IMG_256

**移动APP安全检测报告**

|  |  |
| --- | --- |
| **APP基本信息** | |
| **软件应用名称** |  |
| **包名** |  |
| **版本号** |  |
| **软件大小** |  |
| **文件MD5** |  |
| **检测完成时间** |  |
| **加固信息** |  |

**北京鼎源科技有限公司**

**二O一六年**

尊敬的客户：您好！

北京鼎源科技有限公司感谢您对我们的信任和支持。现将对您的APP应用的检测报告呈上。

**———————————————————————————————————————**

**报告阅读说明**

本次安全检测报告从应用安全、源码安全、数据安全和漏洞扫描等四个方面对您的APP进行的安全检测。由于检测方法的不同，检测结果可能会有差异。

您的安全检测报告结论是基于您提供的APK文件版本进行的检测，如果您提供的APK版本信息不完整，可能会导致相关检测结论有偏差。

由于检测项目本身的局限性，本次检测结果未发现风险并不代表没有风险，如您有更深层次的检测需求，请及时与我公司联系。

**———————————————————————————————————————**

**APP安全检测报告摘要总结**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 总计 | 高危 | 中危 | 低危 |
| 测评项目数 | 40 | 7 | 19 | 14 |
| 存在问题测评项目数 |  |  |  |  |
| 发现问题 |  |  |  |  |
| 总评 |  | | | |

|  |
| --- |
| **风险比重分布图** |
|  |

**专家建议与指导**

**总体建议**

|  |
| --- |
|  |

**【1】应用安全**

|  |
| --- |
|  |

**【2】源码安全**

|  |
| --- |
|  |

**【3】数据安全**

|  |
| --- |
|  |

**【4】漏洞扫描**

|  |
| --- |
|  |

**APP安全检测依据**

|  |
| --- |
| **《移动应用安全检测基准》** |
| **《移动互联网应用软件安全评估大纲》** |
| **《信息安全技术 公共及商用服务信息系统个人信息保护指南》** |
| **《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》** |

**APP安全检测报告摘要**

|  |  |  |  |
| --- | --- | --- | --- |
| **一、基础检测（自动）** | | | |
| **类别** | **风险评估项** | **风险等级** | **检测结果** |
| **应用安全** | **模拟器检测** | **高危** |  |
| **动态调试检查** | **中危** |  |
| **WebView安全** | **中危** |  |
| **本地拒绝服务** | **中危** |  |
| **Activity安全** | **低危** |  |
| **Broadcast Receiver安全** | **低危** |  |
| **Service安全** | **低危** |  |
| **Content Provider安全** | **低危** |  |
| **Intent安全** | **低危** |  |
| **日志信息检查** | **低危** |  |
| **权限管理** | **低危** |  |
| **动态注册广播** | **低危** |  |
| **反调试保护** | **低危** |  |
| **源码安全** | **程序签名校验检查** | **高危** |  |
| **完整性校验检查** | **高危** |  |
| **代码混淆检查** | **高危** |  |
| **反编译防范检测** | **高危** |  |
| **内存代码安全** | **高危** |  |
| **资源文件保护检查** | **中危** |  |
| **硬编码-密码敏感词编码检查** | **中危** |  |
| **硬编码-密钥敏感词编码检查** | **中危** |  |
| **主配置文件保护检查** | **中危** |  |
| **安全编码规范-调用ROOT权限检查** | **中危** |  |
| **未移除WebView组件系统隐藏接口** | **中危** |  |
| **随机数不安全使用** | **中危** |  |
| **硬编码-敏感字符串检查** | **低危** |  |
| **安全编码规范-加密算法检查** | **低危** |  |
| **安全编码规范-全反射调用检查** | **低危** |  |
| **安全编码规范-明文SQL语句检查** | **低危** |  |
| **数据安全** | **应用数据任意备份** | **高危** |  |
| **内存数据安全** | **高危** |  |
| **存储数据检查** | **中危** |  |
| **远程数据通讯协议** | **中危** |  |
| **Content Provider目录遍历脆弱点** | **中危** |  |
| **Content Provider URI脆弱点** | **中危** |  |
| **卸载清除** | **低危** |  |
| **漏洞** | **电话拨打权限绕过漏洞检查** | **高危** |  |
| **反射漏洞注入风险** | **中危** |  |
| **选择漏洞注入风险** | **中危** |  |
| **HTTPS关闭主机名验证** | **中危** |  |
| **zip文件目录遍历漏洞** | **中危** |  |
| **WebView组件忽略SSL证书验证错误** | **中危** |  |
| **内网测试信息残留** | **低危** |  |
| **恶意行为** | **广告检测** | **高危** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **二、中级检测（手动）** | | | |
| **类别** | **风险评估项** | **风险等级** | **检测结果** |
| **应用安全** | **日志信息渗透** | **高危** | **待渗透测试** |
| **动态调试渗透** | **高危** | **待渗透测试** |
| **Activity劫持** | **高危** | **待渗透测试** |
| **进程保护** | **高危** | **待渗透测试** |
| **支付控制** | **高危** | **待渗透测试** |
| **登录控制** | **高危** | **待渗透测试** |
| **支付密码设置** | **高危** | **待渗透测试** |
| **双因子认证** | **高危** | **待渗透测试** |
| **超时重新授权** | **高危** | **待渗透测试** |
| **密码强度** | **高危** | **待渗透测试** |
| **测试数据包含** | **中危** | **待渗透测试** |
| **第三方SDK安全** | **中危** | **待渗透测试** |
| **源码安全** | **程序签名校验渗透** | **高危** | **待渗透测试** |
| **完整性校验渗透** | **高危** | **待渗透测试** |
| **代码混淆渗透** | **高危** | **待渗透测试** |
| **DEX保护强度渗透** | **高危** | **待渗透测试** |
| **SO保护强度渗透** | **高危** | **待渗透测试** |
| **资源文件保护渗透** | **高危** | **待渗透测试** |
| **业务敏感逻辑渗透** | **高危** | **待渗透测试** |
| **反编译防范渗透** | **高危** | **待渗透测试** |
| **数据安全** | **密码专用键盘保护** | **高危** | **待渗透测试** |
| **存储数据渗透** | **高危** | **待渗透测试** |
| **敏感数据截获** | **高危** | **待渗透测试** |
| **敏感数据残留** | **高危** | **待渗透测试** |
| **数据访问控制** | **高危** | **待渗透测试** |
| **敏感数据加密** | **高危** | **待渗透测试** |
| **远程数据通信加密** | **高危** | **待渗透测试** |
| **数据传输完整性** | **高危** | **待渗透测试** |
| **本地数据通讯安全** | **高危** | **待渗透测试** |
| **转账安全性检测** | **高危** | **待渗透测试** |
| **安装包中敏感信息加密** | **高危** | **待渗透测试** |
| **界面切换后面敏感信息需清空** | **高危** | **待渗透测试** |
| **数据输入敏感数据显示** | **中危** | **待渗透测试** |
| **本地数据通讯权限检查** | **中危** | **待渗透测试** |
| **会话安全** | **中危** | **待渗透测试** |
| **重放攻击** | **中危** | **待渗透测试** |
| **数据输出敏感数据显示** | **低危** | **待渗透测试** |
| **证书验证** | **低危** | **待渗透测试** |
| **漏洞** | **下载任意APK** | **中危** | **待渗透测试** |
| **Webview绕过证书校验** | **中危** | **待渗透测试** |
| **浏览器的intent scheme url攻击检测** | **中危** | **待渗透测试** |
| **手势密码绕过** | **中危** | **待渗透测试** |
| **被调用安装任意apk** | **中危** | **待渗透测试** |
| **被调用卸载任意apk** | **中危** | **待渗透测试** |
| **全局可读写内部文件** | **低危** | **待渗透测试** |
| **恶意行为** | **病毒检测** | **高危** | **待渗透测试** |
| **服务器安全** | **跨权漏洞** | **高危** | **待渗透测试** |
| **SQL注入** | **中危** | **待渗透测试** |
| **XSS跨站脚本** | **中危** | **待渗透测试** |
| **缓冲区溢出** | **中危** | **待渗透测试** |
| **文件上传漏洞** | **中危** | **待渗透测试** |
| **数据库泄露** | **中危** | **待渗透测试** |
| **弱口令漏洞** | **低危** | **待渗透测试** |

