



MoGua

油管18+ 1.0.3.APK 分析报告



APP名称:

油管18+

包名:	zkuma.dtkda.lwmdi
域名线索:	20条
URL线索:	19条
邮箱线索:	2条
分析日期:	2025年7月8日
分析平台:	摸瓜APK反编译平台

文件名: ytbs80675-v4.16.168.apk
文件大小: 24.88MB
MD5值: 38112714ed8f07981b8dbb2d0f829693
SHA1值: 63180312510d9c6b045d96d54d65f0c3ef8effa3
SHA256值: eb18379d7ab3117ed687542c736aa98384e1a66f7b7d61ed1017b83a49598766

i APP 信息

App名称: 油管18+
包名: xkuma.dtkda.lwmdi
主活动Activity: xkuma.dtkda.lwmdi.MainActivity
安卓版本名称: 1.0.3
安卓版本: 4

🔍 域名线索

域名	服务器信息
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
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
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
dartbug.com	IP: 216.239.34.21 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
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
developer.android.com	IP: 142.250.73.142 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
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
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

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
g.co	IP: 142.250.217.110 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
issuetracker.google.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.ibm.com	IP: 23.42.126.170 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
default.url	没有服务器地理信息.
r9nhvykt.vip	IP: 104.21.36.105 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
	IP: 64.182.27.164 所属国家: United States of America

www.unicode.org	地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204
developer.mozilla.org	IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
aomedia.org	IP: 122.248.226.57 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
developer.apple.com	IP: 17.253.85.201 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
ns.adobe.com	没有服务器地理信息.
journeyapps.com	IP: 13.35.37.111 所属国家: Taiwan (Province of China) 地区: Taipei 城市: Taipei 纬度: 25.038172 经度: 121.563599

URL信息	Url所在文件
http://dashif.org/guidelines/last-segment-number	c1/d.java
http://dashif.org/guidelines/trickmode	c1/d.java
http://dashif.org/thumbnail_tile	c1/d.java
http://dashif.org/guidelines/thumbnail_tile	c1/d.java
https://github.com/Baseflow/flutter-permission-handler/issues	e4/t.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/g.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	d1/n0.java
<a href="https://x</LA_URL>">https://x</LA_URL>	d1/m0.java
https://default.url	d1/m0.java
https://issuetracker.google.com/issues/new?component=413107&template=1096568	g3/c.java
https://docs.flutter.dev/deployment/android	p8/d.java
https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted	w0/q.java
http://g.co/dev/packagevisibility	w0/w.java
https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread	y0/v0.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	f0/m.java
http://ns.adobe.com/xap/1.0/	e2/b.java
https://aomedia.org/emsg/ID3	h2/a.java

https://developer.apple.com/streaming/emsg-id3	h2/a.java
https://journeyapps.com/	摸瓜V1引擎
https://github.com/journeyapps/zxing-android-embedded	摸瓜V1引擎
https://github.com/nodeca/pica	摸瓜V2引擎
https://github.com/richttr/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://www.unicode.org/copyright.html	lib/arm64-v8a/libflutter.so
https://github.com/flutter/flutter/issues	lib/arm64-v8a/libflutter.so
https://dartbug.com/52121	lib/arm64-v8a/libflutter.so
https://r9nhvykt.vip/front/	lib/armeabi-v7a/libapp.so
https://developer.mozilla.org/en-US/docs/Web/HTTP/Status	lib/armeabi-v7a/libapp.so
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
https://github.com/dart-lang/language/issues/3488	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android	lib/armeabi-v7a/libapp.so
http://www.unicode.org/copyright.html	lib/armeabi-v7a/libflutter.so
https://github.com/flutter/flutter/issues	lib/armeabi-v7a/libflutter.so

https://dartbug.com/52121.	lib/armeabi-v7a/libflutter.so
----------------------------	-------------------------------

✉ 邮箱线索

邮箱地址	所在文件
appro@openssl.org	lib/arm64-v8a/libflutter.so
_immutablelist@0150898._mk _double@0150898.fromintege _growablelist@0150898._literal _tca@32287047.lzc _typeerror@0150898._create _bytebuffer@7027147._new _assertionerror@0150898._create	lib/armeabi-v7a/libapp.so

☰ 手机线索

手机号	所在文件
17512775099	z6/a.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: CN=11, OU=11, O=11, L=11, ST=11, C=11
签名算法: rsassa_pkcs1v15
有效期自: 2024-06-25 10:40:39+00:00
有效期至: 2049-06-19 10:40:39+00:00
发行人: CN=11, OU=11, O=11, L=11, ST=11, C=11
序列号: 0x1
哈希算法: sha256
md5值: 46f7ee99233c2bc90d8ed8c817b9b5ce
sha1值: c91f6f18b5566b81f794ee942086cfa3f001b3c9
sha256值: 1b5ea7f7f2b468cada5a69fb293fbc8436d528cf49e078401ce648d56dc90cdf
sha512值: 626d2d76cc4a3637c27917b4f0a8d79f08495199f4dd6a2b9e4f45975e0d8fb3420fe7c360b930ad5867105e3575ef5dcceca6779d0947b775dcf5c174675891
公钥算法: rsa
密钥长度: 2048
指纹: a3a44d67a1443286ed5c58857b9bd389a7855f76470da52aa62303f869aec15a

硬编码敏感信息

可能的敏感信息
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.READ_MEDIA_AUDIO	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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
android.permission.ADD_VOICEMAIL	危险	将语音邮件添加到系统中	允许应用程序将语音邮件添加到系统中
android.permission.USE_SIP	危险	拨打/接听互联网电话	允许应用程序使用 SIP 服务拨打/接听互联网电话
android.permission.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
android.permission.WRITE_CALL_LOG	危险		允许应用程序写入（但不读取）用户号召日志数据。
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
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.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.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.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
xkuma.dtkda.lwmdi.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信