setWifiEnabled(Z)Z... 【android.permission.BLUETOOTH】：

	相关代码： ....local v0, blueadapter:Landroid/bluetooth/BluetoothAdapter;...
解决方案	N/A

3.3.2 四大组件配置安全规范检测

3.3.2.1 Activity 最小化特权检测

检测目的	检测应用 Activity 权限攻击
重要等级	高
危害	应用组件如果存在权限攻击漏洞则该组件能够被外部的其他组件直接调用，这样就可能产生泄露隐私数据或者应用程序崩溃等漏洞。恶意应用可以传递有害数据或者命令给受害的 Broadcast Receiver，而 Receiver 接收到有害的数据或者命令时可能泄露数据或者做一些不当的操作。也有可能 Receiver 去开启其它的 Activity 或者 Service，从而产生更大的危害。Activity 被恶意应用开启，可能有一下危害：修改程序的状态或者数据；用户被欺骗（比如用户点击一个恶意应用的 Setting，恶意应用开启受害应用的设置，此时用户以为在修改恶意应用的 Setting，这样受害应用的设置可能被用户无意识的修改）；被调用的 Activity 可能返回隐私的信息给恶意应用，造成数据泄露；可能会是应用程序崩溃，造成拒绝服务等漏洞。
检测结果	高危
检测详情	总共检测 Activity 配置代码【48】条； 检测到未进行正确配置的代码【1】条； 检测到正确配置的代码【47】条 未进行正确配置的代码为： activity android:exported="true" android:launchMode="1" android:name="com.gaotai.ydxygwjs.wxapi.WXPayEntryActivity" android:theme="@7F0E0112" 正确 Activity 组件配置的代码为： activity android:label="@7F0D002C" android:name="com.gaotai.ydxygwjs.MainActivity" android:screenOrientation="1" android:theme="@7F0E0099" android:windowSoftInputMode="0x00000022" activity android:name="com.gaotai.ydxygwjs.activity.my.GTGwMySettingActivity" android:screenOrientation="1" activity

	android:name="com.gaotai.ydxygwjs.activity.login.GTGwChoiceVerification Activity" android:screenOrientation="1" activity android:name="com.gaotai.ydxygwjs.activity.login.GTGwVerificationOfIden tityActivity" android:screenOrientation="1" activity android:name="com.gaotai.ydxygwjs.activity.login.GTGwVerificationOfPho neActivity" android:screenOrientation="1" ... 此处省略【42】条数据 ...
解决方案	设置组件 EXPORTED=False 并且尽量不包含任何的 Intent Filter。

3.3.2.2 Service 最小化特权检测

检测目的	检测应用 Service 权限
重要等级	中
危害	Service 执行的操作一般比较敏感，比如更新数据库、提供事件通知等，因此一定要确保访问 Service 的组件有一定的权限。否则可能被恶意应用提供获取重要信息的漏洞，没有声明任何权限的应用即可在没有任何提示的情况下启动该服务，完成该服务所作操作，对系统安全性产生极大影响。
检测结果	安全
检测详情	总共检测 service 身份配置代码【6】条； 检测到未进行正确配置的代码【0】条； 检测到正确配置的代码【6】条； 正确 service 组件配置的代码为： service android:enabled="true" android:name="com.baidu.location.f" android:process=":remote" service android:enabled="true" android:name="com.gaotai.ydxygwjs.service.IMChatService" android:priority="2147483647" service android:enabled="true" android:name="com.gaotai.ydxygwjs.service.PushService" android:process=":push" service android:name="com.tencent.imsdk.session.remote.SessionService" android:process=":network" service android:name="com.tencent.imsdk.session.remote.AssistService"

	android:process=":network" ... 此处省略【1】条数据 ...
解决方案	N/A

3.3.2.3 Broadcast Receiver 最小化特权检测

检测目的	检测应用 Broadcast Receiver
重要等级	高
危害	Broadcast Receiver 设计的初衷是从全局考虑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，所以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，这样会造成应用被攻击，有可能导致应用直接退出，处理逻辑出错等问题。
检测结果	高危
检测详情	总共检测 receiver 配置代码【2】条； 检测到未进行正确配置的代码【2】条； 检测到正确配置的代码【0】条； 未进行正确配置的代码为： receiver android:name="com.gaotai.ydxygwjs.AppRegister" receiver android:name="com.tencent.imsdk.session.SessionBroadcastReceiver"
解决方案	广播发送方通常选择给每个发送 Broadcast Intent 授予 Android 权限；接收方不但需要符合 Intent filter 的接收条件，还要求 Broadcast Receiver 也必须具有特定权限（给发送方授予权限要一致）才能接收（双层过滤）。尽量使用 LocalBroadcastManager，LocalBroadcastManager 只会将广播限定在当前应用程序中。

