



MoGua

超享花 2.0.5.APK 分析报告



APP名称:

超享花

包名: PxNE.WTIJEK.oRuPHJHo.yuvzPzOjtv

域名线索: 7条

URL线索: 19条

邮箱线索: 1条

分析日期: 2025年7月3日

分析平台: [摸瓜APK反编译平台](#)

文件名: 04ss3RT.apk
文件大小: 15.61MB
MD5值: a1938da1e9854bad82cea22aea1ab4c5
SHA1值: 05e8acd7111dd8ff233210a959a9364e1279b5d1
SHA256值: dfaf1033f8f23463079d64736ce682a76532dde65868c1b0907e38cf027a7697

i APP 信息

App名称: 超享花
包名: PxNE.WTlJEK.oRuPHJHo.yuvzPzOjtv
主活动Activity: com.shell.app.app_shell.MainActivity
安卓版本名称: 2.0.5
安卓版本: 2506210

🔍 域名线索

域名	服务器信息
developer.android.com	IP: 142.250.73.78 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
www.example.com	IP: 23.46.155.166 所属国家: Japan 地区: Osaka 城市: Osaka 纬度: 34.694218 经度: 135.502228
issuetracker.google.com	IP: 142.250.69.174 所属国家: United States of America 地区: California

	城市: Mountain View 纬度: 37.405991 经度: -122.078514
ns.adobe.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 纬度: 1.289987 经度: 103.850281
docs.flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
schemas.android.com	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://www.example.com	com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java
http://schemas.android.com/apk/res/android	A/d.java
http://schemas.android.com/apk/res/android	A/b.java
https://github.com/google/gson/blob/main/Troubleshooting.md	A/j.java

https://issuetracker.google.com/issues/new?component=907884&template=1466542	R/C0069s.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	R/N.java
https://issuetracker.google.com/issues/241760537	R/b0.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	R/C0070t.java
http://ns.adobe.com/xap/1.0/\u0000	Z/h.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/p.java
http://schemas.android.com/apk/res/android	p0/p.java
http://schemas.android.com/apk/res/android	p0/AbstractC0604a.java
https://docs.flutter.dev/deployment/android	f2/CallableC0237b.java
https://github.com/google/gson/blob/main/Troubleshooting.md	q1/C0686a.java
https://github.com/google/gson/blob/main/Troubleshooting.md	l1/O.java
https://github.com/google/gson/blob/main/Troubleshooting.md	l1/C0531A.java
https://github.com/Baseflow/flutter-permission-handler/issues	H0/b.java
https://github.com/google/gson/blob/main/Troubleshooting.md	p1/C0618a.java
https://github.com/google/gson/blob/main/Troubleshooting.md	n1/AbstractC0570c.java

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	P0/j.java

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=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2025-05-27 02:48:36+00:00
有效期至: 2025-08-25 02:48:36+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x9d84bd5f0c635783
哈希算法: sha256
md5值: 6fc026c9f2b1efcc9e229fe76c8236ce
sha1值: e08f8c83b37380fa8e4887fcb668a216ac034f57
sha256值: cd100fb551018a45ba6f47fac2548ae028b509baf1f2ef12f3fbfeacdbe401d9
sha512值: d3274c5f2a36d888df5cff0e4b8f7afd93c173bc36a65100f2af806dbe16544f07bf5e90530241f9452e08cf087328ce8b6641df231444e1c72bface5e826eb2
公钥算法: rsa
密钥长度: 2048
指纹: 94b06c2aa97629fb87584f72e2b4626236b86b3897e2640c2192a903dbf570e9

硬编码敏感信息

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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.VIDEO_CAPTURE	未知	Unknown permission	Unknown permission from android reference
android.permission.AUDIO_CAPTURE	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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
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.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人 (地址) 数据。恶意应用程序可以使用它来删除或修改您的联系人数据
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
android.permission.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
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.READ_EXTERNAL_STORAGE	危险	读取外部存储内容	允许应用程序从外部存储读取

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_VISUAL_USER_SELECTED	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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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
PxNE.WTlJEK.oRuPHJHo.yuvzPzOjtv.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。