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

**SWAG（ 1.0.5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 | SWAG |
| 版本 | 1.0.5 |
| 包名 | qurmb.pguxn.sxnza |
| 域名线索 | 20条 |
| URL线索 | 19条 |
| APP图标 |  |
| 分析日期 | 2025年6月27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 | swg4958-v4.10.414.apk |
| 文件大小 | 23.74MB |
| MD5值 | ef7a36adcaea450b693313d3c1ff0ccd |
| SHA1值 | 58e45b9935a3c331096c357ba11fd6a5af422add |
| SHA256值 | a8e7a2bc66904749ca7f4a47d93ab89c212c9a729ba5129f5a6c2a47ed069c51 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | SWAG |
| 包名 | qurmb.pguxn.sxnza |
| 主活动Activity | qurmb.pguxn.sxnza.MainActivity |
| 安卓版本名称 | 1.0.5 |
| 安卓版本 | 6 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| flutter.dev | IP: 199.36.158.100  所属国家: United States of America  地区: California  城市: Mountain View |
| www.unicode.org | IP: 64.182.27.164  所属国家: United States of America  地区: Texas  城市: Dallas |
| journeyapps.com | IP: 18.65.168.90  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| developer.mozilla.org | IP: 34.111.97.67  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| api.flutter.dev | IP: 199.36.158.100  所属国家: United States of America  地区: California  城市: Mountain View |
| issuetracker.google.com | IP: 142.250.69.174  所属国家: United States of America  地区: California  城市: Mountain View |
| g.co | IP: 142.250.217.78  所属国家: United States of America  地区: California  城市: Mountain View |
| r9nhyvkt.vip | IP: 172.67.192.146  所属国家: United States of America  地区: California  城市: San Francisco |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| ns.adobe.com | 没有服务器地理信息. |
| dashif.org | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| default.url | 没有服务器地理信息. |
| docs.flutter.dev | IP: 199.36.158.100  所属国家: United States of America  地区: California  城市: Mountain View |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| developer.android.com | IP: 142.251.33.78  所属国家: Canada  地区: Ontario  城市: Toronto |
| www.ibm.com | IP: 23.42.126.170  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| dartbug.com | IP: 216.239.32.21  所属国家: United States of America  地区: California  城市: Mountain View |
| developer.apple.com | IP: 17.253.85.201  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| schemas.microsoft.com | IP: 13.107.246.73  所属国家: United States of America  地区: Washington  城市: Redmond |
| aomedia.org | IP: 103.42.176.244  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/Baseflow/flutter-permission-handler/issues | e4/t.java |
| https://docs.flutter.dev/deployment/android | io/flutter/embedding/engine/loader/FlutterLoader.java |
| https://developer.android.com/guide/topics/permissions/overview | io/flutter/plugin/platform/PlatformPlugin.java |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense | d1/n0.java |
| https://x</LA\_URL> | d1/m0.java |
| https://default.url | d1/m0.java |
| http://dashif.org/guidelines/last-segment-number | c1/d.java |
| http://dashif.org/guidelines/trickmode | c1/d.java |
| http://dashif.org/thumbnail\_tile | c1/d.java |
| http://dashif.org/guidelines/thumbnail\_tile | c1/d.java |
| https://issuetracker.google.com/issues/new?component=413107&template=1096568 | g3/c.java |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread | y0/v0.java |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted | w0/q.java |
| http://g.co/dev/packagevisibility. | w0/w.java |
| https://issuetracker.google.com/issues/new?component=907884&template=1466542 | f0/m.java |
| http://ns.adobe.com/xap/1.0/ | e2/b.java |
| https://aomedia.org/emsg/ID3 | h2/a.java |
| https://developer.apple.com/streaming/emsg-id3 | h2/a.java |
