



MoGua

撸先生 2.4.0.APK 分析报告



APP名称:

撸先生

包名:	com.tvlutv
域名线索:	9条
URL线索:	7条
邮箱线索:	3条
分析日期:	2025年6月6日
分析平台:	摸瓜APK反编译平台

文件名: lusir_0219.apk
文件大小: 21.33MB
MD5值: fcce11f8dfcac6400a56a9769fea6e67
SHA1值: 50ce005d16e8ea34e7cae3e6f11e0967ece25656
SHA256值: 7b2616b1c34eb3fdbdef5f78815a74bb44718a276419846360527cf4fb46e7d8

i APP 信息

App名称: 撸先生
包名: com.tvlutv
主活动Activity: com.tvlutv.MainActivity
安卓版本名称: 2.4.0
安卓版本: 1001

🔍 域名线索

域名	服务器信息
api.hichatapi.com	IP: 172.67.191.20 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
developer.android.com	IP: 142.251.42.238 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。
	IP: 34.111.97.67

developer.mozilla.org	所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
www.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
aomedia.org	IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
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.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
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

URL线索

URL信息	Url所在文件
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/c.java
http://ns.adobe.com/xap/1.0/\u0000	r/a.java
https://developer.android.com/reference/javax/net/ssl/SSLSocket	y1/z.java
https://aomedia.org/emsg/ID3	Mogua Engine V2
https://github.com/richtr/NoSleep.js/issues/15	Mogua Engine V2
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)	Mogua Engine V2
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html	lib/armeabi-v7a/libapp.so
https://api.hichatapi.com/api.php	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.	lib/armeabi-v7a/libapp.so
https://github.com/flutter/flutter/issues/new.	lib/armeabi-v7a/libapp.so
http://www.w3.org/XML/1998/namespace	lib/armeabi-v7a/libflutter.so
http://www.w3.org/2000/xmlns/	lib/armeabi-v7a/libflutter.so
<a)."="" href="https://www.w3.org/Style/CSS/Test/Fonts/Ahem/">https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).	lib/armeabi-v7a/libflutter.so

✉ 邮箱线索

邮箱地址	所在文件
ccc_icon@2x.png ccc_icon@3x.png bi@2x.png bi@3x.png gou@2x.png gou@3x.png gou_pink@3x.png withdraw@2x.png withdraw@3x.png	Mogua Engine V2
avlusir@gmail.com _typeerror@0150898._create _immutablelist@0150898._nk _double@0150898.fromintege _growablelist@0150898._literal _az@706287047.yqe gou_pink@3x.png withdraw@3x.png _bytebuffer@7027147._new ccc_icon@3x.png _assertionerror@0150898._create bi@3x.png gou@3x.png	lib/armeabi-v7a/libapp.so
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so

☰ 手机线索

🌸 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=lusir, ST=lusir, L=lusir, O=lusir, OU=lusir, CN=lusir
签名算法: rsassa_pkcs1v15
有效期自: 2023-06-15 07:23:10+00:00
有效期至: 2050-10-31 07:23:10+00:00
发行人: C=lusir, ST=lusir, L=lusir, O=lusir, OU=lusir, CN=lusir
序列号: 0x2cfdfeac
哈希算法: sha256
md5值: 16af6b7ca60293b1411607c990281b18
sha1值: 2ecb28ce21c76a07fea813e96646f2172b9b7b04
sha256值: eb7c9bffe313478feea51f3779ceb4d1eff87ca25b278a61118d87a8b032e39e
sha512值: d6be5d980b26d5f07d6a2cf3443501522bd0eaf9aaaf449f3743723cbade177c311c373018915aebetae62de919ab5700c1660c1e74adc99373d2fe1fac5ebca
公钥算法: rsa
密钥长度: 2048
指纹: cb03c5838e00ab9dc9f7faf2013791173841977309c5ba8d221741d88ad17229

🔑 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.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_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.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。
com.tvlutv.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信