**权限信息报告**

|  |  |  |  |
| --- | --- | --- | --- |
| **三、权限信息安全** | | | |
| **类别** | **风险评估项** | **风险等级** | **评估结果** |
| **权限信息安全** | **android.permission.WRITE\_SMS 写短信** | **高危** |  |
| **android.permission.RECEIVE\_SMS 监控接收短信** | **高危** |  |
| **android.permission.READ\_CONTACTS 读取联系人信息** | **高危** |  |
| **android.permission.READ\_SMS**  **读取短信** | **高危** |  |
| **android.permission.SEND\_SMS**  **发送短信** | **高危** |  |
| **com.android.browser.permission.WRITE\_HISTORY\_BOOKMARKS**  **写浏览器书签** | **高危** |  |
| **com.android.browser.permission.READ\_HISTORY\_BOOKMARKS**  **读取浏览器书签** | **中危** |  |
| **com.android.launcher.permission.INSTALL\_SHORTCUT**  **创建快捷方式** | **中危** |  |
| **android.permission.BRICK**  **请求能够禁用设备** | **高危** |  |
| **android.permission.INTERNET 连接网络** | **高危** |  |
| **android.permission.READ\_PHONE\_STATE**  **读取电话状态** | **高危** |  |
| **android.permission.WRITE\_EXTERNAL\_STORAGE**  **写外部存储器（如：SD卡）** | **高危** |  |
| **android.permission.ACCESS\_CHECKIN\_PROPERTIES**  **允许读写访问 "properties"表在checkin数据库中改值可以修改上传** | **中危** |  |
| **android.permission.ACCESS\_LOCATION\_EXTRA\_COMMANDS**  **应用程序访问位置的额外命令** | **中危** |  |
| **android.permission.ACCESS\_MOCK\_LOCATION**  **程序创建模拟位置** | **中危** |  |
| **android.permission.ACCESS\_NETWORK\_STATE**  **访问GSM网络有关信息** | **中危** |  |
| **android.permission.ACCESS\_SURFACE\_FLINGER**  **使用SurfaceFlinger底层特性** | **高危** |  |
| **android.permission.BLUETOOTH 连接到已配对的蓝牙设备** | **中危** |  |
| **android.permission.BLUETOOTH\_ADMIN 程序发现和配对蓝牙设备** | **中危** |  |
| **android.permission.BROADCAST\_STICKY**  **广播常用intents** | **高危** |  |
| **android.permission.CALL\_PRIVILEGED 拨打任何号码包含紧急号码无需通过拨号用户界面需要用户确认** | **高危** |  |
| **android.permission.CHANGE\_COMPONENT\_ENABLED\_STATE**  **改变其他组件的使能状态** | **高危** |  |
| **android.permission.CHANGE\_CONFIGURATION**  **修改当前设置** | **高危** |  |
| **android.permission.CHANGE\_WIFI\_STATE**  **改变Wi-Fi连接状态** | **中危** |  |
| **android.permission.CLEAR\_APP\_CACHE 清除应用缓存** | **高危** |  |
| **android.permission.CLEAR\_APP\_USER\_DATA**  **清除用户设置** | **高危** |  |
| **android.permission.CONTROL\_LOCATION\_UPDATES**  **允许无线模块启用禁止位置更新** | **中危** |  |
| **android.permission.DELETE\_CACHE\_FILES**  **删除缓存文件** | **中危** |  |
| **android.permission.DELETE\_PACKAGES 删除包** | **高危** |  |
| **android.permission.DEVICE\_POWER 访问底层电源管理** | **中危** |  |
| **android.permission.DISABLE\_KEYGUARD**  **禁用键盘锁** | **中危** |  |
| **android.permission.DUMP**  **从系统服务返回状态抓取信息** | **中危** |  |
| **android.permission.EXPAND\_STATUS\_BAR**  **应用在状态栏扩展或收缩** | **中危** |  |
| **android.permission.FACTORY\_TEST 作为一个工厂测试程序** | **中危** |  |
| **android.permission.FLASHLIGHT 访问闪光灯** | **中危** |  |
| **android.permission.FORCE\_BACK 强制后退操作在顶层** | **中危** |  |
| **android.permission.GET\_ACCOUNTS 访问帐户列表** | **中危** |  |
| **android.permission.HARDWARE\_TEST 允许访问硬件** | **中危** |  |
| **android.permission.INJECT\_EVENTS 截获用户事件如按键、触摸、轨迹球** | **高危** |  |
| **android.permission.INSTALL\_PACKAGES**  **安装packages** | **高危** |  |
| **android.permission.MANAGE\_APP\_TOKENS**  **在窗口管理器中管理程序** | **中危** |  |
| **android.permission.PERSISTENT\_ACTIVITY**  **设置其他的activities显示** | **中危** |  |
| **android.permission.PROCESS\_OUTGOING\_CALLS**  **监视、修改有关拨出电话的信息** | **中危** |  |
| **android.permission.READ\_CALENDAR 读取用户日历数据** | **中危** |  |
| **android.permission.READ\_FRAME\_BUFFER**  **抓屏或访问帧缓冲** | **中危** |  |
| **android.permission.READ\_INPUT\_STATE**  **当前按键状态** | **中危** |  |
| **android.permission.READ\_LOGS 读取底层系统日志文件** | **中危** |  |
| **android.permission.READ\_OWNER\_DATA 读取所有者数据** | **中危** |  |
| **android.permission.READ\_SYNC\_SETTINGS**  **读取同步设置** | **中危** |  |
| **android.permission.READ\_SYNC\_STATS 读取同步状态** | **中危** |  |
| **android.permission.REBOOT**  **重新启动设备** | **中危** |  |
| **android.permission.RECEIVE\_BOOT\_COMPLETED**  **接收到ACTION\_BOOT\_COMPLETED** | **中危** |  |
| **android.permission.RECEIVE\_MMS 接收MMS彩信** | **中危** |  |
| **android.permission.RECEIVE\_WAP\_PUSH**  **接收WAP PUSH信息** | **中危** |  |
| **android.permission.RECORD\_AUDIO 录制音频** | **中危** |  |
| **android.permission.REORDER\_TASKS 排列任务** | **中危** |  |
| **android.permission.WRITE\_APN\_SETTINGS**  **写入APN设置** | **中危** |  |
| **android.permission.WRITE\_CALENDAR 写入用户日历数据** | **中危** |  |
| **android.permission.WRITE\_CONTACTS 写入联系人数据** | **中危** |  |
| **android.permission.WRITE\_GSERVICES 修改Google地图服务** | **中危** |  |
| **android.permission.WRITE\_OWNER\_DATA**  **写入所有者数据** | **中危** |  |
| **android.permission.WRITE\_SETTINGS 读取或写入系统设置** | **中危** |  |
| **android.permission.WRITE\_SYNC\_SETTINGS**  **写入同步设置** | **中危** |  |
| **com.android.voicemail.permission.ADD\_VOICEMAIL**  **增加语音邮件** | **中危** |  |
| **android.permission.MOUNT\_UNMOUNT\_FILESYSTEMS**  **挂载、反挂载外部文件系统** | **高危** |  |
| **android.permission.ACCESS\_FINE\_LOCATION**  **通过GPS芯片接收卫星的定位信息** | **中危** |  |
| **android.permission.CALL\_PHONE 拨打电话** | **中危** |  |
| **android.permission.RESTART\_PACKAGES**  **重启其他程序** | **中危** |  |
| **android.permission.SET\_WALLPAPER 设置桌面壁纸** | **中危** |  |
| **android.permission.ACCESS\_COARSE\_LOCATION**  **通过WiFi或移动基站的方式获取用户错略的经纬度信息** | **中危** |  |
| **android.permission.ACCESS\_WIFI\_STATE**  **访问Wi-Fi网络状态信息** | **低危** |  |
| **android.permission.ADD\_SYSTEM\_SERVICE**  **发布系统级服务** | **低危** |  |
| **android.permission.BATTERY\_STATS 更新手机电池统计信息** | **低危** |  |
| **android.permission.BROADCAST\_PACKAGE\_REMOVED**  **在删除应用程序包后广播提示消息** | **低危** |  |
| **android.permission.CAMERA**  **请求访问使用照相设备** | **低危** |  |
| **android.permission.GET\_PACKAGE\_SIZE**  **获取任何package占用空间容量** | **低危** |  |
| **android.permission.GET\_TASKS 获取有关当前或最近运行的任务信息** | **低危** |  |
| **android.permission.INTERNAL\_SYSTEM\_WINDOW**  **允许打开使用系统用户界面的窗口** | **低危** |  |
| **android.permission.MODIFY\_AUDIO\_SETTINGS**  **修改全局音频设置** | **低危** |  |
| **android.permission.SET\_ACTIVITY\_WATCHER**  **控制已经在全局系统中启动的activities** | **低危** |  |
| **android.permission.SET\_ANIMATION\_SCALE**  **修改全局信息比例** | **低危** |  |
| **android.permission.SET\_DEBUG\_APP 配置程序处于调试状态** | **低危** |  |
| **android.permission.SET\_ORIENTATION 底层访问设置屏幕方向和实际旋转** | **低危** |  |
| **android.permission.SET\_PREFERRED\_APPLICATIONS**  **修改列表参数** | **低危** |  |
| **android.permission.SET\_PROCESS\_FOREGROUND**  **强制当前程序运行到前台** | **低危** |  |
| **android.permission.SET\_PROCESS\_LIMIT**  **允许设置最大的运行进程数量** | **低危** |  |
| **android.permission.SET\_TIME\_ZONE 设置时间区域** | **低危** |  |
| **android.permission.STATUS\_BAR 打开、关闭或禁用状态栏及图标** | **低危** |  |
| **android.permission.SUBSCRIBED\_FEEDS\_READ**  **访问订阅RSS Feed内容** | **低危** |  |
| **android.permission.SUBSCRIBED\_FEEDS\_WRITE**  **写入或修改订阅内容的数据库** | **高危** |  |
| **android.permission.VIBRATE**  **访问振动设备** | **低危** |  |
| **android.permission.WAKE\_LOCK 使用WakeLocks使得进程在休眠时从屏幕消失** | **低危** |  |
| **android.permission.READ\_EXTERNAL\_STORAGE**  **读取外部存储** | **低危** |  |
| **android.permission.DIAGNOSTIC 允许程序RW诊断资源** | **低危** |  |
| **android.permission.CHANGE\_NETWORK\_STATE**  **允许程序改变网络连接状态** | **高危** |  |
| **android.permission.MASTER\_CLEAR 清除一切数据** | **高危** |  |
| **android.permission.MODIFY\_PHONE\_STATE**  **允许修改话机状态如电源人机接口等** | **高危** |  |
| **android.permission.SET\_ALWAYS\_FINISH**  **允许程序控制是否活动间接完成在处于后台时** | **低危** |  |
| **android.permission.SET\_WALLPAPER\_HINTS**  **允许程序设置壁纸hits** | **低危** |  |
| **android.permission.SIGNAL\_PERSISTENT\_PROCESSES**  **允许程序请求发送信号到所有显示的进程中** | **高危** |  |
| **android.permission.SYSTEM\_ALERT\_WINDOW**  **允许一个程序打开窗口使用 TYPE\_SYSTEM\_ALERT显示在其他所有程序的顶层** | **高危** |  |
| **android.permission.ACCOUNT\_MANAGER 账户管理获取账户验证信息** | **高危** |  |
| **android.permission.AUTHENTICATE\_ACCOUNTS**  **验证账户允许一个程序通过账户验证方式访问账户管理ACCOUNT\_MANAGER相关信息** | **高危** |  |
| **android.permission.BIND\_APPWIDGET 绑定小插件允许一个程序告诉appWidget服务需要访问小插件的数据库** | **低危** |  |
| **android.permission.BIND\_DEVICE\_ADMIN**  **绑定设备管理请求系统管理员接收者receiver** | **低危** |  |
| **android.permission.BIND\_INPUT\_METHOD**  **绑定输入法请求InputMethodService服务** | **低危** |  |
| **android.permission.BIND\_REMOTEVIEWS**  **绑定RemoteView必须通过RemoteViewsService服务来请求** | **低危** |  |
| **android.permission.BIND\_WALLPAPER 绑定壁纸必须通过WallpaperService服务来请求** | **低危** |  |
| **android.permission.BROADCAST\_SMS 收到短信时广播** | **高危** |  |
| **android.permission.BROADCAST\_WAP\_PUSH**  **WAP PUSH广播** | **高危** |  |
| **android.permission.CHANGE\_WIFI\_MULTICAST\_STATE**  **改变WiFi多播状态** | **高危** |  |
| **android.permission.CWJ\_GROUP 底层访问权限允许CWJ账户组访问底层信息** | **高危** |  |
| **android.permission.CELL\_PHONE\_MASTER\_EX**  **手机优化大师扩展权限** | **高危** |  |
| **android.permission.GLOBAL\_SEARCH 允许全局搜索** | **高危** |  |
| **android.permission.INSTALL\_LOCATION\_PROVIDER**  **安装定位提供** | **低危** |  |
| **android.permission.KILL\_BACKGROUND\_PROCESSES**  **结束后台进程允许程序调用killBackgroundProcesses(String).方法结束后台进程** | **高危** |  |
| **android.permission.MANAGE\_ACCOUNTS 允许程序管理AccountManager中的账户列表** | **高危** |  |
| **android.permission.MTWEAK\_USER 允许mTweak用户访问高级系统权限** | **高危** |  |
| **android.permission.MTWEAK\_FORUM 允许使用mTweak社区权限** | **高危** |  |
| **android.permission.MOUNT\_FORMAT\_FILESYSTEMS**  **格式化可移动文件系统比如格式化清空SD卡** | **高危** |  |
| **android.permission.NFC**  **允许程序执行NFC近距离通讯操作用于移动支持** | **高危** |  |
| **android.permission.com.android.alarm.permission.SET\_ALARM**  **设置闹铃提醒** | **低危** |  |
| **android.permission.UPDATE\_DEVICE\_STATS**  **更新设备状态** | **低危** |  |
| **android.permission.USE\_CREDENTIALS 使用证书** | **高危** |  |
| **android.permission.USE\_SIP**  **使用SIP视频** | **低危** |  |
| **android.permission.WRITE\_SECURE\_SETTINGS**  **允许程序读写系统安全敏感的设置项** | **高危** |  |

**APP安全检测详细报告**

|  |
| --- |
| **应用安全** |
| **检测项** | **模拟器检测** |
| **风险描述** | **评估样本是否可以在模拟器环境下运行** |
| **风险级别** | **高危** |
| **风险危害** | **1.应用可以在模拟器下运行**  **2.可以被定制的模拟器下调试带来被逆向的风险** |
| **评估结论** |  |
| **风险分析** | **由于应用运行过程中没有做相关的模拟器识别和检测功能，导致应用可以在模拟器上运行和调试** |
| **风险详情** |  |
| **处理建议** | **1.对模拟器的IMSI、IDS、默认文件等几个方面进行检测**  **2.基于模拟器CPU信息的检测**  **3.关键路径检测特定模拟器检测**  **4.检测模拟器电量** |

|  |
| --- |
| **应用安全** |
| **检测项** | **动态调试检查** |
| **风险描述** | **应用的android:debuggable属性为true时，应用则可以使用jdb调试，进而可以使用其他工具进行调试** |
| **风险级别** | **中危** |
| **风险危害** | 1. **应用可以在非开发版手机系统中被动态调试** 2. **应用内部信息可以使用jdb命令获取或修改** 3. **应用执行流程可以使用jdb进行分析**   **便于其他工具进行动态调试** |
| **评估结论** |  |
| **风险分析** | **由于应用的调试配置开启，导致应用的调试限制极低，可以使用多种工具动态分析应用的核心流程和敏感数据** |
| **风险详情** |  |
| **处理建议** | **1.将应用中的debuggable属性显式配置为false**  **2.对应用采取反调试保护措施，防止其他工具的调试** |

|  |
| --- |
| **应用安全** |
| **检测项** | **WebView安全** |
| **风险描述** | **评估样本是否存在WebView漏洞被恶意利用** |
| **风险级别** | **中危** |
| **风险危害** | **1.通过javasrriptInterface接口远程挂马**  **2.远程获取shell** |
| **评估结论** |  |
| **风险分析** | **在android的sdk中封装了webView控件。这个控件主要用开控制的网页浏览。在程序中装载webView控件，可以设置属性**  **（颜色，字体等）。类似PC下directUI的功能。在webView 下有一个非常特殊的接口函数addJavascriptInterface。能实现**  **本地java和js的交互。利用addJavascriptInterface这个接口函数可实现穿透webkit控制android 本机。** |
| **风险详情** |  |
| **处理建议** | **1.Android 4.2 （api17）已经开始采用新的接口函数java中应该叫方法：@JavascriptInterface 代替addjavascriptInterface, 有些android 2.3不再升级，浏览器需要兼容。**  **2.在使用js2java的bridge时候，需要对每个传入的参数进行验证，屏蔽攻击代码。**  **3.控制相关权限或者尽可能不要使用js2java的bridge。** |

