Evaluation Warning: The document was created with Spire.Doc for Python.

**华瑞银行（ 8.0.6版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 华瑞银行 |
| 版本 | 8.0.6 |
| 包名 | com.huaruibank.android.hulubank |
| 域名线索 | 19条 |
| URL线索 | 2条 |
| APP图标 |  |
| 分析日期 | 2025年6月26日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | 华瑞银行.apk |
| 文件大小 | 66.65MB |
| MD5值 | 6379e3d85c8fea628b5c30ea123eeed6 |
| SHA1值 | 1e0dd836a8290f28b5f44043da5172a83f343042 |
| SHA256值 | e510775d5dd4f8fb21bd5e719bed23d6cab2ddc70aafe47476766fb2cfab685a |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 华瑞银行 |
| 包名 | com.huaruibank.android.hulubank |
| 主活动Activity | com.alipay.mobile.quinox.LauncherActivity |
| 安卓版本名称 | 8.0.6 |
| 安卓版本 | 954 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| 00000098.mobilebank | 没有服务器地理信息.  |
| render.alipay.com | IP: 27.221.78.204 所属国家: China 地区: Shandong 城市: Qingdao  |
| ..mybank.cn | 没有服务器地理信息.  |
| ..poseidong.com | 没有服务器地理信息.  |
| act.aligames.com | IP: 218.11.15.212 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| ..jimingkeji.com.cn | 没有服务器地理信息.  |
| 00000014.mobilebank | 没有服务器地理信息.  |
| 20000920.h5app.alipay.com | 没有服务器地理信息.  |
| a.alipayobjects.com | IP: 221.194.147.197 所属国家: China 地区: Hebei 城市: Langfang  |
| openauth.alipay.com | IP: 203.209.247.64 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| ..mucfc.com | 没有服务器地理信息.  |
| ..fapiao | 没有服务器地理信息.  |
| mpaas.shrbank.com | IP: 118.126.51.70 所属国家: China 地区: Shanghai 城市: Shanghai  |
| m.51yzone.com | IP: 121.199.193.25 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| ..jss.com.cn | 没有服务器地理信息.  |
| a.idsuipai | 没有服务器地理信息.  |
| sky.vip.youku.com | IP: 116.196.142.207 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| as.alipayobjects.com | IP: 116.142.245.228 所属国家: China 地区: Beijing 城市: Beijing  |
| static.alipay.com | IP: 203.209.245.120 所属国家: China 地区: Zhejiang 城市: Hangzhou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://mpaas.shrbank.com:443/E56672F051655\_prd/v1.0.0.0/images/fail.png  | 摸瓜V2引擎  |
| https://mpaas.shrbank.com:443/E56672F051655-prd/00000098/1.0.0.39\_all/nebula/00000098\_1.0.0.39.amr  | 摸瓜V2引擎  |
| https://00000098.mobilebank\_prd.shrbank.com  | 摸瓜V2引擎  |
| https://mpaas.shrbank.com:443/E56672F051655-prd/00000014/1.0.0.41\_all/nebula/fallback/  | 摸瓜V2引擎  |
| https://mpaas.shrbank.com:443/E56672F051655-prd/00000014/1.0.0.41\_all/nebula/00000014\_1.0.0.41.amr  | 摸瓜V2引擎  |
| https://00000014.mobilebank\_prd.shrbank.com  | 摸瓜V2引擎  |
| https://(.\*[.]mybank[.]cn)$\  | 摸瓜V2引擎  |
| https://(jskp  | 摸瓜V2引擎  |
| https://m[.]51yzone[.]com$\  | 摸瓜V2引擎  |
| https://.\*[.]((jimingkeji[.]com[.]cn)  | 摸瓜V2引擎  |
| https://.\*[.]jimingkeji[.]com[.]cn$\  | 摸瓜V2引擎  |
| https://(((betaalipay  | 摸瓜V2引擎  |
| https://((a[.]idsuipai)  | 摸瓜V2引擎  |
| https://act[.]aligames[.]com$\  | 摸瓜V2引擎  |
| https://((www  | 摸瓜V2引擎  |
| https://((sky[.]vip[.]youku[.]com)  | 摸瓜V2引擎  |
| https://(sky[.]vip[.]youku[.]com  | 摸瓜V2引擎  |
| https://.\*[.]jss[.]com[.]cn$\  | 摸瓜V2引擎  |
| https://.\*[.](fapiao  | 摸瓜V2引擎  |
| https://((x  | 摸瓜V2引擎  |
| https://.\*[.]mucfc[.]com$\  | 摸瓜V2引擎  |
| https://.\*[.]poseidong[.]com$\  | 摸瓜V2引擎  |
| https://openauth.alipay.com/oauth2/publicAppAuthorize.htm?app\_id=2016042601338846&scope=auth\_userinfo&redirect\_uri=http%3a%2f%2fjsfwpt.lsyypt.com%2fhkOrder%2fjshksqfwc&state=fwcljhk\  | 摸瓜V2引擎  |
| https://openauth.alipay.com/oauth2/publicAppAuthorize.htm?app\_id=2016042601338846&scope=auth\_userinfo&redirect\_uri=http%3a%2f%2fjsfwpt.lsyypt.com%2fhkOrder%2fjshkjlfwc&state=fwchkjl\  | 摸瓜V2引擎  |
| https://openauth.alipay.com/oauth2/publicAppAuthorize.htm?app\_id=2016042601338846&scope=auth\_userinfo&redirect\_uri=http%3A%2F%2Fjsfwpt.lsyypt.com%2FhkOrder%2Fjshksqcfw&state=csfw\  | 摸瓜V2引擎  |
| https://openauth.alipay.com/oauth2/publicAppAuthorize.htm?app\_id=2014042900005397&auth\_skip=true&scope=auth\_base&redirect\_uri=https%3A%2F%2Foauth.cc.cmbchina.com%2FOauthPortal%2Falipay%2Fcallback%3Foauth\_id%3D20405188%26callback\_uri%3Dhttps%3A%2F%2Fxyk.cmbchina.com%2FmyAccount%2Fonekeyquery%2Findex\  | 摸瓜V2引擎  |
| https://a.alipayobjects.com/amui/native/9.0/amui.css  | 摸瓜V2引擎  |
| https://as.alipayobjects.com/g/component/antbridge/1.1.3/antbridge.min.js  | 摸瓜V2引擎  |
| https://static.alipay.com/alibridge/1.0.0/alibridge.min.js  | 摸瓜V2引擎  |
| https://as.alipayobjects.com/g/h5-lib/antui/9.9.0-2/rem/antui.css  | 摸瓜V2引擎  |
| https://as.alipayobjects.com/g/h5-lib/vue/1.0.26/vue.min.js  | 摸瓜V2引擎  |
| https://a.alipayobjects.com/g/antui/antui/10.0.0/rem/antui.css  | 摸瓜V2引擎  |
| https://a.alipayobjects.com/g/antui/antui-img/1.0.0/page-result/error.png  | 摸瓜V2引擎  |
| https://a.alipayobjects.com/g/antui/antui-img/1.0.0/page-result/system\_busy.png  | 摸瓜V2引擎  |
| https://a.alipayobjects.com/g/antui/antui-img/1.0.0/page-result/blank\_page.png  | 摸瓜V2引擎  |
| https://a.alipayobjects.com/g/antui/antui-img/1.0.0/page-result/404.png\  | 摸瓜V2引擎  |
| https://render.alipay.com/p/f/result/index.html?type=result-busy&scene=industry\_container\_monitor\  | 摸瓜V2引擎  |
| https://20000920.h5app.alipay.com/www/error.htm?from=nebulaPageError\  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: CN=HRDBank 签名算法: rsassa\_pkcs1v15 有效期自: 2015-05-18 13:05:45+00:00 有效期至: 3014-09-18 13:05:45+00:00 发行人: CN=HRDBank 序列号: 0x1407b525 哈希算法: sha256 md5值: a28e28f69ae55299c0416149bc695e3d sha1值: 3891a5b667ffc8302842dc63f704633f2aff6e1b sha256值: e98ac6d432d397bba94846b80858e4a785307e4918b4c75f02d2067883756da8 sha512值: 92fad2f9ea9e0e5aa43181fe6251bfb64cab7c4e6657c2d754c0fb1a4567720d21134d7b53d40480816402cf1f9b7e58cd8c29eb278dfa2112261b2bb0c30854 公钥算法: rsa 密钥长度: 2048 指纹: ff1d7d686a04ffc7b0fd9c9caf34875a96fffc829a5b3a3ad7e4e26837ad33c2**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 此APP的危险动作**