| https://journeyapps.com/ | 摸瓜V1引擎 |
| https://github.com/journeyapps/zxing-android-embedded | 摸瓜V1引擎 |
| https://github.com/nodeca/pica | 摸瓜V2引擎 |
| https://github.com/richtr/NoSleep.js/issues/15 | 摸瓜V2引擎 |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released) | 摸瓜V2引擎 |
| http://www.unicode.org/copyright.html | lib/arm64-v8a/libflutter.so |
| https://github.com/flutter/flutter/issues. | lib/arm64-v8a/libflutter.so |
| https://dartbug.com/52121. | lib/arm64-v8a/libflutter.so |
| https://r9nhyvkt.vip/front/ | lib/armeabi-v7a/libapp.so |
| https://developer.mozilla.org/en-US/docs/Web/HTTP/Status | lib/armeabi-v7a/libapp.so |
| http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd | lib/armeabi-v7a/libapp.so |
| https://api.flutter.dev/flutter/material/Scaffold/of.html | lib/armeabi-v7a/libapp.so |
| https://github.com/dart-lang/language/issues/3488 | lib/armeabi-v7a/libapp.so |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android. | lib/armeabi-v7a/libapp.so |
| http://www.unicode.org/copyright.html | lib/armeabi-v7a/libflutter.so |
| https://github.com/flutter/flutter/issues. | lib/armeabi-v7a/libflutter.so |
| https://dartbug.com/52121. | lib/armeabi-v7a/libflutter.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| appro@openssl.org | lib/arm64-v8a/libflutter.so |
| \_immutablelist@0150898.\_mk  \_vca@33287047.mxc  \_double@0150898.fromintege  \_growablelist@0150898.\_literal  \_typeerror@0150898.\_create  \_bytebuffer@7027147.\_new  \_assertionerror@0150898.\_create | lib/armeabi-v7a/libapp.so |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099 | z6/a.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: CN=11, OU=1, O=1, L=11, ST=11, C=1 签名算法: rsassa\_pkcs1v15 有效期自: 2024-10-17 03:18:58+00:00 有效期至: 2049-10-11 03:18:58+00:00 发行人: CN=11, OU=1, O=1, L=11, ST=11, C=1 序列号: 0x1 哈希算法: sha256 md5值: bf05f1913f0eaa721b3dec4004b79db0 sha1值: 73197ca68a2e33e29ac289bbf3039339fbfb6aa4 sha256值: 682f763fe25cdfa7cc552eef20621d1ac27a6424a9756a8564befa77d1f4d569 sha512值: e918bfd7efd6dad99a8dd2a0e9d3019d3215c6e4392fbd8b894a5ee76f61131a1eecb03e28d881ceb4a7bf571b9be3f248b748e664056b22fb455fe75e83048b 公钥算法: rsa 密钥长度: 2048 指纹: 953c8863b9538790a7b1c4455e22a1ff260beec3664a6508a76c9e93eeaf3ff3**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "library\_zxingandroidembedded\_author" : "JourneyApps" |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/" |

## **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.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 |
| 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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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\_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.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| 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.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| android.permission.ADD\_VOICEMAIL | 危险 | 将语音邮件添加到系统中 | 允许应用程序将语音邮件添加到系统中 |
| android.permission.USE\_SIP | 危险 | 拨打/接听互联网电话 | 允许应用程序使用 SIP 服务拨打/接听互联网电话 |
| android.permission.READ\_CALL\_LOG | 危险 |  | 允许应用程序读取用户的通话日志 |
| android.permission.WRITE\_CALL\_LOG | 危险 |  | 允许应用程序写入（但不读取）用户号召日志数据。 |
| android.permission.ACCESS\_MEDIA\_LOCATION | 危险 | 访问的任何地理位置 | 允许应用程序访问的任何地理位置持久保存在用户的共享集合 |
| 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.REQUEST\_DELETE\_PACKAGES | 正常 |  | 允许应用程序请求删除包 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| qurmb.pguxn.sxnza.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 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。**