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

**情欲AV（ 1.1.9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 | 情欲AV |
| 版本 | 1.1.9 |
| 包名 | com.qingyuav.hcqt |
| 域名线索 | 8条 |
| URL线索 | 5条 |
| APP图标 |  |
| 分析日期 | 2025年6月21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 | qingyuavv1.1.9\_ch\_1SFGm3.apk |
| 文件大小 | 31.04MB |
| MD5值 | 4e2e30bd126ade8eca502ae5872091bd |
| SHA1值 | 7c216e746c769966b6c542b988c5eb5a5d08a437 |
| SHA256值 | 3e458838ea50190a1f08a8741ff36e41db7e87fced1c7410c64290e347ad25e2 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 情欲AV |
| 包名 | com.qingyuav.hcqt |
| 主活动Activity | com.qingyuav.hcqt.MainActivity |
| 安卓版本名称 | 1.1.9 |
| 安卓版本 | 119 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.unicode.org | IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| journeyapps.com | IP: 18.65.168.3 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| api.shorebird.devupdater | 没有服务器地理信息.  |
| dartbug.com | IP: 216.239.38.21 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| aomedia.org | IP: 157.240.2.50 所属国家: United States of America 地区: California 城市: Menlo Park  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| 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  |
| https://aomedia.org/emsg/ID3  | 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://api.shorebird.devUpdater  | lib/arm64-v8a/libflutter.so  |
| http://://should  | lib/arm64-v8a/libflutter.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |

### **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: True 找到 1 个唯一证书 主题: C=beijing, ST=beijing, L=beijing, O=qs1727205583187, OU=ip1727205583187, CN=nbzm 签名算法: rsassa\_pkcs1v15 有效期自: 2024-09-24 19:19:43+00:00 有效期至: 2074-09-12 19:19:43+00:00 发行人: C=beijing, ST=beijing, L=beijing, O=qs1727205583187, OU=ip1727205583187, CN=nbzm 序列号: 0x5820ae90 哈希算法: sha512 md5值: d16faa8aab41fca62382cf40d7b8bc5a sha1值: 23eb606fd293b2e6b0527911b7286f67664c94c8 sha256值: 0c1979e9f694fa4333de8f044ed5e60efbca77572e9de1bcd25e782b92a6d539 sha512值: d70648527e0a7eff62704b129586ba9338534c6697269b42c673e929a2c49974a1a16bb8473f00ad28df7d1d833f42bb2ef64e382e99656712a8d9c84e896684 公钥算法: rsa 密钥长度: 4096 指纹: 913febe7741ed853e45b594a75d0223dfbadc0b3bff3f8176802852c3609ab09**

## **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.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.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.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.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.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.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 |
| Manifest.permission.CAPTURE\_AUDIO\_OUTPUT | 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.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.INSTALL\_PACKAGES | 系统需要 | 直接安装应用程序 | 允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序 |
| 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.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| android.permission.REQUEST\_DELETE\_PACKAGES | 正常 |  | 允许应用程序请求删除包 |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| com.qingyuav.hcqt.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.qingyuav.hcqt.MainActivity | **Schemes**: um.65c316ae95b14f599d24b346://, ypoj02://, a9c9xv://,  |

**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。**