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

**51萝莉（ 4.1.0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 | 51萝莉 |
| 版本 | 4.1.0 |
| 包名 | me.kwqle.yydiqv |
| 域名线索 | 13条 |
| URL线索 | 18条 |
| APP图标 |  |
| 分析日期 | 2025年6月19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 | qd\_4.1.0\_250617\_3.apk |
| 文件大小 | 15.9MB |
| MD5值 | 1ba1eec76b8c22d3b612e6fcd568ec5f |
| SHA1值 | d363f8e5b63ddded7975b60a4e83288e36b3c4b1 |
| SHA256值 | 977942e9ca0acda072b9ec3ebe17785472f0ed21ecfe6a03e727bd4ae77cc847 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 51萝莉 |
| 包名 | me.kwqle.yydiqv |
| 主活动Activity | com.spaceseven.qidu.activity.SplashActivity |
| 安卓版本名称 | 4.1.0 |
| 安卓版本 | 410 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| sapi01.xkpamyk.xyz | IP: 156.255.123.42 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| cfg.flurry.com | IP: 69.147.80.15 所属国家: United States of America 地区: New York 城市: New York City  |
| www.example.com | IP: 96.7.229.92 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| schemas.microsoft.com | IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| data.flurry.com | 没有服务器地理信息.  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| exoplayer.dev | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| dashif.org | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| schemas.android.com | 没有服务器地理信息.  |
| raw.githubusercontent.com | IP: 185.199.111.133 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| ns.adobe.com | 没有服务器地理信息.  |
| api.login.yahoo.com | IP: 74.6.160.138 所属国家: United States of America 地区: New York 城市: New York City  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | c/d/a/i.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | c/d/a/i.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | c/d/a/i.java  |
| http://%s:%d/%s  | c/d/a/k.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | c/d/a/k.java  |
| http://%s:%d/%s  | c/d/a/g.java  |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread  | c/g/a/a/i2.java  |
| http://dashif.org/guidelines/trickmode  | c/g/a/a/z2/u0/f.java  |
| http://dashif.org/guidelines/last-segment-number  | c/g/a/a/z2/u0/m/d.java  |
| http://dashif.org/guidelines/trickmode  | c/g/a/a/z2/u0/m/d.java  |
| https://x</LA\_URL>  | c/g/a/a/s2/i0.java  |
| https://x  | c/g/a/a/s2/i0.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | c/g/a/a/s2/j0.java  |
| http://ns.adobe.com/xap/1.0/  | c/g/a/a/u2/h0/a.java  |
| https://sapi01.xkpamyk.xyz/api.php,https://sapi02.xjargryv.xyz/api.php,https://sapi03.xkpamyk.xyz/api.php  | c/n/a/m/x0.java  |
| http://www.example.com  | com/flurry/sdk/ed.java  |
| https://cfg.flurry.com/sdk/v1/config  | com/flurry/sdk/cl.java  |
| https://cfg.flurry.com/sdk/v1/config  | com/flurry/sdk/by.java  |
| https://data.flurry.com/v1/flr.do  | com/flurry/sdk/br.java  |
| https://api.login.yahoo.com/oauth2/device\_session  | com/flurry/sdk/ef.java  |
| http://schemas.android.com/apk/res/android  | com/hjq/permissions/PermissionUtils.java  |
| https://raw.githubusercontent.com/little-5/backup/master/seven.txt  | com/spaceseven/qidu/activity/SplashActivity.java  |
| https://github.com/vinc3m1  | 摸瓜V1引擎  |
| https://github.com/vinc3m1/RoundedImageView  | 摸瓜V1引擎  |
| https://github.com/vinc3m1/RoundedImageView.git  | 摸瓜V1引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | c/d/a/i.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099  | c/g/b/c/a.java  |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |

## **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: C=Singapore, ST=Singapore, L=Singapore, O=., OU=., CN=. 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-17 11:45:51+00:00 有效期至: 2026-06-17 11:45:51+00:00 发行人: C=Singapore, ST=Singapore, L=Singapore, O=., OU=., CN=. 序列号: 0x1a72443d 哈希算法: sha256 md5值: 77bc3e250ceb1fec15f7556d407d5bd5 sha1值: 1e2f2b9f5e5fa958c2925a552b75ef2d5a1dcb49 sha256值: c0f54c988e6083d8741acff09f966d3ed7f36a18131ee96b0a91fa1b1bf71421 sha512值: 6e10e529000d370e52c90613f7e8d2c85849b40b5bf5c0a257cc6acf54e1fc3c7cb895fd96ca757b6a9ca85fa626c1c15ed9b9ba6f493548f982a8ec390751ef 公钥算法: rsa 密钥长度: 2048 指纹: 8546334ef9761cb2ba4876b0461dac1b443001982ac15e322145fefc5ad34666**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "library\_roundedimageview\_author" : "Vince Mi"  |
| "library\_roundedimageview\_authorWebsite" : "https://github.com/vinc3m1"  |
| "str\_auth\_apply" : "认证申请"  |
| "str\_input\_account\_user\_name" : "请输入持卡人姓名"  |
| "str\_mod\_pwd" : "修改密码"  |
| "str\_mod\_pwd\_success" : "密码修改成功"  |
| "str\_official\_auth" : "官方认证"  |

## **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\_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.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.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\_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.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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| 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.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 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.READ\_CLIPBOARD\_IN\_BACKGROUND | 未知 | Unknown permission | Unknown permission from android reference |
| 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.WRITE\_CLIPBOARD | 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.SYSTEM\_OVERLAY\_WINDOW | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |

## **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。**