| 向手机申请的权限 | 是否危险 | 类型  | 详细情况 |
| --- | --- | --- | --- |
| android.permission.ACCESS\_WIFI\_STATE | 正常 | 查看Wi-Fi状态 | 允许应用程序查看有关 Wi-Fi 状态的信息 |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| android.permission.ACCESS\_NETWORK\_STATE | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.READ\_EXTERNAL\_STORAGE | 危险 | 读取外部存储器内容 | 允许应用程序从外部存储读取 |
| android.permission.WRITE\_EXTERNAL\_STORAGE | 危险 | 读取/修改/删除外部存储内容 | 允许应用程序写入外部存储 |
| android.permission.READ\_PHONE\_STATE | 危险 | 读取电话状态和身份 | 允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等 |
| android.permission.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| android.permission.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| android.permission.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| android.permission.ACCESS\_FINE\_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| android.permission.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。  |
| android.permission.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| android.permission.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| android.permission.USE\_FINGERPRINT | 正常 | allow use of指纹 | 该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE\_BIOMETRIC |
| android.permission.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| android.permission.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| com.android.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.REQUEST\_INSTALL\_PACKAGES | 危险 | 允许应用程序请求安装包。 | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。 |
| com.huaruibank.android.hulubank.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.heytap.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE\_MEDIA\_PROJECTION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ZTE\_HEARTYSERVICE\_MANAGEMENT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.WAKE\_LOCK | 正常 | 防止手机睡眠  | 允许应用程序防止手机进入睡眠状态 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.alipay.mobile.quinox.LauncherActivity | **Schemes**: shrbank://, **Hosts:** platformapi, **Path Prefixes:** /startapp,  |

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**