|  |
| --- |
| **应用安全** |
| **检测项** | **本地拒绝服务** |
| **风险描述** | **攻击者通过intent发送空数据、异常或畸形数据给受害者应用，导致其崩溃** |
| **风险级别** | **中危** |
| **风险危害** | **本地拒绝服务漏洞不仅可以导致安全防护等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），而且也可被竞争方应用利用来攻击，使得自己的应用崩溃，造成不同程度的经济利益损失。** |
| **评估结论** |  |
| **风险分析** | **Android应用本地拒绝服务漏洞源于程序没有对Intent.getXXXExtra()获取的异常或者畸形数据处理时没有进行异常捕获，从而导致攻击者可通过向受害者应用发送此类空数据、异常或者畸形数据来达到使该应用崩溃的目的** |
| **风险详情** |  |
| **处理建议** | **1.在使用Intent获取Extra数据时增加异常处理，防止抛出异常引发崩溃**  **2.在使用getAction时对返回值进行null检查后再使用**  **3.在使用Intent获取Array、List类的的数据时，检查长度后再做操作** |

|  |
| --- |
| **应用安全** |
| **检测项** | **Activity安全** |
| **风险描述** | **公开暴露的Activity组件可以被任意应用启动** |
| **风险级别** | **低危** |
| **风险危害** | **1.绕过本地认证**  **2.本地拒绝服务**  **3.界面劫持**  **4.UXSS**  **5.隐式启动Intent包含敏感数据**  **6.Fragment注入（绕过PIN+拒绝服务）**  **7.WebView RCE** |
| **评估结论** |  |
| **风险分析** | **由于Activity组件公开暴露，恶意应用可以在外部通过Intent隐式启动目标Activity或者构造能使Activity功能失效的Intent进行拒绝服务攻击等** |
| **风险详情** |  |
| **处理建议** | 1. **App内使用的私有Activity不应配置intent-filter，如果配置了intent-filter需设置exported属性为false** 2. **使用默认taskAffinity** 3. **使用默认launchMode** 4. **启动Activity时不设置intent的FLAG\_ACTIVITY\_NEW\_TASK标签** 5. **谨慎处理接收的intent以及其携带的信息** 6. **签名验证内部（in-house）app** 7. **当Activity返回数据时需注意目标Activity是否有泄露信息的风险** 8. **目的Activity十分明确时使用显式启动** 9. **谨慎处理Activity返回的数据，目的Activity返回的数据可能是恶意应用伪造的** 10. **验证目标Activity是否恶意app，以免受到intent欺骗，可用hash签名验证**   **尽可能不发送敏感信息，应考虑到启动public Activity中intent的信息均有可能被恶意应用窃取的风险** |

|  |
| --- |
| **应用安全** |
| **检测项** | **Broadcast Receiver安全** |
| **风险描述** | **公开暴露的Broadcast Receiver组件可以接收所有app发出的广播** |
| **风险级别** | **低危** |
| **风险危害** | **1.伪造消息代码执行**  **2.拒绝服务**  **3.敏感信息泄露**  **4.权限绕过** |
| **评估结论** |  |
| **风险分析** | **由于广播接收器的exported属性设置不当且配置了intent-filter项目，导致恶意应用可以构造隐式Intent攻击广播接收器；利用广播传输敏感信息时，容易导致恶意应用截获载体Intent导致敏感数据丢失** |
| **风险详情** |  |
| **处理建议** | 1. **私有广播接收器设置exported属性为false，并且不配置intent-filter（私有广播接收器依然能接收到同UID的广播）** 2. **对接收来的广播进行验证** 3. **内部app之间的广播使用protectionLevel=’signature’验证其是否真的是内部app** 4. **发送广播时需注意接收app是否会泄露信息** 5. **发送的广播包含敏感信息时需指定广播接收器，使用显示意图或setPackage()接口函数** 6. **Sticky broadcast粘性广播中不应该包含敏感信息** 7. **Ordered Broadcast建议设置接收权限receiverPermission，避免恶意应用设置高优先级抢收此广播后并执行abortBroadcast()方法** |

|  |
| --- |
| **应用安全** |
| **检测项** | **Service安全** |
| **风险描述** | **公开暴露的service组件可以被其他应用访问** |
| **风险级别** | **低危** |
| **风险危害** | **1.权限提升**  **2.services劫持**  **3.拒绝服务**  **4.消息伪造** |
| **评估结论** |  |
| **风险分析** | **由于service组件公开且对访问数据的过滤处理不当的话，恶意应用可以构造隐式Intent对service组件进行攻击，导致组件出现拒绝服务或执行意外操作** |
| **风险详情** |  |
| **处理建议** | **1.只有应用自身使用的service应设置为私有**  **2.service接收到的数据需谨慎处理**  **3.内部service需使用签名级别的protectionLevel来校验内部应用的调用**  **4.不应在service创建(onCreate方法被调用)的时候决定是否提供服务，应在onStartCommand/onBind/onHandleIntent等方法被调用的时候判断**  **5.当service返回数据时，应判断数据接收app是否有信息泄露的风险**  **6.有明确的服务需调用时要使用显式Intent**  **7.尽量不发送敏感信息**  **8.合作service需对合作公司的app签名做校验** |

|  |
| --- |
| **应用安全** |
| **检测项** | **Content Provider安全** |
| **风险描述** | **公开暴露的Content Provider组件可以被其他APP访问，如果此Content Provider的实现有问题，则可能产生任意数据访问、SQL注入、目录遍历等风险** |
| **风险级别** | **低危** |
| **风险危害** | **1.私有权限定义错误导致数据被任意访问（定义了私有权限，但没有定义私有权限的级别，或定义权限的级别不够，导致恶意应用只要声明这个权限就能够访问到相应的Content Provider提供的数据，造成数据泄露）**  **2.本地SQL注入**  **3.目录遍历漏洞(设置访问权限有问题，没有对传入的Uri进行限制和过滤)** |
| **评估结论** |  |
| **风险分析** | **由于Content Provider组件的exported属性设置不当，权限设置不妥，导致恶意应用可以任意访问数据；对于使用SQLite存储的数据，恶意应用可以构造注入SQL语句，对查询方式有问题的应用进行SQL注入攻击** |
| **风险详情** |  |
| **处理建议** | 1. **在设计APP时，对于用户隐私数据或其他重要数据等不必要提供给外部应用使用的，要在AndroidManifest文件中将其exported属性显式的设为false(Content Provider组件在Android2.2(API Level 8)系统上无法设为不导出，建议声明最低SDK版本为8以上；API Level 17以下的所有应用的exported属性默认值为true，对于不必要导出的组件，其exported属性需显式设为false)** 2. **正确定义私有权限(protectionLevel属性尽量设置为signature)** 3. **防止本地SQL注入(一定不要使用拼接来组装SQL语句)** 4. **防止目录遍历（去除组件中不必要的openFile接口；过滤限制** 5. **域访问，对访问的目标文件的路径进行有效判断）**   **通过检测签名来授权合作方应用访问(将合作方APP的签名Hash值预埋在提供Provider的APP中，请求访问时检查签名，签名匹配才能访问)** |

|  |
| --- |
| **应用安全** |
| **检测项** | **Intent安全** |
| **风险描述** | **评估样本是否存在Intent漏洞使被其他程序恶意调用** |
| **风险级别** | **低危** |
| **风险危害** | **1.恶意调用**  **2.恶意接受数据**  **3.仿冒应用，例如（恶意钓鱼，启动登录界面）**  **4.恶意发送广播、启动应用服务。**  **5.调用组件，接受组件返回的数据**  **6.拦截有序广播** |
| **评估结论** |  |
| **风险分析** | **在Android上的Intent-based攻击很普遍，这种攻击轻则导致应用程序崩溃，重则可能演变提权漏洞。当然，通过静态特征**  **匹配，Intent-Based的恶意样本还是很容易被识别出来的。然而最近出现了一种基于Android Browser的攻击手**  **段——Intent Scheme URLs攻击。这种攻击方式利用了浏览器保护措施的不足，通过浏览器作为桥梁间接实现Intend-**  **Based攻击。相比于普通Intend-Based攻击，这种方式极具隐蔽性，而且由于恶意代码隐藏WebPage中，传统的特征匹配**  **完全不起作用。除此之外，这种攻击还能直接访问跟浏览器自身的组件（无论是公开还是私有）和私有文件，比**  **如cookie文件，进而导致用户机密信息的泄露。** |
| **风险详情** |  |
| **处理建议** | 1. **最小化组件暴露** 2. **设置组件访问权限** 3. **暴露组件的代码检查**   **4.利用Intent.parseUri解析uri，获取原始的intent对象**  **5.通过Context.startActivityIfNeeded或者Context.startActivity发送intent** |

|  |
| --- |
| **应用安全** |
| **检测项** | **日志信息检查** |
| **风险描述** | **评估样本是否存在日志泄露的漏洞** |
| **风险级别** | **低危** |
| **风险危害** | **通过logcat可以查看应用中的日志信息，如果日志使用不当可能造成用户数据的泄露** |
| **评估结论** |  |
| **风险分析** | **android.permission.READ\_LOGS:app读取日志权限，android 4.1之前版本通过申请READ\_LOGS权限就可以读取其他应**  **用的log了。但是谷歌发现这样存在安全风险，于是android 4.1以及之后版本，即使申请了READ\_LOGS权限也无法读取**  **其他应用的日志信息了。4.1版本中 Logcat的签名变为“signature|system|development”了，这意味着只有系统签名的app或**  **者root权限的app才能使用该权限。普通用户可以通过ADB查看所有日志。** |
| **风险详情** |  |
| **处理建议** | **关闭调试日志调用，或者确保日志的输出使用了正确的级别，涉及敏**  **感数据的日志信息在发布版本中被关闭** |

|  |
| --- |
| **应用安全** |
| **检测项** | **权限管理** |
| **风险描述** | **评估样本是否存在app权限控制高于实际使用所需权限控制级别** |
| **风险级别** | **低危** |
| **风险危害** | **1.其他程序越权访问此应用**  **2.被其他程序运行时篡改** |
| **评估结论** |  |
| **风险分析** | **没有设置合理的权限控制**  **normal：低风险权限，在安装的时候，系统会自动授予权限给 application。**  **dangerous：高风险权限，系统不会自动授予权限给 app，在用到的时候，会给用户提示。**  **signature：签名权限，在其他 app 引用声明的权限的时候，需要保证两个 app 的签名一致。这样系统就会自动授予权限给第三方 app，而不**  **提示给用户。**  **signatureOrSystem：这个权限是引用该权限的 app 需要有和系统同样的签名才能授予的权限，一般不推荐使用。** |
| **风险详情** |  |
| **处理建议** | 1. **最小化权限控制** 2. **使暴露的组件修改权限**   **建议使用signature权限，部分源代码未注明的情况下默认使用normal权限。** |

|  |
| --- |
| **应用安全** |
| **检测项** | **动态注册广播** |
| **风险描述** | **使用registerReceiver动态注册的广播在组件的生命周期里是默认导出的。导出的广播可以导致拒绝服务、数据泄漏或是越权调用。** |
| **风险级别** | **低危** |
| **风险危害** | **1.本地APP中广播外泄**  **2.外部广播传递到本地APP中** |
| **评估结论** |  |
| **风险分析** | **Android 可以在配置文件中声明一个receiver或者动态注册一个receiver来接收广播信息，攻击者假冒APP构造广播发送给被攻击的receiver，是被攻击的APP执行某些敏感行为或者返回敏感信息等，如果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，会造成用户的信息泄漏甚至是财产损失** |
| **风险详情** |  |
| **处理建议** | **1.通过给将要传递的广播绑定权限**  **2.对接收来的广播进行验证，返回结果时需注意接收APP是否会泄露信息** |

|  |
| --- |
| **应用安全** |
| **检测项** | **反调试保护** |
| **风险描述** | **为了防止 APK 被动态调试，可以检测是否有调试器连接。Android 系统在 android.os.Debug 类中提供了 isDebuggerConnected()方法，用于检测是否有调试器连接。可以在 Application 类中调用 isDebuggerConnected()方法，判断是否有调试器连接，如果有，直接退出程序** |
| **风险级别** | **低危** |
| **风险危害** | **应用未设置启用反调试保护机制，恶意攻击者可以反编译源程序后，在程序中任意设置断点并进行动态调试，窥探客户端的数据流和工作流。大大降低了黑客分析程序逻辑的难度，导致敏感数据加密逻辑被分析** |
| **评估结论** |  |
| **风险分析** | **由于业务考虑或开发策略，选择了信任所有证书就会引起问题** |
| **风险详情** |  |
| **处理建议** | **建议增加反调试保护机制** |

|  |
| --- |
| **源码安全** |
| **检测项** | **程序签名校验检查** |
| **风险描述** | **应用存在重新打包和重新签名的安全风险，为了提高安全性有必要对签名信息进行校验** |
| **风险级别** | **高危** |
| **风险危害** | 1. **应用可以被篡改内容后重新签名发布** 2. **应用可以被植入恶意代码后重新签名发布** |
| **评估结论** |  |
| **风险分析** | **应用没有添加原始签名的校验的话，将导致应用被二次打包和重新签名的攻击** |
| **风险详情** |  |
| **处理建议** | 1. **Native层本地签名校验** 2. **服务器校验** |

