安全检查评估报告

趣声

卓护 Annhub	检测单位	卓护加固	文档名称	安全检测报告
	送检时间	2018-6-12	检测技术版本	Version 1.0

一、检测概况

1.1 应用信息

文件名	HelloWorld
包名	com.example.helloworld
MD5	8696d01788bf7047bc61aaff55e8f1d1
SHA-1	B4:3C:81:71:AB:70:A8:E7:4F:41:40:FF:EC:D7:02:D2:3A:EE:8D:A3
大小	1.25MB
证书	CN=Android Debug, O=Android, C=US,CN=Android Debug, O=Android, C=US

1.2 威胁图表

风险项 **5**　　漏洞数 **6**

二、安全检测

2.1 权限检测

权限信息		
READ_EXTERNAL_STORAGE 读取 SD 卡上的内容	INSTALL_DRM 未知权限	GET_TASKS 检索当前运行的应用程序
WRITE_EXTERNAL_STORAGE 修改/删除 SD 卡中的内容	PROCESS_OUTGOING_CALLS 拦截外拨电话	READ_LOGS 读取系统日志文件
ACCESS_WIFI_STATE 查看 WLAN 状态	ACCESS_COARSE_LOCATION 大概位置	WRITE_OWNER_DATA 写入所有者数据
READ_PHONE_STATE 读取手机状态和身份	ACCESS_DRM 未知权限	RECEIVE_BOOT_COMPLETED 开机时自动启动

SYSTEM_OVERLAY_WINDOW 未知权限	ACCESS_FINE_LOCATION 精准的(GPS)位置	GET_PACKAGE_SIZE 计算应用程序存储空间
WAKE_LOCK 防止手机休眠	ACCESS_NETWORK_STATE 查看网络状态	com.android.launcher.permission.INSTALL_SHORTCUT 未知权限
ACCESS_BACKGROUND_SERVICE 未知权限	com.UNINSTALL_SHORTCUT 未知权限	SEND_SMS 发送短信
com.android.launcher.permission.UNINSTALL_SHORTCUT 未知权限	KILL_BACKGROUND_PROCESSES 结束后台进程	RECEIVE_USER_PRESENT 未知权限
DISABLE_KEYGUARD 停用键锁	SYSTEM_ALERT_WINDOW 显示系统级警报	com.android.vending.BILLING 未知权限
WRITE_SETTINGS 修改全局系统设置	INTERNET 访问网络	CHANGE_WIFI_STATE 更改 WLAN 状态
ACCESS_LOCATION_EXTRA_COMMANDS 访问额外的位置信息提供程序命令	VIBRATE 控制振动器	com.android.launcher.permission.READ_SETTINGS 未知权限
CHANGE_NETWORK_STATE 更改网络连接性	CHANGE_CONFIGURATION 更改用户界面设置	DOWNLOAD_WITHOUT_NOTIFICATION 未知权限
READ_EXTERNAL_STORAGE 读取 SD 卡上的内容	INSTALL_DRM 未知权限	GET_TASKS 检索当前运行的应用程序
WRITE_EXTERNAL_STORAGE 修改/删除 SD 卡中的内容	PROCESS_OUTGOING_CALLS 拦截外拨电话	READ_LOGS 读取系统日志文件
ACCESS_WIFI_STATE 查看 WLAN 状态	ACCESS_COARSE_LOCATION 大概位置	WRITE_OWNER_DATA 写入所有者数据
READ_PHONE_STATE 读取手机状态和身份	ACCESS_DRM 未知权限	RECEIVE_BOOT_COMPLETED 开机时自动启动
SYSTEM_OVERLAY_WINDOW 未知权限	ACCESS_FINE_LOCATION 精准的(GPS)位置	GET_PACKAGE_SIZE 计算应用程序存储空间
WAKE_LOCK 防止手机休眠	ACCESS_NETWORK_STATE 查看网络状态	com.android.launcher.permission.INSTALL_SHORTCUT 未知权限
ACCESS_BACKGROUND_SERVICE 未知权限	com.UNINSTALL_SHORTCUT 未知权限	SEND_SMS 发送短信
com.android.launcher.permission.UNINSTALL_SHORTCUT 未知权限	KILL_BACKGROUND_PROCESSES 结束后台进程	RECEIVE_USER_PRESENT 未知权限
DISABLE_KEYGUARD 停用键锁	SYSTEM_ALERT_WINDOW 显示系统级警报	com.android.vending.BILLING 未知权限

