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

**荣裕易拍（ 1.2.9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 | 荣裕易拍 |
| 版本 | 1.2.9 |
| 包名 | com.rongyu.yipai |
| 域名线索 | 7条 |
| URL线索 | 13条 |
| APP图标 |  |
| 分析日期 | 2025年6月3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 | 荣裕(1)[1].apk |
| 文件大小 | 34.14MB |
| MD5值 | 000a495b29f8736104bb9e8721721098 |
| SHA1值 | 26cb5bd55e1c30693ad127e0e291248a7afca5d6 |
| SHA256值 | 0904cdaba3262549960e95b0bdc257d0d710e18f1fc6cb375b418f8d3b89d6ae |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 荣裕易拍 |
| 包名 | com.rongyu.yipai |
| 主活动Activity | com.dev.ft\_main.SplashActivity |
| 安卓版本名称 | 1.2.9 |
| 安卓版本 | 34 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| long.open.weixin.qq.com | IP: 112.65.193.150  所属国家: China  地区: Shanghai  城市: Shanghai |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| web.rongyuhehealth.com | IP: 104.18.17.174  所属国家: United States of America  地区: California  城市: San Francisco |
| www.slf4j.org | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| rongyuyigou.oss-cn-hangzhou.aliyuncs.com | IP: 101.67.62.121  所属国家: China  地区: Zhejiang  城市: Huzhou |
| open.weixin.qq.com | IP: 140.207.121.14  所属国家: China  地区: Shanghai  城市: Shanghai |
| mp.weixin.qq.com | IP: 140.207.176.25  所属国家: China  地区: Shanghai  城市: Shanghai |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://web.rongyuhehealth.com/ypxy/yhxy.html | com/dev/ft\_mine/ui/AboutUsActivity.java |
| https://web.rongyuhehealth.com/ypxy/yszc.html | com/dev/ft\_mine/ui/AboutUsActivity.java |
| https://rongyuyigou.oss-cn-hangzhou.aliyuncs.com | com/dev/lib\_common/utils/XUtils.java |
| https://web.rongyuhehealth.com/ypxy/yhxy.html | com/dev/ft\_login/LoginActivity.java |
| https://web.rongyuhehealth.com/ypxy/yszc.html | com/dev/ft\_login/LoginActivity.java |
| https://rongyuyigou.oss-cn-hangzhou.aliyuncs.com/ | com/dev/ft\_main/SplashActivity.java |
| https://web.rongyuhehealth.com/ypxy/yszc.html | com/dev/ft\_main/SplashActivity.java |
| https://web.rongyuhehealth.com/ypxy/yhxy.html | com/dev/ft\_main/SplashActivity.java |
| https://)([\\s\\S]+) | com/huawei/hms/scankit/p/t3.java |
| https://mp.weixin.qq.com/publicpoc/opensdkconf?action=GetShareConf&appid= | com/tencent/mm/opensdk/openapi/WXAPiSecurityHelper.java |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid= | com/tencent/mm/opensdk/diffdev/a/c.java |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid= | com/tencent/mm/opensdk/diffdev/a/b.java |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling | io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0 | io/reactivex/rxjava3/exceptions/UndeliverableException.java |
| https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection | org/java\_websocket/AbstractWebSocket.java |
| https://www.slf4j.org/codes.html | org/slf4j/LoggerFactory.java |

### **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: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: CN=CN, OU=CN, O=CN, L=CN, ST=CN, C=CN 签名算法: rsassa\_pkcs1v15 有效期自: 2024-10-14 14:04:53+00:00 有效期至: 2049-10-08 14:04:53+00:00 发行人: CN=CN, OU=CN, O=CN, L=CN, ST=CN, C=CN 序列号: 0x1 哈希算法: sha256 md5值: 3ddf5ec51547c51098fd48ed073e5845 sha1值: d17d4420a2b98134370bb13f526aaa5f3b6cc43e sha256值: a98af3030c930b9fa357c4bc908b48fe77c90e2d0bb0a281b8716e2a2b6c916c sha512值: a95a87a6c3905f965744373b857f26a2f0f0b4beb04f420f1b40093b04226bd2c961297053b75b6e46abca520e8d454f4cd0b3716bea86ffe692dc138fb54880 公钥算法: rsa 密钥长度: 2048 指纹: 4983eee65510cf504b75c281f198c7604b8f8543a1d71eef5f9f25928f16ff0a**

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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\_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.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.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。 |
| 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.READ\_CONTACTS | 危险 | 读取联系人数据 | 允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人 |
| android.permission.READ\_PHONE\_NUMBERS | 危险 |  | 允许到设备的读访问的电话号码。这是 READ\_PHONE\_STATE 授予的功能的一个子集,但对即时应用程序公开 |
| android.permission.WRITE\_MEDIA\_STORAGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.READ\_MEDIA\_VISUAL\_USER\_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| com.rongyu.yipai.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.CAPTURE\_VIDEO\_OUTPUT | 正常 |  | 允许应用程序捕获视频输出 |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| android.permission.NFC | 正常 | 控制近场通信 | 允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信 |
| org.simalliance.openmobileapi.SMARTCARD | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**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。**