|  |
| --- |
| **源码安全** |
| **检测项** | **完整性校验检查** |
| **风险描述** | **应用很容易被恶意篡改后进行二次打包重新发布，存在极强的完整性破坏风险** |
| **风险级别** | **高危** |
| **风险危害** | **应用容易被反编译篡改和二次打包发布** |
| **评估结论** |  |
| **风险分析** | **由于应用没有采取必要的防反编译保护手段和二次打包校验措施，导致应用容易被反编译篡改和二次打包发布** |
| **风险详情** |  |
| **处理建议** | **1.对应用添加保护标志，使反编译操作失效**  **2.对应用运行时添加校验，使运行时失效** |

|  |
| --- |
| **源码安全** |
| **检测项** | **代码混淆检查** |
| **风险描述** | **没有经过混淆加密的DEX文件很容易通过反编译工具还原为smali文件或java文件，对于恶意逆向分析提供便利** |
| **风险级别** | **高危** |
| **风险危害** | **DEX文件中的逻辑容易暴露，核心算法和敏感数据容易被窃取** |
| **评估结论** |  |
| **风险分析** | **由于DEX文件没有经过混淆加密保护，应用容易通过反编译工具还原为java代码，根据其函数名和类名等信息可以预测应用行为分析应用功能** |
| **风险详情** |  |
| **处理建议** | **1.开发中使用proguard对应用java源码进行混淆加密编译**  **2.在发布后对DEX文件进行更高强度的混淆加密** |

|  |
| --- |
| **源码安全** |
| **检测项** | **反编译防范检测** |
| **风险描述** | **没有经过反编译保护可能会使恶意用户获取程序源码** |
| **风险级别** | **高危** |
| **风险危害** | **恶意用户获取程序源码可能会知晓程序的内部逻辑等重要信息** |
| **评估结论** |  |
| **风险分析** | **没有经过反编译保护可能会使恶意用户获取程序源码** |
| **风险详情** |  |
| **处理建议** | **对程序进行加壳保护，在Manifest文件中加入不存在的资源引用。** |

|  |
| --- |
| **源码安全** |
| **检测项** | **内存代码安全** |
| **风险描述** | **内存中的代码可以被捕获和篡改** |
| **风险级别** | **高危** |
| **风险危害** | **用户敏感逻辑泄露** |
| **评估结论** |  |
| **风险分析** | **内存中的敏感逻辑可以被篡改，影响业务逻辑的正常运行，危害极大** |
| **风险详情** |  |
| **处理建议** | **对应用进行加固，对内存中的代码进行校验防止被篡改。** |

|  |
| --- |
| **源码安全** |
| **检测项** | **资源文件保护检查** |
| **风险描述** | **没有经过资源文件保护可能会使恶意用户获取资源文件** |
| **风险级别** | **中危** |
| **风险危害** | **资源可能被恶意用户获取** |
| **评估结论** |  |
| **风险分析** | **没有经过资源文件保护可能会使恶意用户获取资源文件** |
| **风险详情** |  |
| **处理建议** | **根据资料对资源文件进行保护** |

|  |
| --- |
| **源码安全** |
| **检测项** | | **硬编码-密码敏感词编码检查** |
| **风险描述** | | **源码中用户名密码等敏感信息用具有固定含有的名称表示** |
| **风险级别** | | **中危** |
| **风险危害** | | **用户名密码等敏感信息如若用具有特定含义的名称命名容易被攻击者进行跟踪测试，进而影响应用安全** |
| **评估结论** | |  |
| **风险分析** | | **用户名，密码等敏感词被作为关键词在源码中搜索后作为对象进行跟踪，动态调试时根据关键字的运行记录可以定位关键方法的位置。** |
| **风险详情** | |  |
| **处理建议** | | **1.利用无意义的变量名替换敏感词，做好对比记录**  **2.对敏感词加密** |

|  |
| --- |
| **源码安全** |
| **检测项** | | **硬编码-密钥敏感词编码检查** |
| **风险描述** | | **源码中密钥方法等敏感词被跟踪调试的风险** |
| **风险级别** | | **中危** |
| **风险危害** | | **源码接口，方法参数等需要加密用到密钥方法被跟踪调试，影响应用关键方法的安全** |
| **评估结论** | |  |
| **风险分析** | | **Cipher类中的方法如getProvider() getAlgorithm()等作为关键词搜索到的参数等，可作为跟踪调试的对象，又如keyGeneratord方法可对生成的key进行加密** |
| **风险详情** | |  |
| **处理建议** | | **去除敏感词表示，更换变量名** |

|  |
| --- |
| **源码安全** |
| **检测项** | | **主配置文件保护检查** |
| **风险描述** | | **Apk可能被反编译和修改** |
| **风险级别** | | **中危** |
| **风险危害** | | **没有进行主配置文件保护的程序可能被轻易的反编译** |
| **评估结论** | |  |
| **风险分析** | | **由于配置文件中存在着大量的信息，例如服务名、Activity名等等，如果被反编译了，可能会泄露APK内部的一些信息。此外，将AndroidManifest文件反编译后加上debuggable标识，再对程序进行重打包，就有可能对程序进行非法的调试，进而进行破解。** |
| **风险详情** | |  |
| **处理建议** | | **在AndroidManifest文件中添加不存在的资源标识。** |

|  |
| --- |
| **源码安全** |
| **检测项** | | **安全编码规范-调用ROOT权限检查** |
| **风险描述** | | **恶意应用加入Root用户组后存在感染系统和其他应用的风险** |
| **风险级别** | | **中危** |
| **风险危害** | | **获得Root权限后以便于进行搜索查询注入等操作，影响手机安全** |
| **评估结论** | |  |
| **风险分析** | | **需要调用Root权限的应用除了部分安全应用外大部分均为恶意应用或伪装成普通应用的恶意应用，该类应用如若获得Root权限将会对系统和系统内的应用，造成账户丢失，数据遗失等问题** |
| **风险详情** | |  |
| **处理建议** | | **限制不必要的Root权限** |

|  |
| --- |
| **源码安全** |
| **检测项** | | **未移除WebView组件系统隐藏接口** |
| **风险描述** | | **android webview组件包含3个隐藏的系统接口：searchBoxJavaBridge\_, accessibilityTraversal以及accessibility，恶意程序可以利用它们实现远程代码执行** |
| **风险级别** | | **中危** |
| **风险危害** | | **攻击者可以利用这个实例执行远程代码** |
| **评估结论** | |  |
| **风险分析** | | **当BrowserFrame初始化的时候，会创建一个 android.webkit.SearchBoxImpl实例，并将此实例使用searchBoxJavaBridge\_这个名字添加为JavaScript Object，而攻击者可以利用这个实例执行远程代码** |
| **风险详情** | |  |
| **处理建议** | | **请通过显示调用removeJavascriptInterface移除这三个系统隐藏接口** |

|  |
| --- |
| **源码安全** |
| **检测项** | | **随机数不安全使用** |
| **风险描述** | | **调用SecureRandom类中的setSeed方法** |
| **风险级别** | | **中危** |
| **风险危害** | | **生成的随机数具有确定性，存在被破解的可能性** |
| **评估结论** | |  |
| **风险分析** | | **在调用SecureRandom类的构造函数SecureRandom(byte[] seed)和setSeed()方法设置随机种子，这两种方式都会导致生成的随机数可以预测，导致后续依赖于该随机数的加密不安全** |
| **风险详情** | |  |
| **处理建议** | | **1.不使用setSeed方法**  **2.使用/dev/urandom或者/dev/random来初始化伪随机数生成器** |

|  |
| --- |
| **源码安全** |
| **检测项** | | **硬编码-敏感字符串检查** |
| **风险描述** | | **当用户在使用应用的过程中，输入库中敏感字符串以后的处理机制** |
| **风险级别** | | **低危** |
| **风险危害** | | **敏感字符串不做处理，将影响使用应用的用户使用环境** |
| **评估结论** | |  |
| **风险分析** | | **对于敏感字符串，国家规定和谐的词语以及客户定制的敏感词不进行处理可能会违反国家政策，破坏应用的使用环境** |
| **风险详情** | |  |
| **处理建议** | | **在应用中添加方法，根据词库屏蔽敏感字符串** |

|  |
| --- |
| **源码安全** |
| **检测项** | | **安全编码规范-加密算法检查** |
| **风险描述** | | **检查应用中是否使用了加密算法对关键信息进行保护** |
| **风险级别** | | **低危** |
| **风险危害** | | **1.暴露关键信息**  **2.暴露重要逻辑** |
| **评估结论** | |  |
| **风险分析** | | **在代码的关键点如登录注册等需要与后台进行交互的位置上使用加密算法利于保护用户信息以及关键代码实现，** |
| **风险详情** | |  |
| **处理建议** | | **1.不要使用自定义的加密算法**  **2.采用强度足够的加密算法进行加密操作**  **3.对加密算法逻辑进行保护** |

|  |
| --- |
| **源码安全** |
| **检测项** | **安全编码规范-全反射调用检查** |
| **风险描述** | **评估样本是否存在不安全的全反射调用** |
| **风险级别** | **低危** |
| **风险危害** | **1.木马攻击**  **2.信息泄露**  **3.拒绝服务** |
| **评估结论** |  |
| **风险分析** | **由于使用不安全的全反射调用，导致恶意代码执行** |
| **风险详情** |  |
| **处理建议** | **1.如果无需与JS交互，请删除对addJavascriptInterface函数的调用**  **2.在载入页面时对URL进行白名单判定，只有存在白名单中的域才允许导出或调用相关的Java类或方法** |

|  |
| --- |
| **源码安全** |
| **检测项** | **安全编码规范-明文SQL语句检查** |
| **风险描述** | **评估样本app编码中是否出现不安全的SQL语句** |
| **风险级别** | **低危** |
| **风险危害** | **1.SQL注入攻击**  **2.脱库攻击**  **3.数据泄露攻击** |
| **评估结论** |  |
| **风险分析** | **在涉及数据的操作中，存在不安全的SQL语句，需要遍历检查** |
| **风险详情** |  |
| **处理建议** | **1.少用空值作为查询条件**  **2.对数字型的SQL查询采用明确的数字型强制类型转换**  **3.对字符型的参数进行转移后，能防止攻击者输入单引号、双引号、反斜线等“闭合类字符”进行闭合注入**  **4.不允许访问系统变量**  **5.不允许访问系统函数**  **6.禁止永真条件**  **7. 不允许访问系统表** |

|  |
| --- |
| **数据安全** |
| **检测项** | **应用数据任意备份** |
| **风险描述** | **AndroidManifest.xml中的android:allowBackup属性设置不当会导致adb命令backup和restore的使能，可以备份和恢复应用程序数据** |
| **风险级别** | **高危** |
| **风险危害** | **1.应用数据可以通过adb backup命令备份出来**  **2.备份出来的数据可以被解密破解**  **3.应用中的敏感数据会泄露**  **恢复备份的数据后，应用可以使用备份时的数据** |
| **评估结论** |  |
| **风险分析** | **由于AndroidManifest.xml中的android:allowBackup属性设置不当，应用中的敏感数据可以被备份到本地，导致数据被窃取和泄露** |
| **风险详情** |  |
| **处理建议** | **将AndroidManifest.xml中的android:allowBackup属性显式设置为false** |

|  |
| --- |
| **数据安全** |
| **检测项** | **内存数据安全** |
| **风险描述** | **评估样本是否存在内存数据安全问题** |
| **风险级别** | **高危** |
| **风险危害** | **用户信息、密码等敏感重要的信息明文存储在Shared Preferences文件中，导致攻击者可通过root手机来查看敏感信息。** |
| **评估结论** |  |
| **风险分析** | **使用MODE\_WORLD\_READABLE模式创建Shared Preferences文件，使得其他应用对该Shared Preferences文件具备可读的权限。使用MODE\_WORLD\_WRITEABLE模式创建Shared Preferences文件并含有“android:sharedUserId”属性值，使得其他应用对该应用的Shared Preferences文件具备可写的权限。在具备root权限的程序或用户对任何应用程序通过任意模式创建的的Shared Preferences文件都具有可读可写的权限。** |
| **风险详情** |  |
| **处理建议** | **1.避免使用MODE\_WORLD\_WRITEABLE和MODE\_WORLD\_READABLE模式创建进程间通信的**  **文件，此处即为Shared Preferences；**  **2避免将密码等敏感数据信息明文存储在Shared Preferences中** |