行为信息		
Dynamic_Load 动态加载	Reflection_Call 反射调用	

三、风险评估

Java 代码保护风险	
评估项	
风险描述	
风险影响	
评估方案	
评估结果	
风险分析	
风险详情	
解决方案	
Java 层调试标记风险	
评估项	
风险描述	
风险影响	
评估方案	
评估结果	
风险分析	
风险详情	
解决方案	
组件导出风险	
评估项	
风险描述	
风险影响	
评估方案	
评估结果	
风险分析	
风险详情	
解决方案	
敏感函数调用风险	
评估项	
风险描述	
风险影响	
评估方案	
评估结果	
风险分析	
风险详情	
解决方案	
调试日志函数调用风险	
评估项	
风险描述	
风险影响	

评估方案	
评估结果	
风险分析	
风险详情	
解决方案	
动态调试攻击风险	
评估项	
风险描述	
风险影响	
评估方案	
评估结果	
风险分析	
风险详情	
解决方案	
动态注入攻击风险	
评估项	
风险描述	
风险影响	
评估方案	
评估结果	
风险分析	
风险详情	
解决方案	
APP 篡改/二次打包攻击风险	
评估项	
风险描述	
风险影响	
评估方案	
评估结果	
风险分析	
风险详情	
解决方案	
应用数据任意备份风险	
评估项	
风险描述	
风险影响	
评估方案	
评估结果	
风险分析	
风险详情	
解决方案	

明文数字证书风险	
评估项	
风险描述	
风险影响	
评估方案	
评估结果	
风险分析	
风险详情	
解决方案	
未使用 HTTPS 协议传输数据风险	
评估项	
风险描述	
风险影响	
评估方案	
评估结果	
风险分析	
风险详情	
解决方案	
WebView 明文存储密码风险	
评估项	
风险描述	
风险影响	
评估方案	
评估结果	
风险分析	
风险详情	
解决方案	

四、漏洞扫描

内网测试信息残留漏洞	
评估项	内网测试信息残留漏洞
漏洞描述	检测程序代码内部是否包含残留测试信息，例如内网 url 地址等。
漏洞影响	低
评估方案	通过检测是否包含内网 URl 地址,判断是否发布包中是否包含测试数据。残留的测试数据，例如 URL 地址，测试账号，密码，可能会被盗取并恶意利用在正式服务器上进行攻击，例如账号重试，攻击安全薄弱的测试服务器以获取服务器安全漏洞或者逻辑漏洞。
评估结果	安全
漏洞分析	该 App 应用中未包含测试数据信息。
漏洞详情	N/A
解决方案	N/A

下载任意 apk 漏洞	
评估项	下载任意 apk 漏洞
漏洞描述	检测应用中是否存在下载任意 apk 的漏洞。
漏洞影响	中
评估方案	具有下载 apk 功能的组件存在导出漏洞，并且未对组件调用者进行校验。攻击者可利用导出组件的手段下载攻击者指定的任意 apk 文件，并且在下载过程中伪装 apk 文件的下载信息，例如图标、描述等，导致用户被诱导下载安装恶意应用。
评估结果	安全
漏洞分析	该 App 应用中不存在可被导出的具有下载 apk 功能的组件。
漏洞详情	N/A
解决方案	N/A
HTTPS 未校验服务器证书漏洞	
评估项	HTTPS 未校验服务器证书漏洞
漏洞描述	检测 App 程序在使用 HTTPS 协议传输数据时是否对服务器证书进行完整校验。
漏洞影响	中
评估方案	使用 HTTPS 协议时，客户端必须对服务器证书进行完整校验，以验证服务器是真实合法的目标服务器。如果没有校验，客户端可能与仿冒的服务器建立通信链接，即“中间人攻击”。仿冒的中间人可以冒充服务器与银行客户端进行交互，同时冒充银行客户端与银行服务器进行交互，在充当中间人转发信息的时候，窃取手机号，账号，密码等敏感信息。
评估结果	安全
漏洞分析	该 Apk 经过加固保护，可能存在的 HTTPS 未校验服务器证书漏洞无法被获取。为获得更深入的测评信息，请联系下方邮箱或者服务热线，提交人工测试申请。
漏洞详情	N/A
解决方案	N/A
content provider 数据泄露漏洞	
评估项	content provider 数据泄露漏洞
漏洞描述	检测 App 是否存在 Content Provider 数据泄露风险。
漏洞影响	高
评估方案	Content provider 可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。
评估结果	安全
漏洞分析	该 App 应用中不存在可被其他程序访问的 content provider 数据。
漏洞详情	N/A
解决方案	N/A
数据库注入漏洞	
评估项	数据库注入漏洞
漏洞描述	检测 App 应用的数据库是否存在 sql 注入漏洞。
漏洞影响	高
评估方案	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，app 本地数据库可能被注入攻击。这种风险可能导致存储的敏感数据信息被查询泄露，