3.3.2.4 Intent 检测

检测目的	检测应用 Intent 安全性
重要等级	中
危害	应用创建 Intent 传递数据到其他 Activity，如果创建的 Activity 不是在同一个 Task 中打开，就很可能被其他的 Activity 劫持读取到 Intent 内容，跨 Task 的 Activity 通过 Intent 传递敏感信息是不安全的；显示调用和隐式调用都能过在不同应用间传递数据可能造成的风险包括：恶意调用；

	恶意接受数据；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	安全
检测详情	检测出隐式 Intent 跳转【0】条：
解决方案	N/A

3.3.3 数据安全规范检测

3.3.3.1 调试信息检测

检测目的	检测应用是否存在调试信息
重要等级	高
危害	在开发安卓应用时候，添加调试 Log 信息是一个非常常用的手段，打印 Log 也是一个良好的习惯，有助于程序员快速的定位错误位置和错误信息。但是如果发布出去的应用未及关闭 Log 信息的输出，则有可能泄露应用的逻辑处理和一些账号等信息。
检测结果	安全
检测详情	检测出调试信息函数共【0】条：
解决方案	N/A

3.3.3.2 测试数据移除检测

检测目的	检测应用是否存在测试数据
重要等级	高
危害	如果应用里面包含测试数据残留，可能会造成测试账号或者测试信息外泄，如果测试中有重要数据残留，则会造成重要数据泄露。
检测结果	安全
检测详情	检测出测试数据共【0】条。
解决方案	N/A

3.3.3.3 异常处理检测

检测目的	检测应用是否存在异常处理逻辑
重要等级	低
危害	遇到软件没有捕获的异常之后，系统会弹出这个默认的强制关闭对话框。我们当然不希望用户看到这种现象，简直是对用户心灵上的打击，而且

	对我们的 bug 的修复也是毫无帮助的。我们需要的是软件有一个全局的异常捕获器，当出现一个我们没有发现的异常时，捕获这个异常，并且将异常信息记录下来，或者上传到服务器公开发这分析出现异常的具体原因。如果不进行异常捕获则会大大降低用户体验。
检测结果	低危
检测详情	检测到此 APP 未绑定全局 CrashHander
解决方案	添加全部异常捕获类，添加方法比较简单，谷歌官方有相应的使用说明。

3.3.3.4 跨域访问漏洞

检测目的	检测应用是否存在跨域访问漏洞
重要等级	高
危害	攻击者可以利用该漏洞，可远程获取用户隐私数据（包括手机应用数据、照片、文档等敏感信息），还可窃取用户登录凭证，在受害者毫无察觉的情况下实现对 APP 用户账户的完全控制。由于该组件广泛应用于 Android 平台，导致大量 APP 受影响，构成较为严重的攻击威胁。
检测结果	安全
检测详情	
解决方案	N/A

3.3.4 代码安全规范检测

3.3.4.1 硬编码检测

检测目的	检测应用代码中是否使用了硬编码
重要等级	低
危害	大部分程序语言里，可以将一个固定数值定义为一个标记，然后用这个特殊标记来取代变量名称。当标记名称改变时，变量名不变，这样，当重新编译整个程序时，所有变量都不再是固定值，这样就更容易的实现了改变变量的目的。尽管通过编辑器的查找替换功能也能实现整个变量名称的替换，但也很有可能出现多换或者少换的情况，而在计算机程序中，任何小错误的出现都是不可饶恕的。最好的方法是单独为变量名划分空间，来实现这种变化，就如同前面说的那样，将需要改变的变量名暂时用一个定义好的标记名称来代替就是一种很好的方法。通常情况下，都应该避免使用硬编码方法。
检测结果	安全
检测详情	总共检测资源文件中包含 url【0】条
解决方案	N/A