



MoGua

奕杉聪旅行 1.0.1.APK 分析报告



APP名称:

奕杉聪旅行

包名:	sdad.goacnhlcf
域名线索:	24条
URL线索:	28条
邮箱线索:	0条
分析日期:	2025年7月3日
分析平台:	摸瓜APK反编译平台

文件名: cb184ef765e64b86bb21fa07ecee2fa1.apk
文件大小: 28.95MB
MD5值: f78adf66140a047387bcf73d8beed408
SHA1值: 14f3daf583de73b1939cbe5a9fe9af210c8e1631
SHA256值: 2eae4f9213d0e7c67a1dcbbe8672f7cceb34bbc9edcbb63cb60872ce59d27b7c

i APP 信息

App名称: 奕杉聪旅行
包名: sdad.goacnhlcf
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0.1
安卓版本: 100

🔍 域名线索

域名	服务器信息
www.mescroll.com	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
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
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
mobilegwpre.alipay.com	IP: 110.75.138.35 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
yishanqiangzhi.oss-cn-hangzhou.aliyuncs.com	IP: 118.31.219.205 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
mobilegw.alipay.com	IP: 203.209.245.129 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
schemas.android.com	没有服务器地理信息.
h5.m.taobao.com	IP: 125.38.11.99 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
m3w.cn	IP: 116.196.151.14 所属国家: China 地区: Zhejiang 城市: Jinhua 纬度: 30.013470 经度: 120.288658

ns.adobe.com	没有服务器地理信息.
er.dcloud.io	没有服务器地理信息.
mcgw.alipay.com	IP: 116.142.245.205 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
mobilegw.alipaydev.com	IP: 110.75.132.131 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
loggw-exsdk.alipay.com	IP: 110.76.6.78 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
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
quilljs.com	IP: 172.66.40.163 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

mclient.alipay.com	IP: 116.142.245.227 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
wappaygw.alipay.com	IP: 116.142.245.205 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
wwew.rnhiod.cn	IP: 154.38.118.20 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
render.alipay.com	IP: 124.165.219.237 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
service.dcloud.net.cn	IP: 110.40.181.119 所属国家: China 地区: Beijing 城市: Beijing

	纬度: 39.907501 经度: 116.397102
www.google.com	IP: 199.16.158.12 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
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

 URL线索

URL信息	Url所在文件
https://mobilegwpre.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/m/l/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/m/l/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/m/l/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	com/alipay/sdk/m/l/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/m/l/a.java

https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/m/l/a.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/m/m/a.java
https://render.alipay.com/p/s/i?scheme=%s	com/alipay/sdk/app/OpenAuthTask.java
https://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
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://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://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/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
http://www.rnhiod.cn/	摸瓜V1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://yishanqiangzhi.oss-cn-hangzhou.aliyuncs.com/wangzhi.json?v=	摸瓜V2引擎
https://yishanqiangzhi.oss-cn-hangzhou.aliyuncs.com/zaixiankefu.json?v=	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://www.mescroll.com/img/mescroll-totop.png	摸瓜V2引擎
https://service.dcloud.net.cn/uniapp/feedback.html	摸瓜V2引擎

邮箱线索

手机线索

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=beijing, ST=beijing, L=beijing, O=gs1751003522624, OU=bx1751003522624, CN=gvlz
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-27 05:52:03+00:00
有效期至: 2075-06-15 05:52:03+00:00
发行人: C=beijing, ST=beijing, L=beijing, O=gs1751003522624, OU=bx1751003522624, CN=gvlz
序列号: 0x7bee4f21
哈希算法: sha512
md5值: 00be203a201a2ff5cc40fa661a00849c
sha1值: 717d0723b35e69fe089fb3038d054f44f2d7ed54

sha256值: f6bce14052309270e7ca23ae813c776951850a8504c770f0256c1de55630fcf6

sha512值: f6473c8d3d6a32b9d286154e38c73cd705167b411c43e3c105ca7544fa8a9e2b93878c301eb86333a36ae44a8bb7e8ae0036fcac03dc5e06e7b88788f574090e

公钥算法: rsa

密钥长度: 4096

指纹: 71acc2ec2aa54fce23d4df4361601249388201c5b3e5d6c71ba64504c61dc3b4

 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_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.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.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。

应用内通信

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。