	例如账户名，密码等，或者产生查询异常导致应用崩溃。
评估结果	安全
漏洞分析	该 App 应用无数据库注入漏洞。
漏洞详情	N/A
解决方案	N/A
全局可读写的内部文件漏洞	
评估项	全局可读写的内部文件漏洞
漏洞描述	检测 App 应用中是否存在内部文件，可被其他任意 App 读写。
漏洞影响	中
评估方案	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。如果此类文件包含了关键配置信息，账户信息数据等敏感信息，可能会被盗取或者恶意篡改，导致如程序无法运行，业务逻辑被修改等问题。
评估结果	存在漏洞
漏洞分析	该 App 应用中存在全局可读写的内部文件，其中内部文件中可能存在敏感信息，其他应用可以直接读写该文件信息。

漏洞详情	{
	"readable":[
	"libDexHelper-x86.so",
	"libDexHelper.so"
	],
	"writeable":[]
	}

解决方案	根据需要严格控制文件的全局读写权限；对于必须使用的全局可读写文件，严格审核其中是否包含敏感信息。
Webview 远程代码执行漏洞	
评估项	Webview 远程代码执行漏洞
漏洞描述	检测 app 应用的 webview 组件中是否存在远程代码执行漏洞。
漏洞影响	高
评估方案	Webview 是 Android 用于浏览网页的组件，其包含的接口函数 addJavascriptInterface 可以将 Java 类或方法导出以供 JavaScript 调用，实现网页 JS 与本地 JAVA 的交互。由于系统没有限制已注册 JAVA 类的方法调用，因此未注册的其它任何 JAVA 类也可以被反射机制调用，这样可能导致被篡改的 URL 中存在的恶意代码被执行，用户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。
评估结果	安全
漏洞分析	该 Apk 经过加固保护，可能存在 webview 组件远程代码执行漏洞无法被获取。为获得更深入的测评信息，请联系下方邮箱或者服务热线，提交人工测试申请。
漏洞详情	N/A
解决方案	N/A
Webview 绕过证书校验漏洞	
评估项	Webview 绕过证书校验漏洞
漏洞描述	检测 App 应用的 webview 组件是否在发现 https 网页证书错误后继续加载页面。
漏洞影响	低

评估方案	客户端的 Webview 组件访问使用 HTTPS 协议加密的 url 时，如果服务器证书校验错误，客户端应该拒绝继续加载页面。但如果重载 WebView 的 onReceivedSslError()函数并在其中执行 handler.proceed()，客户端可以绕过证书校验错误继续访问此非法 URL。这样将会导致“中间人攻击”，攻击者冒充服务器与银行客户端进行交互，同时冒充银行客户端与银行服务器进行交互，在充当中间人转发信息的时候，窃取手机号，账号，密码等敏感信息。
评估结果	安全
漏洞分析	该 Apk 经过加固保护，可能存在的 Webview 绕过证书校验漏洞无法被获取。为获得更深入的测评信息，请联系下方邮箱或者服务热线，提交人工测试申请。
漏洞详情	N/A
解决方案	N/A