



MoGua

快手约炮 4.1.0.APK 分析报告



APP名称:

快手约炮

包名: com.md.mdzhihu240722

域名线索: 39条

URL线索: 10条

邮箱线索: 0条

分析日期: 2025年7月19日

分析平台: [摸瓜APK反编译平台](#)

文件名: zhihu240722_zhihu_240713_4.1.0 101.apk
文件大小: 39.2MB
MD5值: 8e89839fee6842181304a015cb600978
SHA1值: bd3c7742628f83a63f5c44317693073581bd8d56
SHA256值: 6cbf51d3c47d44c9740451fb0575421eec2656c5348faf5892f201cab493c83b

i APP 信息

App名称: 快手约炮
包名: com.md.mdzhihu240722
主活动Activity: com.example.zhihu_client.MainActivity
安卓版本名称: 4.1.0
安卓版本: 101

🔍 域名线索

域名	服务器信息
eghrty.fgbhiojegr9.com8	没有服务器地理信息.
vip1-cre.bscdnd.com	IP: 172.247.238.68 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052570 经度: -118.243904
mdksbls3img.mm-thk.com	IP: 218.11.6.238 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041599 经度: 114.478081

aomedia.org	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
mdksbls3img.mm-thk.com.slowdark.com	IP: 218.11.6.238 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041599 经度: 114.478081
schemas.microsoft.com	IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
ifbgkeowq.keuaosld.com8	没有服务器地理信息.
dsy5y4qpkltc2.cloudfront.net8	没有服务器地理信息.
d2v33kdrpsrqsx.cloudfront.net8	没有服务器地理信息.
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
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
sketch.com	IP: 13.249.160.67 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
230424cdn-mb.cdn1008.com	IP: 101.227.79.216 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
gtm-sg-6wr308fr422.gtm-i2d3.com	IP: 14.128.34.40 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
d23jd0j9r0fajb.cloudfront.net	IP: 18.65.168.102 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
exoplayer.dev	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
	IP: 103.51.147.152 所属国家: Hong Kong

frtyjerw.ijkfrghj9.com	地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
stackoverflow.com	IP: 104.18.32.7 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
d2v33kdrpsrqszy.cloudfront.net	IP: 13.35.51.126 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
hcdnw122.maoyun.cdnhwcbv122.com	IP: 218.11.6.238 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041599 经度: 114.478081
developer.apple.com	IP: 17.253.87.202 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
mmpp4.hcjvdum.com	IP: 172.67.156.156 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
asddui49shbcudjhj.com	IP: 101.227.79.216 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
dsy5y4qpkltc2.cloudfront.net	IP: 99.84.50.75 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
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 纬度: 40.065647 经度: -79.891724
ifbgkeowq.keuaosld.com	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
	IP: 34.111.97.67 所属国家: United States of America

developer.mozilla.org	地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
mdksbls3img.mm-thk.com.fc1bcf28.cdnhwcaoc115.cn	IP: 218.11.6.238 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041599 经度: 114.478081
frtyjerw.ijkfrghj9.com8	没有服务器地理信息.
eghrty.fgbhiojegr9.com	IP: 103.51.147.154 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
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
zy.zhouyilsadjkfsadfs.com	IP: 14.128.34.40 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
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
ghk.ikjiew93gh.com8	没有服务器地理信息.
www.ibm.com	IP: 23.13.189.250 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
ghk.ikjiew93gh.com	IP: 103.51.147.154 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
137.220.137.58	IP: 137.220.137.58 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322

 URL线索

URL信息	Url所在文件
http://ns.adobe.com/xap/1.0/\u0000	b/i/a/a.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	c/i/a/a/n1.java
https://x</LA_URL>	c/i/a/a/w1/d0.java

https://x	c/i/a/a/w1/d0.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	c/i/a/a/w1/e0.java
https://developer.apple.com/streaming/emsg-id3	c/i/a/a/z1/j/a.java
https://aomedia.org/emsg/ID3	c/i/a/a/z1/j/a.java
https://developer.android.com/reference/javax/net/ssl/SSLSocket	io/flutter/plugins/k/t.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/d.java
https://github.com/flutter/flutter/issues/2897).It	io/flutter/plugin/platform/k.java
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://schemas.android.com/apk/res/android	摸瓜V3引擎
vip1-cre.bscdnd.com	摸瓜V3引擎
https://ifbgkeowq.keuaosld.com	摸瓜V3引擎
https://github.com/flutter/flutter/issues/2897).It	摸瓜V3引擎
mdksbls3img.mm-thk.com	摸瓜V3引擎
https://frtyjerw.ijkfrghj9.com	摸瓜V3引擎
https://frtyjerw.ijkfrghj9.com8	摸瓜V3引擎
https://aomedia.org/emsg/ID3	摸瓜V3引擎
https://ghk.ikjiew93gh.com	摸瓜V3引擎

