MoGua

xxxxx 3.2.8.APK 分析报告

APP名称:	xxxxx
包名:	com.klhlejau.wtniby

域名线索:	18条
URL线索:	46条
邮箱线索:	0条
分析日期:	2025年7月31日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 72796c3fb8d0401d1e3740dec6ac3c18.apk
文件大小: 47.28MB
MD5值: ec344188d13ebe471383904611015c44
SHA1值: 33984561761fc3a105467ff9a98382eefbc97c8b
SHA256值: 91fe7c9edd75ffd597e09f53e3b46d52848f76a54fd58ff2427f2e6efb115ca5

APP 信息

App名称: xxxxx
包名: com.klhlejau.wtniby
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 3.2.8
安卓版本: 999

域名线索

域名	服务器信息
ext.dcloud.net.cn	**IP**: 123.125.244.28 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
apis.map.qq.com	**IP**: 116.130.224.140 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.ceshi.com	**IP**: 170.33.13.248 **所属国家**: United States of America **地区**: Virginia **城市**: Herndon **纬度**: 38.969570 **经度**: -77.386147
schemas.android.com	没有服务器地理信息.
er.dcloud.io	没有服务器地理信息.
	IP: 123.125.244.28 **所属国家**: China

ask.dcloud.net.cn	**地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
s2.ax1x.com	**IP**: 116.202.217.92 **所属国家**: Germany **地区**: Bayern **城市**: Gunzenhausen **纬度**: 48.323860 **经度**: 11.601019
ns.adobe.com	没有服务器地理信息.
m3w.cn	**IP**: 116.196.150.237 **所属国家**: China **地区**: Zhejiang **城市**: Jinhua **纬度**: 30.013470 **经度**: 120.288658
at.alicdn.com	**IP**: 221.195.63.237 **所属国家**: China **地区**: Hebei **城市**: Cangzhou **纬度**: 38.316669 **经度**: 116.866669
zego-public.oss-cn-shanghai.aliyuncs.com	**IP**: 0.0.0.0 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
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
	IP: 127.0.0.1

er.dcloud.net.cn	**所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
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
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
storage.zego.im	IP: 116.142.235.232 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
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
www.google.com	IP: 199.16.158.182 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
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://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/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://ask.dcloud.net.cn/article/283	io/dcloud/feature/utsplugin/ProxyModule.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/p/r.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/p/r.java
https://ask.dcloud.net.cn/article/283	io/dcloud/p/h1.java
https://er.dcloud.io/rv	io/dcloud/p/d0.java
https://er.dcloud.net.cn/rv	io/dcloud/p/d0.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://service.dcloud.net.cn/uniapp/feedback.html	摸瓜V2引擎
https://s2.ax1x.com/2020/03/10/8CvKmt.png	摸瓜V2引擎
https://s2.ax1x.com/2020/03/10/8CjxSJ.png	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
http://www.ceshi.com	摸瓜V2引擎
https://apis.map.qq.com/ws/	摸瓜V2引擎
https://apis.map.qq.com/ws/place/v1/search	摸瓜V2引擎
https://apis.map.qq.com/ws/geocoder/v1/	摸瓜V2引擎
https://apis.map.qq.com/ws/district/v1/list	摸瓜V2引擎
https://apis.map.qq.com/ws/district/v1/getchildren	摸瓜V2引擎
https://apis.map.qq.com/ws/distance/v1/	摸瓜V2引擎
https://apis.map.qq.com/ws/direction/v1/	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://ext.dcloud.net.cn/plugin?id=3617	摸瓜V2引擎
https://at.alicdn.com/t/font_2442084_o72ps3802ih.eot);src:url(https://at.alicdn.com/t/font_2442084_o72ps3802ih.eot	摸瓜V2引擎
https://at.alicdn.com/t/font_2442084_o72ps3802ih.woff2)	摸瓜V2引擎
https://at.alicdn.com/t/font_2442084_o72ps3802ih.woff)	摸瓜V2引擎
https://at.alicdn.com/t/font_2442084_o72ps3802ih.ttf)	摸瓜V2引擎

https://at.alicdn.com/t/font_2442084_o72ps3802ih.svg	摸瓜V2引擎
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=	摸瓜V2引擎
https://quilljs.com/	摸瓜V2引擎
https://quilljs.com	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://storage.zego.im/demo/201808270915.mp4	摸瓜V2引擎
http://zego-public.oss-cn-shanghai.aliyuncs.com/sdk-doc/assets/bike.mp3	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎

https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎

邮箱线索

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: True
找到 1 个唯一证书
主题: C=eshOx, ST=T9EL2, L=kBlAQ, O=qz1752716646998, OU=pv1752716646998, CN=oooe
签名算法: rsassa_pkcs1v15
有效期自: 2025-07-17 01:44:07+00:00
有效期至: 2075-07-05 01:44:07+00:00

发行人: C=eshOx, ST=T9EL2, L=kBlAQ, O=qz1752716646998, OU=pv1752716646998, CN=oooe
序列号: 0x79214484
哈希算法: sha512
md5值: 0e0b3af238497b0084e98b69b47cddcd
sha1值: b372d6a37ff26e342d959af9671934ceca3dbdcb
sha256值: 15935ef35ddf957e860f96ef30dc29bf0ad26e607ad772fe747f731c7633352a
sha512值: 98dcf562ee25f064a48e3898b5e6e152f27a4662fc46c10bebfe32ae92c70f30b4041b9669a0400caa90b94a63dac0681a27b65ce01c7562aaf20aea967a5652
公钥算法: rsa
密钥长度: 4096
指纹: 7c6e604fe212b5cf9e10c97d4b5ef5855348120d8045f596d90e30ccad730a09

🔑 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_tips_certificate" : "certificate"
"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"
"dcloud_tips_certificate" : "证书"

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**	**类型**	**详细情况**

	险		
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_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_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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
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.START_ACTIVITIES	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正		允许常规应用程序使用 Service.startForeground。

	常		
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
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_COMPANION_START_FOREGROUND_SERVICES_FROM_BACKGROUND	未知	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	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.FOREGROUND_SERVICE_MEDIA_PLAYBACK	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.BIND_JOB_SERVICE	未知	Unknown permission	Unknown permission from android reference
android.permission.DEVICE_POWER	合法	打开或关闭手机	允许应用程序打开或关闭手机
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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径

android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
com.klhlejau.wtniby.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价

android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息

应用内通信