|  |
| --- |
| **数据安全** |
| **检测项** | **存储数据检查** |
| **风险描述** | **本地存储的数据容易被恶意用户的分析和破解** |
| **风险级别** | **中危** |
| **风险危害** | **本地存储的数据在没有经过加密措施处理时，很容易被相关工具打开，造成敏感信息泄露和数据篡改侵害** |
| **评估结论** |  |
| **风险分析** | **由于应用默认本地存储的数据是没有经过加密处理的，本地数据容易遭受泄露和篡改侵害** |
| **风险详情** |  |
| **处理建议** | 1. **尽量不要把敏感数据存储在本地，把用户名密码存储在keystore内** 2. **ContentProvider要使用带参数的数据操作，防止SQL注入** |

|  |
| --- |
| **数据安全** |
| **检测项** | **远程数据通讯协议** |
| **风险描述** | **在远程数据通讯过程中，使用http协议传输数据时，所有数据均为明文传输** |
| **风险级别** | **中危** |
| **风险危害** | **1.传输数据容易被截获进行抓包分析**  **2.数据包中的敏感信息容易被分析篡改** |
| **评估结论** |  |
| **风险分析** | **由于没有使用加密协议，数据包内容没有得到有效保护，导致传输中的敏感信息容易被分析篡改** |
| **风险详情** |  |
| **处理建议** | **1.尽量使用https等加密协议进行数据传输**  **2.数据包中的敏感信息不能用明文传输** |

|  |
| --- |
| **数据安全** |
| **检测项** | **Content Provider目录遍历脆弱点** |
| **风险描述** | **评估样本是否存在Content Provider 目录遍历脆弱点漏洞使被其他程序恶意调用** |
| **风险级别** | **中危** |
| **风险危害** | **攻击者利用该应用暴露的Content Provider的openFile()接口进行文件目录遍历以达到访问任意可读文件的目的** |
| **评估结论** |  |
| **风险分析** | **Android Content Provider存在文件目录遍历安全漏洞，该漏洞源于对外暴露Content Provider组件的应用，没有对Content Provider组件的访问进行权限控制和对访问的目标文件的Content Query Uri进行有效判断，攻击者可以利用该应用暴露的Content Provider的openFile()接口进行文件目录遍历以达到访问任意可读文件的目的** |
| **风险详情** |  |
| **处理建议** | **1.将不必要导出的Content Provider设置为不导出**  **2.去除没有必要的OpenFile()接口**  **3.过滤限制跨域访问，对访问的目标文件的路径进行有效判断**  **4.设置权限来进行内部应用通过Content Provider的数据共享** |

|  |
| --- |
| **数据安全** |
| **检测项** | **Content Provider URI脆弱点** |
| **风险描述** | **评估样本是否存在Content Provider URI脆弱点漏洞使被其他程序恶意调用** |
| **风险级别** | **中危** |
| **风险危害** | **攻击者利用该应用暴露的Content Provider的openFile()接口进行文件目录遍历以达到访问任意可读文件的目的** |
| **评估结论** |  |
| **风险分析** | **content URI 是一个标志provider中的数据的URI．Content URI中包含了整个provider的以符号表示的名字(它的authority) 和指向一个表的名字(一个路径)。当你调用一个客户端的方法来操作一个provider中的一个表，指向表的content URI是参数之一。** |
| **风险详情** |  |
| **处理建议** | **1.minSdkVersion不低于9**  2. **不向外部app提供的数据的私有content provider设置exported=“false”避免组件暴露(编译api小于17时更应注意此点)**  **3.使用参数化查询避免注入**  **4.内部app通过content provid交换数据设置protectionLevel=“signature”验证签名**  **5.公开的content provider确保不存储敏感数据**  **6. Uri.decode() before use ContentProvider.openFile()**  **提供asset文件时注意权限保护** |

|  |
| --- |
| **漏洞** |
| **检测项** | **电话拨打权限绕过漏洞检查** |
| **风险描述** | **com.android.phone.PhoneGlobals$NotificationBroadcastReceiver是导出的且没有做任何的权限限制，任意应用都可以发送intent来调用它** |
| **风险级别** | **高危** |
| **风险危害** | **恶意应用可以通过发送构造的intent来调用NotificationBroadcastReceiver实现对指定电话号码的拨打** |
| **评估结论** |  |
| **风险分析** | **由于android开发人员的疏忽，BroadcastReceiver导出应该在其标签中加上属性android:exported=”false”,但开发人员漏掉了”android:”，写成了exported=”false”，这样的属性是不起作用的，而包含有intent filters的BroadcastReceiver默认是导出的，从而导致此漏洞的发生** |
| **风险详情** |  |
| **处理建议** | **1.代码审计应用中是否被恶意植入了相关调用的代码**  **2.尽量使用已修复该漏洞的系统版本** |

|  |
| --- |
| **漏洞** |
| **检测项** | **反射漏洞注入风险** |
| **风险描述** | **ContentProvider组件访问SQL数据时SQL语句可以被进行反射型注入** |
| **风险级别** | **中危** |
| **风险危害** | **SQL注入会引起SQL数据的泄露，导致敏感信息被访问** |
| **评估结论** |  |
| **风险分析** | **由于SQL语句的处理不规范，导致SQL反射注入风险的存在** |
| **风险详情** |  |
| **处理建议** | **1.使用SQL参数化查询** |

|  |
| --- |
| **漏洞** |
| **检测项** | **选择漏洞注入风险** |
| **风险描述** | **ContentProvider组件访问SQL数据时SQL语句可以被进行选择型注入** |
| **风险级别** | **中危** |
| **风险危害** | **SQL注入会引起SQL数据的泄露，导致敏感信息被访问** |
| **评估结论** |  |
| **风险分析** | **由于SQL语句的处理不规范，导致SQL选择注入风险的存在** |
| **风险详情** |  |
| **处理建议** | **1.使用SQL参数化查询** |

|  |
| --- |
| **漏洞** |
| **检测项** | **HTTPS关闭主机名验证** |
| **风险描述** | **构造HttpClient时，设置HostnameVerifier时参数使用ALLOW\_ALL**  **\_HOSTNAME\_VERIFIER或空的HostnameVerifier** |
| **风险级别** | **中危** |
| **风险危害** | **关闭主机名校验可以导致黑客使用中间人攻击获取加密内容** |
| **评估结论** |  |
| **风险分析** | **由于业务考虑或开发策略，选择了信任所有证书就会引起问题** |
| **风险详情** |  |
| **处理建议** | **1.尽量采用校验服务器证书的方式实现业务**  **2.对传输的数据进行检验** |

|  |
| --- |
| **漏洞** |
| **检测项** | **zip文件目录遍历漏洞** |
| **风险描述** | **方法的返回值中包含有”../”跳转符，需要特别注意不要将文件写到了目标文件夹之外。如果不对”../”跳转符做过滤，就有可能遍历目录，在解压zip文件时以本app的权限覆盖任意文件** |
| **风险级别** | **中危** |
| **风险危害** | **如果没有对 zipEntry.getName进行检查，盲目解压创建文件，将会穿越目录建立文件** |
| **评估结论** |  |
| **风险分析** | **在生成文件时使用了zipEntry.getName()函数，但未过滤getName()函数的返回值是否含有的上级目录字符串(../),攻击者可构造zip文件通过在getName()中包含../从而改变文件的存放位置** |
| **风险详情** |  |
| **处理建议** | **在使用zipEntry.getName()生成文件时，过滤上级目录字符串（../）** |

|  |
| --- |
| **漏洞** |
| **检测项** | **WebView组件忽略SSL证书验证错误** |
| **风险描述** | **WebView调用onReceivedSslError方法时，直接执行handler.proceed()来忽略该证书错误** |
| **风险级别** | **中危** |
| **风险危害** | **忽略SSL证书错误可能引起中间人攻击** |
| **评估结论** |  |
| **风险分析** | **Android WebView组件加载网页发生证书认证错误时，会调用WebViewClient类的onReceivedSslError方法，如果该方法实现调用了handler.proceed()来忽略该证书错误，则会受到中间人攻击的威胁，可能导致隐私泄露** |
| **风险详情** |  |
| **处理建议** | **不要重写onReceivedSslError方法， 或者对于SSL证书错误问题按照业务场景判断，避免造成数据明文传输情况** |

|  |
| --- |
| **漏洞** |
| **检测项** | **内网测试信息残留** |
| **风险描述** | **应用文件中存在残留的调试信息或调试网址，可能被其他恶意用户利用和分析** |
| **风险级别** | **低危** |
| **风险危害** | **1.调试信息暴露可以被用于分析应用功能实现方法**  **2.调试网址暴露可以被用于分析和渗透应用的测试服务器** |
| **评估结论** |  |
| **风险分析** | **由于应用文件中存在残留的调试信息或调试网址，恶意用户可以通过分析调试信息和渗透测试服务器对应用逻辑进行分析或获取服务器端关键信息** |
| **风险详情** |  |
| **处理建议** | **1.将不再使用的调试信息及时清除**  **2.将不用测试网址信息及时清除**  **3.关闭不再使用的测试服务** |

|  |
| --- |
| **恶意行为** |
| **检测项** | **广告检测** |
| **风险描述** | **评估样本是否存在广告** |
| **风险级别** | **高危** |
| **风险危害** | **一般广告对客户体验有影响**  **恶意广告会推送恶意信息** |
| **评估结论** |  |
| **风险分析** | **通过推送给客户产生垃圾信息** |
| **风险详情** |  |
| **处理建议** | **检查androidmanifest.xml是否含有广告sdk特征** |

|  |
| --- |
| **应用安全** |
| **检测项** | **日志信息渗透** |
| **风险描述** | **android.permission.READ\_LOGS:app读取日志权限，android 4.1之前版本通过申请READ\_LOGS权限就可以读取其他应**  **用的log了。但是谷歌发现这样存在安全风险，于是android 4.1以及之后版本，即使申请了READ\_LOGS权限也无法读取**  **其他应用的日志信息了。4.1版本中 Logcat的签名变为“signature|system|development”了，这意味着只有系统签名的app或者root权限的app才能使用该权限。普通用户可以通过ADB查看所有日志。** |
| **风险级别** | **高危** |
| **风险危害** | **调试日志可能暴露用户的重要日志信息，专业人员可能通过对日志信息进行分析窃取用户信息，破解客户端代码逻辑或者为其他调试跟踪等破解手段提供辅助信息** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **该APP存在调试日志的调用，可能发生重要日志信息泄露的风险** |
| **风险详情** | **无** |
| **处理建议** | **1.敏感信息不应用Log.e()/w()/i(), System.out/err 打印**  **2.如果需要打印一些敏感信息建议使用 Log.d()/v()**  **3.Log.d()/v()的返回值不应被使用**  **4.release版apk实现自动删除Log.d()/v()等代码**  **5.公开的APK文件应该是release版而不是development版**  **6.使用BuildConfig.DEBUG ADT的版本不低于21**  **7.即使不用System.out/err程序也有可能输出相关信息，如使用 Exception.printStackTrace()**  **8.ProGuard不能移除如下log：("result:" + value).**  **不应将日志输出到sdscard中，这样会让日志变得全局可读** |

|  |
| --- |
| **应用安全** |
| **检测项** | **动态调试渗透** |
| **风险描述** | **未采取反调试措施的应用，其执行流程可以被IDA等调试工具动态调试** |
| **风险级别** | **高危** |
| **风险危害** | **1.dex文件可以被IDA、smali源码级调试(应用可以反编译)**  **2.so文件可以被IDA等工具调试** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **由于应用未采取必要反调试措施，导致IDA等工具对其动态分析的成本极低，dex文件和so文件中的核心算法或敏感信息容易被窃取** |
| **风险详情** | **无** |
| **处理建议** | **1.将应用中的debuggable属性显式配置为false**  **2.对应用采取反调试保护措施，防止其他工具的调试(检测traceId、检验执行时间差、多进程ptrace检验附加情况、监测调试端口使用情况等)** |

|  |
| --- |
| **应用安全** |
| **检测项** | **Activity劫持** |
| **风险描述** | **输入密码的Activity可能被劫持** |
| **风险级别** | **高危** |
| **风险危害** | **Activity被劫持后，用户可能将用户名和密码输入到虚假的Activity中** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **由于关键的Activity没有针对界面劫持进行检测，因此恶意软件可以获取当前界面的Activity名和所在的包名来判断是否劫持该Activity。当其被劫持后，用户可能将用户名密码输入到虚假的Activity中。** |
| **风险详情** | **无** |
| **处理建议** | **1.在Activity的onStop方法中检测当前界面是否被劫持。**  **2.一旦发现被不属于自身的Activity覆盖，弹出提示框。** |

|  |
| --- |
| **应用安全** |
| **检测项** | **进程保护** |
| **风险描述** | **将指定代码注入到目标进程中并执行** |
| **风险级别** | **高危** |
| **风险危害** | **1.监控用户输入及输出的信息**  **2.截获关键参数信息** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **应用进程在运行中可以被动态注入外部模块，可以对程序逻辑造成破坏** |
| **风险详情** | **无** |
| **处理建议** | **对应用采取加固措施，添加防注入功能** |