mdksbIs3img.mm-thk.com.slowdark.com	摸瓜V3引擎
https://api.flutter.dev/flutter/material/Scaffold/of.html	摸瓜V3引擎
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released	摸瓜V3引擎
http://dashif.org/guidelines/trickmode	摸瓜V3引擎
https://api.flutter.dev/flutter/material/Scaffold/of.html8	摸瓜V3引擎
https://eghrty.fgbhiojegr9.com8	摸瓜V3引擎
https://ghk.ikjiew93gh.com8	摸瓜V3引擎
humpiex	摸瓜V3引擎
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd	摸瓜V3引擎
https://github.com/richtr/NoSleep.js/issues/15	摸瓜V3引擎
230424cdn-mb.cdn1008.com	摸瓜V3引擎
https://eghrty.fgbhiojegr9.com	摸瓜V3引擎
https://d2v33kdrpsrqs.cloudfront.net8	摸瓜V3引擎
https://flutter.dev/go/remove-fab-accent-theme-dependency.	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
gtm-sg-6wr308fr422.gtm-i2d3.com	摸瓜V3引擎
d23jd0j9r0fajb.cloudfront.net	摸瓜V3引擎

https://mmpp4.hcjvdum.com/	摸瓜V3引擎
https://sketch.com	摸瓜V3引擎
frtyjerw.ijkfrghj9.com	摸瓜V3引擎
d2v33kdrpsrqszy.cloudfront.net	摸瓜V3引擎
hcdnw122.maoyun.cdnhwcibv122.com	摸瓜V3引擎
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	摸瓜V3引擎
http://137.220.137.58/ksdomain	摸瓜V3引擎
asddui49shbcudjhj.com	摸瓜V3引擎
uumdkraf	摸瓜V3引擎
https://developer.android.com/guide/topics/permissions/overview	摸瓜V3引擎
dsy5y4qpkltc2.cloudfront.net	摸瓜V3引擎
https://ifbgkeowq.keuaosld.com8	摸瓜V3引擎
https://github.com/flutter/flutter/issues/new.8	摸瓜V3引擎
ifbgkeowq.keuaosld.com	摸瓜V3引擎
https://dsy5y4qpkltc2.cloudfront.net8	摸瓜V3引擎
https://stackoverflow.com/questions/tagged/flutter	摸瓜V3引擎
https://github.com/tekartik/sqlite/blob/master/sqlite/doc/supported_types.md	摸瓜V3引擎
mdksbls3img.mm-thk.com.fc1bcf28.cdnhwcaoc115.cn	摸瓜V3引擎

play.googleapis.com	摸瓜V3引擎
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd8	摸瓜V3引擎
https://mmpp4.hcjvdum.com/8	摸瓜V3引擎
eghrty.fgbhiojegr9.com	摸瓜V3引擎
https://developer.android.com/reference/javax/net/ssl/SSLSocket	摸瓜V3引擎
zy.zhouyilsadjkfsadsf.com	摸瓜V3引擎
https://d2v33kdrpsrqs.cloudfront.net	摸瓜V3引擎
leqhipvlwy	摸瓜V3引擎
http://dashif.org/guidelines/last-segment-number	摸瓜V3引擎
https://github.com/flutter/flutter/issues/new.	摸瓜V3引擎
ghk.ikjiew93gh.com	摸瓜V3引擎

 邮箱线索

 手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/ljkMediaMeta.java

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=zhihu240722, ST=zhihu240722, L=zhihu240722, O=zhihu240722, OU=zhihu240722, CN=zhihu240722
签名算法: rsassa_pkcs1v15
有效期自: 2024-07-19 16:15:17+00:00
有效期至: 2051-12-05 16:15:17+00:00
发行人: C=zhihu240722, ST=zhihu240722, L=zhihu240722, O=zhihu240722, OU=zhihu240722, CN=zhihu240722
序列号: 0x659a95c2
哈希算法: sha256
md5值: cf41461aec9ae1f4e4827bda29aabb8e
sha1值: 93b58d1b86905c4393c14d22a5806d959d4e4bf2
sha256值: 29abf80731add0435189694922aea7d8cbab3b665bd104234cba9a59c55d5a4b
sha512值: 470e94182226bf16172e7c5e50814afd3d4af285d00d855075103b42363e1bd605e36b6b9ffc1ae7308d9aed251975d0ec3036b7f0957eb432bead7a5a8848af
公钥算法: rsa
密钥长度: 2048
指纹: 66603bbf352b01723ac331cbb95af54a2a6bd2fd39d81d999b24beb91ce25d66

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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
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

应用内通信