



MoGua

HUA RUN 2.1.5.APK 分析报告



APP名称:

HUA RUN

包名:	vismqnwe.sadhnirwqe
域名线索:	26条
URL线索:	36条
邮箱线索:	0条
分析日期:	2025年6月27日
分析平台:	摸瓜APK反编译平台

文件名: vismqnwe.sadhnirwqe.apk
文件大小: 27.98MB
MD5值: f2fc99fb9f190efc8c127f09a1973df1
SHA1值: 65d8db14a5ab3693b1620ddaa2d781cace9c9e74
SHA256值: 9fde9a32b521f1611984948126e168d82a7cf833a8780cd31b2c95f7ed982e57

i APP 信息

App名称: HUA RUN
包名: vismqnwe.sadhnirwqe
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 2.1.5
安卓版本: 215

🔍 域名线索

域名	服务器信息
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
bit.ly	IP: 67.199.248.10 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.750134 经度: -73.997009
flow.org	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
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
en.wikipedia.org	IP: 103.102.166.224 所属国家: United States of America 地区: Indiana 城市: Francisco 纬度: 38.333290 经度: -87.447083
www.matts411.com	IP: 199.59.243.228 所属国家: United States of America 地区: Florida 城市: Tampa 纬度: 27.943518 经度: -82.510269
ask.dcloud.net.cn	IP: 124.163.195.89 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
m3w.cn	IP: 124.163.195.65 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508

192.252.181.58	IP: 192.252.181.58 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052986 经度: -118.263687
lame.sf.net	IP: 104.18.21.237 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
stackoverflow.com	IP: 104.18.32.7 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
crbug.com	IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
www.tradingview.com	IP: 198.27.124.186 所属国家: Canada 地区: Quebec 城市: Montreal 纬度: 45.508839 经度: -73.587807
www.google.com	IP: 31.13.94.37 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires

	纬度: -34.603600 经度: -58.381554
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
schemas.android.com	没有服务器地理信息.
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
ns.adobe.com	没有服务器地理信息.
www.apache.org	IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
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
html2canvas.hertzen.com	IP: 104.21.65.51 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
html.spec.whatwg.org	IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton 纬度: 40.858585 经度: -74.163605
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
hertzen.com	IP: 104.21.65.51 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.io	没有服务器地理信息.

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
https://ask.dcloud.net.cn/article/35627	b/a.java
https://ask.dcloud.net.cn/article/35877	b/a.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/283	io/dcloud/feature/utsplugin/ProxyModule.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
https://er.dcloud.io/rv	d/c.java
https://er.dcloud.net.cn/rv	d/c.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/283	i/b.java

https://ask.dcloud.net.cn/article/36199	摸瓜V1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
http://192.252.181.58/	摸瓜V2引擎
https://bit.ly/2ZqJzKp	摸瓜V2引擎
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=	摸瓜V2引擎
https://service.dcloud.net.cn/uniapp/feedback.html	摸瓜V2引擎
https://quilljs.com/	摸瓜V2引擎
https://quilljs.com	摸瓜V2引擎
https://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
https://www.tradingview.com/	摸瓜V2引擎
https://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
">https://html2canvas.hertzen.com>	摸瓜V2引擎
">https://hertzen.com>	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎

http://192.252.181.58/;	摸瓜V2引擎
https://flow.org/blog/2017/05/07/Strict-Function-Call-Arity/).	摸瓜V2引擎
https://github.com/facebook/flow/issues/285	摸瓜V2引擎
https://github.com/vuejs/vuex/issues/1505	摸瓜V2引擎
https://vuejs.org/v2/guide/reactivity.html	摸瓜V2引擎
https://vuejs.org/v2/api/	摸瓜V2引擎
https://vuejs.org/v2/guide/components.html	摸瓜V2引擎
http://stackoverflow.com/a/28210364/1070244	摸瓜V2引擎
https://github.com/paldepind/snabbdom/blob/master/LICENSE	摸瓜V2引擎
https://github.com/vuejs/vue/pull/7730	摸瓜V2引擎
http://www.matts411.com/post/internet-explorer-9-oninput/	摸瓜V2引擎
https://github.com/vuejs/vue-devtools'	摸瓜V2引擎
https://vuejs.org/guide/deployment.html	摸瓜V2引擎
https://html.spec.whatwg.org/multipage/indices.html	摸瓜V2引擎
https://html.spec.whatwg.org/multipage/dom.html	摸瓜V2引擎
http://en.wikipedia.org/wiki/Conditional_comment	摸瓜V2引擎
https://vuejs.org/guide/list.html	摸瓜V2引擎
https://crbug.com/v8/8520	lib/armeabi-v7a/libweexjss.so

http://lame.sf.net	lib/armeabi-v7a/liblamemp3.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libnative-image-transcoder.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libstatic-webp.so
https://crbug.com/v8/8520	lib/x86/libweexjss.so
http://lame.sf.net	lib/x86/liblamemp3.so
https://crbug.com/v8/8520	lib/arm64-v8a/libweexjss.so
http://lame.sf.net	lib/arm64-v8a/liblamemp3.so

 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=CN, O=yourcomname, OU=IT, CN=yourcomname
签名算法: rsassa_pkcs1v15
有效期自: 2024-08-25 07:02:08+00:00
有效期至: 2124-08-01 07:02:08+00:00
发行人: C=CN, O=yourcomname, OU=IT, CN=yourcomname
序列号: 0x4785ae60
哈希算法: sha256

md5值: d07f9836da3f8fe92106bfa99c7aaee1
sha1值: ba815f748426193a08a0293be3e9cbb6ff93eea1
sha256值: f8a730b81ef9efc9ecbab47da853fcca07f5db26477b865b491942d298442338
sha512值: 6b7b0076734582be6eb7d6069428a8628c9aebbc9facc5d93018da3717c6a76d90e2d3936f79653bc9b59bfa4740cc8a7b4949fea7d1d4ca53d612d86704e1cc
公钥算法: rsa
密钥长度: 2048
指纹: a57442bcf0baaa0e149a40d64d276b896e6c034f0a923625924815844244919a

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.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
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
com.asus.msa.SupplementaryDID.ACCESS	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。
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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。

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。