|  |
| --- |
| **应用安全** |
| **检测项** | **支付控制** |
| **风险描述** | **评估样本的支付流程是否完善** |
| **风险级别** | **高危** |
| **风险危害** | **造成支付或内购功能缺失，影响服务提供方利益** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **第三方支付不完善造成商户账号信息泄露，支付成功条件判断漏洞或缓存内购买记录不合理存放使得购买凭证被绕过，给服务提供方造成损失** |
| **风险详情** | **无** |
| **处理建议** | **1.增加放页面劫持等安全措施**  **2.缓存内的用户信息等内容加密保存**  **3.定期清除缓存内信息** |

|  |
| --- |
| **应用安全** |
| **检测项** | **支付密码设置** |
| **风险描述** | **评估样本进行支付时是否需要支付密码，是否有密码输入错误尝试次数限制，登录密码、支付密码是否采用了不同的安全级别** |
| **风险级别** | **高危** |
| **风险危害** | **容易造成在用户不知情或错误操作的情况下完成支付影响用户支付** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **用户在支付时不需要输入密码，或密码安全等级不够造成用户在不知情的情况下完成支付，影响用户的账户安全** |
| **风险详情** | **无** |
| **处理建议** | **1.对密码输入采取错误次数限制**  **2.对不同种类的密码采用不同的安全等级**  **3.禁止不使用密码校验就进行支付等操作** |

|  |
| --- |
| **应用安全** |
| **检测项** | **登录控制** |
| **风险描述** | **应用自动存储用户信息实现自动登录的同时存在用户信息泄密** |
| **风险级别** | **高危** |
| **风险危害** | **用户的账户密码等信息可能泄漏** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **为了实现自动登录和保存密码等功能，用户名和登录密码等信息会被保存在文本内，文本内容不加密或简单加密的情况下可以被提取使用户信息泄漏造成账户安全隐患** |
| **风险详情** | **无** |
| **处理建议** | **用户名密码等信息加密保存** |

|  |
| --- |
| **应用安全** |
| **检测项** | | **双因子认证** |
| **风险描述** | | **双因子认证可以保障用户的某些重要操作的安全性** |
| **风险级别** | | **高危** |
| **风险危害** | | **在用户进行如大额支付，更改密码等重要操作时没有除密码以外的验证手段使非法操作容易完成** |
| **评估结论** | | **待渗透测试** |
| **风险分析** | | **在没有双因子认证的情况下恶意攻击者在获得用户名密码等信息后可以进行任意操作如更改密码等将账户据为己有或盗取账户内资金等** |
| **风险详情** | | **无** |
| **处理建议** | | **添加短信认证，短信认证由接受请求的服务器端发送并验证** |

|  |
| --- |
| **应用安全** |
| **检测项** | | **超时重新授权** |
| **风险描述** | | **评估应用在会话超时的情况下是否要求重新授权** |
| **风险级别** | | **高危** |
| **风险危害** | | **影响应用在用户不操作的情况下的安全性** |
| **评估结论** | | **待渗透测试** |
| **风险分析** | | **当连接超时时没有重新授权的话，会导致通过过期会话访问用户账户的风险** |
| **风险详情** | | **无** |
| **处理建议** | | **1.超时重新授权添加：**  **（1）添加后台监听方法**  **（2）应用转入后台监听启动计时器**  **（3）应用前台启动后停止计时器，并作出判断，如若超时则需要重新授权(跳转至登录页面重新登录或要求重新输入密码)** |

|  |
| --- |
| **应用安全** |
| **检测项** | | **密码强度** |
| **风险描述** | | **密码复杂程度，密码越简单越容易被破解** |
| **风险级别** | | **高危** |
| **风险危害** | | **过于简单的密码容易被简单破解引起账户丢失等情况** |
| **评估结论** | | **待渗透测试** |
| **风险分析** | | **密码强度的大小直接影响到账户被暴力破解的难易程度** |
| **风险详情** | | **无** |
| **处理建议** | | **在源代码中增加对注册密码的判断，通过对注册密码进行判断来确定密码强度，对密码字符串进行拆分单独判断后汇总判断，低于某个强度如全部都是数字或字母则判断注册密码不通过** |

|  |
| --- |
| **应用安全** |
| **检测项** | **测试数据包含** |
| **风险描述** | **检查应用安装文件中是否包含测试数据（包含冗余文件和冗余说明，其中冗余文件包括：含有通信地址等敏感信息的配置文件、含有Java代码的备份文件、测试文件、与应用无关的冗余资源文件等；冗余说明包括：脚本代码中的功能说明、发布者信息、注释掉的代码块等，以及其他文本中出现的冗余说明）** |
| **风险级别** | **中危** |
| **风险危害** | **造成应用安装包冗余，通过测试数据暴露应用功能逻辑的信息** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **应用打包前未将冗余部分删除，应用打包后体积增大，相关信息暴露** |
| **风险详情** | **无** |
| **处理建议** | **查看安装包文件，删除冗余部分** |

|  |
| --- |
| **应用安全** |
| **检测项** | **第三方SDK安全** |
| **风险描述** | **评估样本app在切换界面后是否会留存敏感信息，产生泄露风险** |
| **风险级别** | **中危** |
| **风险危害** | **敏感信息未清空，可能导致敏感信息被盗取** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **在界面切换操作时，是否存在对敏感信息的处理** |
| **风险详情** | **无** |
| **处理建议** | **1.建议对APP编码中的界面切换进行安全加固**  **2.议将allowBackup属性值显示设置为false：出于安全考虑，建议关闭应用备份功能; 在AndroidMenifest.xml文件中，将相应组件的“android:allowBackup”属性设置为“false”** |

|  |
| --- |
| **源码安全** |
| **检测项** | **程序签名校验渗透** |
| **风险描述** | **APP应用存在重新打包和重新签名的安全风险，为了提高安全性有必要对签名信息进行校验** |
| **风险级别** | **高危** |
| **风险危害** | **1.应用可以被篡改内容后重新签名发布**  **2.应用可以被植入恶意代码后重新签名发布**  **3.应用使用的签名校验算法强度不够容易被绕过或屏蔽** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **应用没有添加原始签名的校验的话，将导致应用被二次打包和重新签名的攻击** |
| **风险详情** | **无** |
| **处理建议** | 1. **Native层本地签名校验** 2. **服务器校验** |

|  |
| --- |
| **源码安全** |
| **检测项** | **完整性校验渗透** |
| **风险描述** | **应用很容易被恶意篡改后进行二次打包重新发布，存在极强的完整性破坏风险** |
| **风险级别** | **高危** |
| **风险危害** | **应用容易被反编译篡改和二次打包发布** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **由于应用的防反编译措施强度不够或二次打包校验容易被绕过，导致应用的完整性无法保证** |
| **风险详情** | **无** |
| **处理建议** | **1.对应用添加保护标志和校验代码，使反编译和二次打包后的运行失效**  **2.对应用进行加固，防止应用的保护代码被绕过** |

|  |
| --- |
| **源码安全** |
| **检测项** | **代码混淆渗透** |
| **风险描述** | **没有经过混淆加密的so文件很容易通过反编译工具还原为汇编代码或伪代码，对于恶意逆向分析提供便利** |
| **风险级别** | **高危** |
| **风险危害** | **so文件中的逻辑容易暴露，核心算法和敏感数据容易被窃取** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **由于so文件没有经过混淆处理或加密保护，恶意逆向分析可以对so文件进行还原** |
| **风险详情** | **无** |
| **处理建议** | **1.开发中使用LLVM-Obfuscator对应用c/c++源码进行混淆加密编译**  **2.在发布后对so文件进行加固保护** |

|  |
| --- |
| **源码安全** |
| **检测项** | **DEX保护强度渗透** |
| **风险描述** | **评估样本是否对Dex文件进行了保护处理** |
| **风险级别** | **高危** |
| **风险危害** | **1.程序逻辑被篡改**  **2.收费平台被破坏**  **3.加入恶意推送** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **未对dex文件做过处理的，很容易的可以找到程序的原始逻辑，程序的代码可以被二次篡改** |
| **风险详情** | **无** |
| **处理建议** | **1.对smali文件进行流程混淆**  **2.对smali文件中的字符进行加密**  **3.对dex文件进行加解密处理。** |

|  |
| --- |
| **源码安全** |
| **检测项** | **SO保护强度渗透** |
| **风险描述** | **评估样本是否存在SO保护措施** |
| **风险级别** | **高危** |
| **风险危害** | **1.未保护的SO可以看到源码**  **2.程序的逻辑可以被篡改** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **Android程序的大部分关键代码都写在native层，未对so文件进行保护，这种情况下可以被静态查看或者保护强度不够可以被轻松的动态dump。这将对开发者造成严重的损害。** |
| **风险详情** | **无** |
| **处理建议** | **1.对so文件的elf文件头进行修改**  **2.在对此so文件加载的解密程序中加入ptrace措施**  **3.解密恢复so文件时，防止一次性全部恢复。** |

|  |
| --- |
| **源码安全** |
| **检测项** | **资源文件保护渗透** |
| **风险描述** | **检测资源文件是否经过加固保护，分析其加固保护的强度** |
| **风险级别** | **高危** |
| **风险危害** | **没有进行加固保护或加固保护强度太弱的资源文件会被轻易破解，导致程序敏感信息泄露** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **没有经过资源文件保护可能会使恶意用户获取资源文件** |
| **风险详情** | **无** |
| **处理建议** | **使用具有资源文件防反编译功能的加密加固工具对APP中的资源文件进行加密** |

|  |
| --- |
| **源码安全** |
| **检测项** | **业务敏感逻辑渗透** |
| **风险描述** | **敏感逻辑出现问题有可能使用户账户信息泄露等。** |
| **风险级别** | **高危** |
| **风险危害** | **用户信息泄露** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **在很多情况下，业务逻辑是需要保密的，例如登录的逻辑，汇款的逻辑等。所以应当对业务逻辑进行加密，同时对通讯流程进行加密，这样才能够保证第三方无法猜测业务逻辑。** |
| **风险详情** | **无** |
| **处理建议** | **对应用进行加固，对通讯信道进行加密。** |

|  |
| --- |
| **源码安全** |
| **检测项** | **反编译防范渗透** |
| **风险描述** | **检测应用是否采取了有效的防反编译保护措施，分析其保护强度** |
| **风险级别** | **高危** |
| **风险危害** | **应用没有采取有效的防反编译保护措施或其保护强度不够的话会导致应用被恶意分析人员进行反编译等操作，造成应用敏感信息和核心逻辑的泄露** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **应用可被反编译，可以获取还原的源码** |
| **风险详情** | **无** |
| **处理建议** | **对程序进行加壳保护，在Manifest文件中加入不存在的资源引用。** |

|  |
| --- |
| **数据安全** |
| **检测项** | **密码专用键盘保护** |
| **风险描述** | **监控键盘输入信息** |
| **风险级别** | **高危** |
| **风险危害** | **用户的账户信息被窃取** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **键盘被监控后用户在屏幕上的点击操作将以文本的形式储存并发送到攻击者手中，其中的用户名密码等信息如若丢失则会影响账户安全** |
| **风险详情** | **无** |
| **处理建议** | **使用安全键盘相关的SDK产品或者自定义键盘** |

|  |
| --- |
| **应用安全** |
| **检测项** | **敏感数据截获** |
| **风险描述** | **在应用传输数据的过程中截获特定数据** |
| **风险级别** | **高危** |
| **风险危害** | **1.用户名密码等信息被窃取盗用**  **2.网络数据被截取，可用于分析用户**  **3.伪造网络请求，影响账户安全** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **用户数据被截取，用户信息如个人信息使用习惯等信息被窃取** |
| **风险详情** | **无** |
| **处理建议** | **传输数据加密处理** |

|  |
| --- |
| **数据安全** |
| **检测项** | **数据访问控制** |
| **风险描述** | **数据需要分级处理，设置访问限制** |
| **风险级别** | **高危** |
| **风险危害** | **应用数据中的敏感信息会泄露** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **一方面数据存放的位置决定了数据是否是公开，因此重要数据需要存放在包内的文件夹；另一方面数据需要进行加密** |
| **风险详情** | **无** |
| **处理建议** | **重要数据需要进行加密处理，并设置较高访问权限限制** |

|  |
| --- |
| **数据安全** |
| **检测项** | **敏感数据残留** |
| **风险描述** | **应用储存的用户信息残留在旧界面和容器中会导致泄露** |
| **风险级别** | **高危** |
| **风险危害** | **残留数据中包含的敏感信息泄露** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **网络缓存数据、GUI对象缓存、用户名密码缓存数据等未能及时清除会导致用户数据被窃取盗用** |
| **风险详情** | **无** |
| **处理建议** | **1.设置浏览器不储存缓存或用clearCache()方法来删除任何存储在本地的文件**  **2.在用户离开（切换）应用界面或者注销登录时清除gui界面的数据**  **3.在每一个activity（界面）启动的时候检测用户是否处于登录状态，如果没有则跳转到登录界面。** |

