MoGua

情欲AV 1.1.9.APK 分析报告

APP名称: 情欲AV

包名:	com.qingyuav.hcqt
域名线索:	8条
URL线索:	5条
邮箱线索:	1条
分析日期:	2025年6月21日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: qingyuavv1.1.9_ch_1SFGm3.apk
文件大小: 31.04MB
MD5值: 4e2e30bd126ade8eca502ae5872091bd
SHA1值: 7c216e746c769966b6c542b988c5eb5a5d08a437
SHA256值: 3e458838ea50190a1f08a8741ff36e41db7e87fced1c7410c64290e347ad25e2

APP 信息

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

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 **纬度**: 32.814899 **经度**: -96.879204
developer.mozilla.org	**IP**: 34.111.97.67 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
journeyapps.com	**IP**: 18.65.168.3 **所属国家**: Japan **地区**: Tokyo

	城市: Tokyo **纬度**: 35.689499 **经度**: 139.692322
www.w3.org	IP: 104.18.22.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
github.com	IP: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
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 **纬度**: 39.039474 **经度**: -77.491806
aomedia.org	IP: 157.240.2.50 **所属国家**: United States of America **地区**: California **城市**: Menlo Park **纬度**: 37.436935 **经度**: -122.193604

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

邮箱线索

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

手机线索

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

硬编码敏感信息

可能的敏感信息
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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

应用内通信

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

---