



MoGua

上帝视角 1.1.3.APK 分析报告



APP名称:

上帝视角

包名:	videolive.keystore.app
域名线索:	18条
URL线索:	22条
邮箱线索:	3条
分析日期:	2025年7月5日
分析平台:	摸瓜APK反编译平台

文件名: qisem_117.apk
文件大小: 51.16MB
MD5值: 1732e7e1110b63144e657048045b4701
SHA1值: c7253698ea8aec07650725eed17c483f8e77199
SHA256值: 68e3760dd641a4bc24bba2fbc657adfa35b8d044c766f1ca14e4fdd8842bfc74

i APP 信息

App名称: 上帝视角
包名: videolive.keystore.app
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.1.3
安卓版本: 1

🔍 域名线索

域名	服务器信息
quilljs.com	IP: 172.66.43.93 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
webapi.amap.com	IP: 218.11.15.216 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041599 经度: 114.478081
vuejs.org	IP: 3.33.186.135 所属国家: United States of America 地区: Washington

	城市: Seattle 纬度: 47.627499 经度: -122.346199
ask.dcloud.net.cn	IP: 123.12.235.54 所属国家: China 地区: Henan 城市: Hebi 纬度: 35.899170 经度: 114.192497
www.google.com	IP: 199.59.148.96 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
m3w.cn	IP: 116.196.150.249 所属国家: China 地区: Zhejiang 城市: Jinhua 纬度: 30.013470 经度: 120.288658
service.dcloud.net.cn	IP: 110.40.169.99 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
er.dcloud.io	没有服务器地理信息.
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
apiproxytteea.top	IP: 111.230.107.58 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
maps.googleapis.com	IP: 142.250.217.106 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.
map.qq.com	IP: 116.130.224.82 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
apis.map.qq.com	IP: 116.130.223.114 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

er.dcloud.net.cn	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
ns.adobe.com	没有服务器地理信息.
api.map.baidu.com	IP: 111.206.208.72 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

 URL线索

URL信息	Url所在文件
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/e/b/a.java

https://ask.dcloud.net.cn/article/35877	io/dcloud/e/b/a.java
https://er.dcloud.io/rv	io/dcloud/e/c/h/b.java
https://er.dcloud.net.cn/rv	io/dcloud/e/c/h/b.java
https://ask.dcloud.net.cn/article/283	io/dcloud/g/b.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
https://ask.dcloud.net.cn/article/36199	摸瓜V1引擎
https://github.com/uuidjs/uuid	摸瓜V2引擎
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=\$	摸瓜V2引擎
https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=	摸瓜V2引擎
https://www.google.com/maps/?daddr=	摸瓜V2引擎
https://www.google.com/maps/	摸瓜V2引擎
https://quilljs.com/	摸瓜V2引擎
https://quilljs.com	摸瓜V2引擎
https://apiproxytteea.top:8443/api	摸瓜V2引擎
https://vuejs.org/error-reference/	摸瓜V2引擎

https://service.dcloud.net.cn/uniapp/feedback.html	摸瓜V2引擎
https://map.qq.com/api/js?v=2.exp&	摸瓜V2引擎
https://maps.googleapis.com/maps/api/js?	摸瓜V2引擎
https://webapi.amap.com/maps?v=2.0&	摸瓜V2引擎
https://api.map.baidu.com/api?type=webgl&v=1.0&	摸瓜V2引擎

 邮箱线索

邮箱地址	所在文件
tab1@2x.png tab1-2@2x.png tab2@2x.png tab2-2@2x.png tab4@2x.png tab4-2@2x.png	摸瓜V2引擎
jhruby.web@gmail.com livebg@2x.png img@2x.png shexiangtou-4@2x.png zuanshi@2x.png bofang@2x.png vip@2x.png icon7@2x.png icon4@2x.png icon5@2x.png icon8@2x.png xuanzhong@2x.png zhuyi-2@2x.png dianzan@2x.png	摸瓜V2引擎

jt2@2x.png iconren@2x.png icontime@2x.png	
tab1@2x.png tab1-2@2x.png tab2@2x.png tab2-2@2x.png tab4@2x.png tab4-2@2x.png	摸瓜V2引擎

☰ 手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.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=aa, ST=Unknown, L=aa, O=aa, OU=aa, CN=aa
签名算法: rsassa_pkcs1v15
有效期自: 2024-11-28 12:20:27+00:00
有效期至: 2124-11-04 12:20:27+00:00
发行人: C=aa, ST=Unknown, L=aa, O=aa, OU=aa, CN=aa
序列号: 0x59742c38
哈希算法: sha256
md5值: 71b591bed20287287740f24cc75716f1
sha1值: 2f7bfbb62bf92e1ac3adcb7517734f768aaa2215
sha256值: 3a4c8df65b1d8951525d0c98cc5e87f264f1863ddd5d2c439e7f56c9b6ab944e

sha512值: 4a27e150e12f0fa9769da349ac0f93e7433904c27911180f23b67e929fdf20adaebc0a916a2369d94dba107e9b1d6293c93fd5da9686e32d3c612751941cef1e
公钥算法: rsa
密钥长度: 2048
指纹: b7b237d21e3bbeb15d4da09748770bd186412ef031b5507ac00b1b42f9d677b8

硬编码敏感信息

可能的敏感信息
"dcloud_common_user_refuse_api" : "the user denies access to the API"
"dcloud_io_without_authorization" : "not authorized"
"dcloud_oauth_authentication_failed" : "failed to obtain authorization to log in to the authentication service"
"dcloud_oauth_empower_failed" : "the Authentication Service operation to obtain authorized logon failed"
"dcloud_oauth_logout_tips" : "not logged in or logged out"
"dcloud_oauth_oauth_not_empower" : "oAuth authorization has not been obtained"
"dcloud_oauth_token_failed" : "failed to get token"
"dcloud_permissions_reauthorization" : "reauthorize"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"dcloud_io_without_authorization" : "没有获得授权"
"dcloud_oauth_authentication_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_empower_failed" : "获取授权登录认证服务操作失败"

"dcloud_oauth_logout_tips" : "未登录或登录已注销"
"dcloud_oauth_oauth_not_empower" : "尚未获取oauth授权"
"dcloud_oauth_token_failed" : "获取token失败"
"dcloud_permissions_reauthorization" : "重新授权"

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.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_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.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
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntryActivity	Schemes: ://,