|  |
| --- |
| **数据安全** |
| **检测项** | **敏感数据加密** |
| **风险描述** | **用户信息、程序逻辑可能泄露** |
| **风险级别** | **高危** |
| **风险危害** | **敏感数据中可能包括用户隐私等，造成泄露可能会被第三方利用。** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **用户信息是应用程序应当保护的，不仅仅包括用户的用户名和密码，同样也包括用户的社交信息、照片、视频等。这些文件如果存放在不合适的目录中，就可能使得用户的信息能够被其他程序获取。因此需要对这些信息进行加密。同时，应用内部的一些重要资源，也应当进行加密，防止应用被破解。** |
| **风险详情** | **无** |
| **处理建议** | **对所有敏感数据文件进行加密** |

|  |
| --- |
| **数据安全** |
| **检测项** | **远程数据通信加密** |
| **风险描述** | **在远程数据通讯过程中，使用未加密协议传输数据时，所有数据均为明文传输** |
| **风险级别** | **高危** |
| **风险危害** | **传输数据容易被截获进行抓包分析**  **数据包中的敏感信息容易被分析篡改** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **由于没有使用加密协议，数据包内容没有得到有效保护，导致传输中的敏感信息容易被分析篡改** |
| **风险详情** | **无** |
| **处理建议** | **尽量使用https等加密协议进行数据传输**  **数据包中的敏感信息不能用明文传输** |

|  |
| --- |
| **数据安全** |
| **检测项** | **数据传输完整性** |
| **风险描述** | **在数据传输过程中，数据可以被截获和篡改，篡改后的数据包会导致信息失效或失真，给用户利益造成损失** |
| **风险级别** | **高危** |
| **风险危害** | **使传输的数据内容或结构破坏，导致信息失效无法被接收方使用**  **使传输的数据内容改变，导致信息失真，无法传递准确的信息到接收方** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **由于数据传输时信道或其他因素导致数据会发生错误或被恶意篡改，如果没有校验机制或防篡改机制，数据完整性很容易产生风险** |
| **风险详情** | **无** |
| **处理建议** | **使用加密通信协议进行传输，防止信息被恶意篡改**  **使用纠错校验机制对信息进行校验和纠错，防止信息发生失效** |

|  |
| --- |
| **数据安全** |
| **检测项** | **本地数据通讯安全** |
| **风险描述** | **本地数据在系统组件之间传递时需要对数据的有效性和准确性进行过滤和检验** |
| **风险级别** | **高危** |
| **风险危害** | **如果本地数据通讯过程中，数据源发送错误数据或传送中被恶意篡改都会导致应用出现异常甚至被恶意利用** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **数据源传递错误数据可以导致应用异常或产生拒绝服务**  **数据传输中被恶意篡改可以使应用被错误信息控制** |
| **风险详情** | **无** |
| **处理建议** | **Activity组件在相互交互时要严格过滤Intent内容，防止无效或错误内容处理**  **ContentProvider组件在交互时要对Cursor对象严格过滤**  **Broadcast组件要对广播信息进行筛选**  **AIDL Service组件要过滤接口收到的信息** |

|  |
| --- |
| **数据安全** |
| **检测项** | **转账安全性检测** |
| **风险描述** | **评估样本app是否存在不安全的转账行为** |
| **风险级别** | **高危** |
| **风险危害** | **转账安全性问题会导致用户个人信息及账号信息的泄露，造成隐私和财产损失。** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **需要对转账的整个过程进行风险评估，判断是否存在安全性风险。** |
| **风险详情** | **无** |
| **处理建议** | **建议对APP的转账安全性进行加固。** |

|  |
| --- |
| **数据安全** |
| **检测项** | **安装包中敏感信息加密** |
| **风险描述** | **评估样本app的安装包敏感信息是否存在被盗取的风险** |
| **风险级别** | **高危** |
| **风险危害** | **1.若安装包敏感信息未加密，可能导致程序被反编译和二次前面，APP被伪造和篡改**  **2.获取源码，修改后二次签名** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **需要检查安装包中的存在敏感信息的文件是否被加密** |
| **风险详情** | **无** |
| **处理建议** | **1.DEX混淆**  **2.SO混淆**  **3.DEX加密**  **4.SO加密**  **5.资源文件加密**  **6.反调试\防注入\防HOOK\HOOK技术** |

|  |
| --- |
| **数据安全** |
| **检测项** | **界面切换后面敏感信息需清空** |
| **风险描述** | **评估样本app在切换界面后是否会留存敏感信息，产生泄露风险** |
| **风险级别** | **高危** |
| **风险危害** | **1.泄露用户的账户信息**  **2.泄露用户的个人隐私** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **在界面切换操作时，是否存在对敏感信息的处理** |
| **风险详情** | **无** |
| **处理建议** | **建议将allowBackup属性值显示设置为false：出于安全考虑，建议关闭应用备份功能; 在AndroidMenifest.xml文件中，将相应组件的“android:allowBackup”属性设置为“false”** |

|  |
| --- |
| **数据安全** |
| **检测项** | **数据输入敏感数据显示** |
| **风险描述** | **评估样本app是否存在数据输入敏感数据显示的风险** |
| **风险级别** | **中危** |
| **风险危害** | **身份证或密码未做掩盖，存在被窃取的风险** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **APP需要输入的敏感信息存在被用户周围窥探者窃取的风险** |
| **风险详情** | **无** |
| **处理建议** | **对敏感信息的输入，在界面做星号或者异或的转换** |

|  |
| --- |
| **数据安全** |
| **检测项** | **本地数据通讯权限检查** |
| **风险描述** | **评估样本是否存在超越权限的通讯或信息泄露行为** |
| **风险级别** | **中危** |
| **风险危害** | **1.绕过本地认证**  **2.强制恢复出厂设置**  **3.本地拒绝服务**  **4.隐式启动Intent包含敏感数据**  **5.合谋攻击**  **6.伪造接受短信** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **由于使用不安全的通讯方式，未进行最小权限设置，对app通讯路径检查不完全，造成拒绝废服务攻击及合谋攻击的风险。** |
| **风险详情** | **无** |
| **处理建议** | **1.对信息的传递方式进行改进，如广播机制Broadcast，使用sendOrderedBroadcast，对接收的机制实施优先级设置。**  **2.发送广播可以通过Intent制定具体发送的Andro类，例如本实例在创建广播Intent时，加入下面这行代码，广播将永远只能被DataReceiver接收Intent.setClass(MainActivity.this,DataReceiver.class);** |

|  |
| --- |
| **数据安全** |
| **检测项** | **会话安全** |
| **风险描述** | **应用会话中会使用的cookie、url参数等信息可以被恶意分析者利用** |
| **风险级别** | **中危** |
| **风险危害** | **1.恶意分析人员可以通过cookie、url参数等信息分析程序功能**  **2.会话信息可以被修改参数内容导致应用行为异常** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **由于会话信息可以被分析修改，导致会话中的信息可以被分析或者篡改，用于非法用途** |
| **风险详情** | **无** |
| **处理建议** | **1.对会话内容进行加密，防止恶意分析**  **2.对会话内容进行校验，防止恶意篡改** |

|  |
| --- |
| **数据安全** |
| **检测项** | **重放攻击** |
| **风险描述** | **应用中关键信息没有进行序列和计数校验，可以引起重放攻击** |
| **风险级别** | **中危** |
| **风险危害** | **对关键信息的多次请求会导致短时间内执行多个操作，会导致关键信息被恶意篡改** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **由于对请求序列和计数校验不完善或不准确将导致重放攻击的发生** |
| **风险详情** | **无** |
| **处理建议** | **1.在开发过程中对请求的序列和频率进行限制，防止频繁重放攻击** |

|  |
| --- |
| **数据安全** |
| **检测项** | **数据输出敏感数据显示** |
| **风险描述** | **评估样本app是否存在数据输出敏感数据显示的风险** |
| **风险级别** | **低危** |
| **风险危害** | **身份证或密码未做掩盖，存在被窃取的风险** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **APP需要输出的敏感信息存在被用户周围窥探者窃取的风险** |
| **风险详情** | **无** |
| **处理建议** | **对敏感信息的输出，在界面做星号或者异或的转换** |

|  |
| --- |
| **数据安全** |
| **检测项** | **卸载清除** |
| **风险描述** | **评估样本是否存在app文件未彻底删除的文件及缓存** |
| **风险级别** | **低危** |
| **风险危害** | **1.泄露用户的账户信息**  **2.泄露用户的个人隐私** |
| **评估结论** |  |
| **风险分析** | **APP在卸载后，APP安装目录存在未卸载完成的文件或缓存文件未进行更新，用户隐私数据存在泄漏的危险。** |
| **风险详情** |  |
| **处理建议** | **1.卸载后，查看以下文件/data/data、/data/app，查看是否存在，如果存在，则删除相关文件。**  **2.删除/data/dalvik-cache，立即重启，已经删除的app dalvik-cache文件就会成功删除，并写不会影响其他app的使用。**  **若不能重启手机，可以对/data/dalvik-cache文件进行处理，如进行加密，hash等替换原来的原始文件。** |

|  |
| --- |
| **数据安全** |
| **检测项** | **证书验证** |
| **风险描述** | **应用中在使用ssl、https等通信协议时，使用不当会造成校验失效等问题** |
| **风险级别** | **低危** |
| **风险危害** | **证书验证失效会造成所有证书都成为可信证书，对连接失去保护机制** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **由于环境问题或连接的限制，部分应用在开发中会选择信任所有证书，造成证书验证失效** |
| **风险详情** | **无** |
| **处理建议** | **1.尽量使用有效的证书验证连接** |

|  |
| --- |
| **数据安全** |
| **检测项** | **下载任意APK** |
| **风险描述** | **更新用的APK可能被劫持** |
| **风险级别** | **中危** |
| **风险危害** | **1.用户的用户名和密码被盗取。**  **2.用户被欺骗安装而已软件。** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **由于没有检验升级网址的签名，有可能被中间人攻击。** |
| **风险详情** | **无** |
| **处理建议** | **1.不使用友盟SDK**  **2.下载功能Service组件不要导出，不要允许隐式调用** |

|  |
| --- |
| **漏洞** |
| **检测项** | **全局可读写内部文件** |
| **风险描述** | **评估样本是否存在全局可读写内部文件的风险** |
| **风险级别** | **低危** |
| **风险危害** | **攻击者利用该越权漏洞，对手机系统全局文件进行恶意篡改。** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **无** |
| **风险详情** | **不正确的权限设置，导致系统的文件系统暴露在攻击者范围下，可以随意篡改非root权限的文件。** |
| **处理建议** | **修改文件的访问权限。** |

|  |
| --- |
| **漏洞** |
| **检测项** | **Webview绕过证书校验** |
| **风险描述** | **WebView组件加载网页发生证书认证错误时，会调用WebViewClient类的onReceivedSslError方法，如果该方法实现调用了handler.proceed()来忽略该证书错误，则会受到中间人攻击的威胁，可能导致隐私泄露** |
| **风险级别** | **中危** |
| **风险危害** | **绕过证书验证会受到中间人攻击的威胁，从而导致隐私泄露** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **由于业务需求或开发策略，选择了绕过证书错误的实现方式，则会引起漏洞，导致中间人攻击威胁** |
| **风险详情** | **无** |
| **处理建议** | **1.不调用android.webkit.SslErrorHandler的proceed方法**  **2.当发生证书认证错误时，采用默认的处理方法SslErrorHandler.cancel()，停止加载问题页面** |

|  |
| --- |
| **漏洞** |
| **检测项** | **浏览器的intent scheme url攻击检测** |
| **风险描述** | **检测浏览器是否存在intent scheme url漏洞** |
| **风险级别** | **中危** |
| **风险危害** | **可能导致应用程序崩溃，也可演变提权漏洞** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **相比于普通Intend-Based攻击，这种方式极具隐蔽性。这种攻击还能直接访问跟浏览器自身的组件（无论是公开还是私有）和私有文件，比如cookie文件，进而导致用户机密信息的泄露** |
| **风险详情** | **无** |
| **处理建议** | **建议浏览器及调用浏览器的app进行安全加固** |

|  |
| --- |
| **漏洞** |
| **检测项** | **手势密码绕过** |
| **风险描述** | **安全防护较弱的手势密码有被破解的风险** |
| **风险级别** | **中危** |
| **风险危害** | **App的实施密码未做安全防护，可以被破解或绕过，盗取用户信息。** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **手势密码的密码文件存放在默认目录下，恶意用户可以下载并破解，密码输入为经过安全设置，存在手势密码失效的风险。** |
| **风险详情** | **无** |
| **处理建议** | **对App手势密码进行安全加固，密码文件进行加密处理** |

