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

**快手约炮（ 4.1.0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 | 快手约炮 |
| 版本 | 4.1.0 |
| 包名 | com.md.mdzhihu240722 |
| 域名线索 | 39条 |
| URL线索 | 10条 |
| APP图标 |  |
| 分析日期 | 2025年7月19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 | zhihu240722\_zhihu\_240713\_4.1.0 101.apk |
| 文件大小 | 39.2MB |
| MD5值 | 8e89839fee6842181304a015cb600978 |
| SHA1值 | bd3c7742628f83a63f5c44317693073581bd8d56 |
| SHA256值 | 6cbf51d3c47d44c9740451fb0575421eec2656c5348faf5892f201cab493c83b |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 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 |
| mdksbls3img.mm-thk.com | IP: 218.11.6.238  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| aomedia.org | IP: 185.199.108.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| mdksbls3img.mm-thk.com.slowdark.com | IP: 218.11.6.238  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| schemas.microsoft.com | IP: 13.107.246.73  所属国家: United States of America  地区: Washington  城市: Redmond |
| ifbgkeowq.keuaosld.com8 | 没有服务器地理信息. |
| dsy5y4qpkltc2.cloudfront.net8 | 没有服务器地理信息. |
| d2v33kdrpsrqsz.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 |
| api.flutter.dev | IP: 199.36.158.100  所属国家: United States of America  地区: California  城市: Mountain View |
| sketch.com | IP: 13.249.160.67  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| 230424cdn-mb.cdn1008.com | IP: 101.227.79.216  所属国家: China  地区: Shanghai  城市: Shanghai |
| 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 |
| d23jd0j9r0fajb.cloudfront.net | IP: 18.65.168.102  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| exoplayer.dev | IP: 185.199.108.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| frtyjerw.ijkfrghj9.com | IP: 103.51.147.152  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| stackoverflow.com | IP: 104.18.32.7  所属国家: United States of America  地区: California  城市: San Francisco |
| d2v33kdrpsrqsz.cloudfront.net | IP: 13.35.51.126  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| hcdnw122.maoyun.cdnhwcibv122.com | IP: 218.11.6.238  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| developer.apple.com | IP: 17.253.87.202  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| mmpp4.hcjvdum.com | IP: 172.67.156.156  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 |
| asddui49shbcudjhj.com | IP: 101.227.79.216  所属国家: China  地区: Shanghai  城市: Shanghai |
| dsy5y4qpkltc2.cloudfront.net | IP: 99.84.50.75  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| 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 |
| ifbgkeowq.keuaosld.com | IP: 0.0.0.0  所属国家: -  地区: -  城市: - |
| developer.mozilla.org | IP: 34.111.97.67  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| mdksbls3img.mm-thk.com.fc1bcf28.cdnhwcaoc115.cn | IP: 218.11.6.238  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| 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 |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| zy.zhouyilsadjkfsadfs.com | IP: 14.128.34.40  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| flutter.dev | IP: 199.36.158.100  所属国家: United States of America  地区: California  城市: Mountain View |
| 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 |
| ghk.ikjiew93gh.com | IP: 103.51.147.154  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| 137.220.137.58 | IP: 137.220.137.58  所属国家: Japan  地区: Tokyo  城市: Tokyo |

### **4.2 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 |
| mdksbls3img.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://d2v33kdrpsrqsz.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 |
| d2v33kdrpsrqsz.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/sqflite/blob/master/sqflite/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.zhouyilsadjkfsadfs.com | 摸瓜V3引擎 |
| https://d2v33kdrpsrqsz.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 |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184 | tv/danmaku/ijk/media/player/IjkMediaMeta.java |

## **5. 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**

## **6. 硬编码敏感信息**

## **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.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 |

## **10. 应用内通信**

**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。**