|  |
| --- |
| **漏洞** |
| **检测项** | **被调用安装任意apk** |
| **风险描述** | **APP程序中存在被任意更新或安装病毒程序的风险** |
| **风险级别** | **中危** |
| **风险危害** | **APP程序被强制更新，造成信息损失或拒绝服务攻击** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **APP本身具备更新或者调用系统功能更新app的功能，可以被利用，被其他程序调用并更新，导致拒绝服务攻击。** |
| **风险详情** | **无** |
| **处理建议** | **对APP程序的更新功能进行安全分析，对存在的任意调用风险进行消除** |

|  |
| --- |
| **漏洞** |
| **检测项** | **被调用卸载任意apk** |
| **风险描述** | **APP程序中存在被任意调用卸载的风险** |
| **风险级别** | **中危** |
| **风险危害** | **APP程序被强制卸载，造成信息损失或拒绝服务攻击** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **APP本身具备自我卸载或者调用系统卸载app的功能，可以被利用，被其他程序调用并卸载。** |
| **风险详情** | **无** |
| **处理建议** | **对APP程序的卸载功能进行安全分析，对存在的任意调用风险进行消除** |

|  |
| --- |
| **恶意行为** |
| **检测项** | **病毒检测** |
| **风险描述** | **存在病毒的app会导致手机系统受到病毒的破坏，发生隐私泄露，违规的文件读写操作，监控网络数据等操作** |
| **风险级别** | **高危** |
| **风险危害** | **App的病毒未作安全防护，存在感染病毒的风险** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **病毒会导致系统的防护系统失效，获取系统最高权限，执行特点的操作**  **和指令，给用户造成财产损失和隐私泄露。** |
| **风险详情** | **cn.missfresh.application\_095403.apk.apk, cn.missfresh.application\_095403.apk\_crack.apk** |
| **处理建议** | **使用动态分析和静态分析的方式对病毒进行检测，并对存在的漏洞进行**  **加固。** |

|  |
| --- |
| **服务器安全** |
| **检测项** | **跨权漏洞** |
| **风险描述** | **攻击者通过普通用户提升权限而获得管理员权限，最终控制服务器** |
| **风险级别** | **高危** |
| **风险危害** | **提权漏洞一旦被触发，攻击者就可以非法操纵系统一切可以操纵的资源** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **攻击者利用权限提升漏洞，通过普通用户提升权限而获得管理员权限，最终控制服务器** |
| **风险详情** | **无** |
| **处理建议** | **1.用户端安全设置**  **2.服务器安全权限设置** |

|  |
| --- |
| **服务器安全** |
| **检测项** | **SQL注入** |
| **风险描述** | **1.由于SQL注入，数据库存在被读取或者篡改的风险**  **2.攻击者甚至可以获得更大的权限，进行提权操作** |
| **风险级别** | **中危** |
| **风险危害** | **1.执行一些非授权的 SQL 代码,以修改、窃取或者破坏数据库。**  **2.绕过用户认证机制，使其可以完全的操控远程服务器上的数据库。** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **1.如果应用程序使用一些用户输入的数据来构造动态的SQL语句去访问数据库，将可能遭受到 SQL 注入攻击。**  **2.如果在代码中使用了存储过程，并且这些存储过程缺乏对用户输入的合理限制，则也很容易发生 SQL 注入。**  **3.数据库用户的权限过大，不符合“最小特权”原则，导致SQL注入。**  **4.程序中使用不安全的函数或者不安全的存储过程，将可能遭受到SQL注入攻击。** |
| **风险详情** | **无** |
| **处理建议** | **1.进行完善的代码检查，避免SQL注入漏洞。**  **1.1 使用白名单原则进行过滤，而不要使用黑名单原则。**  **1.2 SQL语句避免使用字符串拼接的形式，建议使用查询参数化（绑定变量）的方法进行查询。**  **1.3 数据类型检测，不同数据类型进行不同的过滤。**  **1.4 使用安全存储过程与安全函数。**  **2.及时进行数据库版本升级，防止数据库版本过低而导致提权漏洞。**  **3.数据库用户权限的设置应遵循“最小权限”原则，防止因为权限过大而导致安全问题。**  **4.对日志进行全面的审计，及时预防攻击行为。**  **5.对数据库进行加密保护。** |

|  |
| --- |
| **服务器安全** |
| **检测项** | **XSS跨站脚本** |
| **风险描述** | **恶意攻击者往Web页面里插入恶意html代码，当用户浏览该页之时，嵌入其中Web里面的html代码会被执行，从而达到恶意用户的特殊目的。** |
| **风险级别** | **中危** |
| **风险危害** | **1.盗取各类用户账号，如机器登录账号、用户网银账号、各类管理员账号**  **2.控制企业数据，包括读取、篡改、添加、删除企业敏感数据的能力**  **3.盗窃企业重要的具有商业价值的资料**  **4.非法转账**  **5.强制发送电子邮件**  **6.网站挂马**  **7.控制受害者机器向其它网站发起攻击** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **由于大多数程序员不太注意对用户输入的字符串进行细致的检验，或经过一定的检验但忽略了相关的细节，容易留下XSS漏洞。而一旦有XSS漏洞经过利用变会造成无可估量的损失。** |
| **风险详情** | **无** |
| **处理建议** | **1.将重要的cookie标记为http only**  **2.只允许用户输入我们期望的数据。**  **3.对数据进行Html Encode 处理过滤或移除特殊的Html标签**  **4.过滤JavaScript 事件的标签** |

|  |
| --- |
| **服务器安全** |
| **检测项** | **缓冲区溢出** |
| **风险描述** | **通过往程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其它指令，以达到攻击的目的。** |
| **风险级别** | **中危** |
| **风险危害** | **1.缓冲区溢出的危害性具有破坏性与隐蔽性的特点。**  **2.破坏性体现在易使服务程序停止运行，服务器死机甚至删除服务器上的数据或者可以执入并运行攻击代码。**  **3.隐蔽性体现在软件漏洞难以避免，缓冲攻击的shellcode的执行不易被察觉，攻击的随机性及不可预测性。** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **1.导致程序运行失败、系统当机、重新启动等后果**  **2.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**  **获得目标主机的控制权** |
| **风险详情** | **无** |
| **处理建议** | **1.代码编写：避免使用危险函数，对于缓冲区的操作要进行严格的边界检查，这可借助一些工具如编译器来实现；**  **2.开发语言：可使用类型­安全的编程语言，如Java；**  **3.运行状态：可进行动态保护，主要是数组边界检查和保证返回指针的完整性；**  **4.基于探测方法的防御：stackguard、StackShield**  **5.非执行的堆栈防御：非执行的堆栈补丁、ASCII 保护内存**  **6.其他防御建议：分割控制和数据堆栈、随机化可执行程序的位置** |

|  |
| --- |
| **服务器安全** |
| **检测项** | **文件上传漏洞** |
| **风险描述** | **攻击者利用程序缺陷绕过系统对文件的验证与处理策略将恶意程序上传到服务器并获得执行服务器端命令的能力** |
| **风险级别** | **中危** |
| **风险危害** | **上传漏洞可以把ASP、JSP、CGI、PHP等格式的木马上传至网站目录内，所得到的权限最低也是WEBSHELL，如果碰到的是安全意识不强的管理员，甚至可以获得管理员权限。** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **由于大多数程序员不太注意对上传文件进行细致的过滤，或经过一定的检验过滤但忽略了相关的细节，容易留下文件上传漏洞，而一旦有文件上传漏洞经过利用变会造成无可估量的损失。** |
| **风险详情** | **无** |
| **处理建议** | **1.检查是否判断了上传文件类型及后缀**  **2.定义上传文件类型白名单，即只允许上传的文件类型**  **3.文件上传目录禁止脚本解析**  **4.建议使用随机字符串重命名文件名，而不是使用用户上传上来的name参数的值。** |

|  |
| --- |
| **服务器安全** |
| **检测项** | **数据库泄露** |
| **风险描述** | **数据库存在泄露的风险，有被非法下载利用的威胁** |
| **风险级别** | **中危** |
| **风险危害** | **数据库泄露，数据库被非法下载，用户信息泄露，根据企业的类型有不同性质的危害** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **数据库泄露主要有以下途径：  1.存储层：直接盗走数据文件或备份文件，异地还原后得到数据  2.数据访问：通过人为获取DBA等高权限用户的口令，或通过权限提升等漏洞得到一个高权限用户身份，进行数据窃取  3.应用层：破解或通过工作便利获取应用中的数据库用户口令，绕开业务系统直接访问所有数据**  **数据库泄露的主要原因：**  **1.假冒合法用户进行非法访问：数据库存在弱口令漏洞，口令容易被破解从而绕过合法业务系统，直接访问数据库；  2.数据库用户权限过大；** |
| **风险详情** | **无** |
| **处理建议** | **1.对数据库加密**  **对核心敏感数据进行加密存储，使数据文件、备份文件中的敏感数据都是密文形态；即使数据文件或备份文件被盗，也可以保证核心敏感数据的安全性，防止批量泄露。**  **2.对数据库连接文件加密**  **3.使用基于数据加密的应用绑定技术，防止非法访问**  **应用绑定技术将数据库用户和合法的业务系统直接绑定，确保该用户只能通过指定的业务系统程序进行核心数据的访问，通过自定义程序、其他管理工具等方式无法进行敏感数据的访问。**  **4.增加用户的身份鉴别强度**  **使用基于物理设备的双因素口令认证技术，使得即使获取密码口令后也不能轻易冒用他人身份。**  **5.数据库管理员需要按最小原则构建安全的权限体系**  **使用加密技术对核心的敏感数据进行加密，同时引入三权分立机制，通过安全管理员控制对密文数据的访问权限，这样即使是DBA用户，在没有被授予密文访问权限的情况下照样无法访问敏感数据。**  **6.修改备份文件名规则，防止数据库备份文件被盗用** |

|  |
| --- |
| **服务器安全** |
| **检测项** | **弱口令漏洞** |
| **风险描述** | **口令的组成是简单数字和字母的简单组合** |
| **风险级别** | **低危** |
| **风险危害** | **1、用户账号被控制**  **2、数据泄露**  **3、服务器被控制**  **4、由于非常多的用户密码通用，导致一家数据泄露，用户在互联网上的其他账号也受到牵连** |
| **评估结论** | **待渗透测试** |
| **风险分析** | **1、对于个人的弱口令被破解，则会导致其账户被控制；**  **2、对于服务器后台的弱口令被破解，则会导致整个服务器被控制、数据泄露等等问题** |
| **风险详情** | **无** |
| **处理建议** | **1.对于口令的设置：**  **1.不使用空口令或系统缺省的口令**  **2.口令长度不小于8个字符**  **3.口令不应该为连续的某个字符或重复某些字符的组合**  **4.口令应该为以下四类字符的组合，大写字母(A-Z)、小写字母(a-z)、数字(0-9)和特殊字符。每类字符至少包含一个。如果某类字符只包含一个，那么该字符不应为首字符或尾字符**  **5.口令中不应包含本人、父母、子女和配偶的姓名和出生日期、纪念日期、登录名、E-mail地址等等与本人有关的信息，以及字典中的单词。**  **6.口令不应该为用数字或符号代替某些字母的单词。**  **7.口令应该易记且可以快速输入，防止他人从你身后很容易看到你的输入。**   1. **至少90天内更换一次口令，防止未被发现的入侵者继续使用该口令。**   **2.对于服务器安全机制：限制错误登录次数**  **3.单位时间内验证的过多则封杀ip** |

|  |  |  |  |
| --- | --- | --- | --- |
| **安全级别的说明** | | | |
| |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  |  |  |  |  |  |  |  |  |  |  | | **一级** | **高危** | **对应用敏感信息和核心数据的安全具有重要影响** |
| |  |  |  | | --- | --- | --- | |  |  |  | | **二级** | **中危** | **对应用敏感信息和核心数据的安全具有一般影响** |
| |  | | --- | |  | | **三级** | **低危** | **对应用敏感信息和核心数据的安全具有轻微影响** |

|  |
| --- |
| **鼎源科技APP安全检测扫描平台**  （[www.appbesafe.com](http://www.appbesafe.com)）  北京鼎源科技有限公司（简称：鼎源科技）（www.devsource.com.cn）成立于2005年，是一家专注于移动互联网信息安全领域研究和开发的高科技企业。自2015年起，公司专注于提供移动APP 应用安全的产品研发与服务，相继推出了鼎源APP加固盾、APP安全检测等一系列移动安全相关的产品。   * 取得软件著作权30项，申请发明专利10多项。 * ISO9001质量管理体系 * 中关村高新技术企业 * 北京市信技术新产品（服务）证书 |