



MoGua

健选商城 1.0.0.APK 分析报告



APP名称:

健选商城

包名:	uni.rjjqplu
域名线索:	51条
URL线索:	59条
邮箱线索:	3条
分析日期:	2025年5月1日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: jxsc.apk

文件大小: 66.14MB
MD5值: 3db3e00cd228ab29a04767aa0bdc1e53
SHA1值: 962dec236403a8e2bf9ed186104be46817b0a71f
SHA256值: 52eb6debabc2f4ec36d1245aab2683709491e7f002eea2beb8252c6d65867a28

i APP 信息

App名称: 健选商城
包名: uni.rjjqplu
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0.0
安卓版本: 100

🔍 域名线索

域名	服务器信息
www.openssl.org	IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
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
map.naver.com	IP: 110.93.151.164 所属国家: Korea (Republic of) 地区: Gyeonggi-do 城市: Seongnam

	纬度: 37.420624 经度: 127.126717
jxsc-1333766888.cos.ap-nanjing.myqcloud.com	IP: 112.80.252.187 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
mths.be	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
jxsc-1333767680.cos.ap-guangzhou.myqcloud.com	IP: 36.248.13.151 所属国家: China 地区: Fujian 城市: Fuzhou 纬度: 26.061390 经度: 119.306107
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
www.opensource.org	IP: 104.22.64.197 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
	IP: 203.209.245.120

ccdapi.alipay.com	所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
66.203.153.164	IP: 66.203.153.164 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
api.tianxingjian1.com	没有服务器地理信息.
jindo.dev.naver.com	IP: 125.209.226.151 所属国家: Korea (Republic of) 地区: Gyeonggi-do 城市: Seongnam 纬度: 37.420624 经度: 127.126717
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
jeromeetienne.github.com	没有服务器地理信息.
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
	IP: 119.167.229.233

mdkhk1.kefuzixun.cn	所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
ns.adobe.com	没有服务器地理信息.
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
zenorocha.github.io	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
layer.layui.com	没有服务器地理信息.
chatlink.mstatik.com	IP: 111.206.23.245 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
service.dcloud.net.cn	IP: 110.40.181.119 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
	IP: 142.250.217.110

code.google.com	所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
admin.tianxingjian6.com	没有服务器地理信息.
tupian.xn--isz43i555a.cn	IP: 143.92.56.185 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
www.denso-wave.com	IP: 23.1.162.230 所属国家: Japan 地区: Osaka 城市: Ibaraki 纬度: 34.816425 经度: 135.568909
m3w.cn	IP: 125.38.214.65 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
api.xn--fiq108eduac35c.com	IP: 101.72.224.113 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
naver.com	IP: 223.130.200.236 所属国家: Korea (Republic of) 地区: Gyeonggi-do

	城市: Seongnam 纬度: 37.420624 经度: 127.126717
dev.dcloud.net.cn	IP: 220.194.123.111 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
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
feross.org	IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont 纬度: 37.548271 经度: -121.988571
jxsc-1333762715.cos.ap-beijing.myqcloud.com	IP: 119.188.21.26 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223
ask.dcloud.net.cn	IP: 115.56.90.192 所属国家: China 地区: Henan 城市: Jiaozuo 纬度: 35.239719 经度: 113.233063
	IP: 43.142.57.168

er.dcloud.net.cn	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.
schemas.android.com	没有服务器地理信息.
www.layui.com	没有服务器地理信息.
example.com	IP: 96.7.128.175 所属国家: United States of America 地区: California 城市: El Segundo 纬度: 33.919201 经度: -118.416580
goo.gl	IP: 142.251.211.238 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
laravel.com	IP: 104.18.3.81 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
npms.io	IP: 104.21.80.1 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

popper.js.org	IP: 172.67.73.64 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
vkceyugu.cdn.bspapp.com	IP: 124.95.190.97 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
www.txjcishan.com	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
discourse.threejs.org	IP: 216.66.8.43 所属国家: United States of America 地区: California 城市: Fremont 纬度: 37.517979 经度: -121.929489
at.alicdn.com	IP: 61.182.131.251 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
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
www.d-project.com	IP: 118.27.125.202 所属国家: Japan 地区: Fukuoka 城市: Fukuoka 纬度: 33.583057 经度: 130.399979
www.codefans.net	IP: 103.48.21.158 所属国家: Australia 地区: New South Wales 城市: Petersham 纬度: -33.894600 经度: 151.154953
www.google.com	IP: 157.240.17.35 所属国家: Switzerland 地区: Zurich 城市: Zurich 纬度: 47.366825 经度: 8.549790

 URL线索

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	j/b.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://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://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://ccdcapi.alipay.com/validateAndCacheCardInfo.json?_input_charset=utf-8&cardNo=	摸瓜V2引擎
http://feross.org >	摸瓜V2引擎
http://66.203.153.164:8081	摸瓜V2引擎
https://admin.tianxingjian6.com	摸瓜V2引擎
https://vkceyugu.cdn.bspapp.com/VKCEYUGU-c3481ce3-b8ab-4b73-bc71-dd13f3a1dd98/4de44de2-6ca2-4166-9a34-1879d7e7fd5c.apk	摸瓜V2引擎
https://feross.org/opensource >	摸瓜V2引擎
https://github.com/ecomfe/zrender/blob/master/LICENSE.txt	摸瓜V2引擎
https://example.com	摸瓜V2引擎
https://admin.tianxingjian6.com/uploads/	摸瓜V2引擎
https://jxsc-1333767680.cos.ap-guangzhou.myqcloud.com/jxsc.json	摸瓜V2引擎
https://jxsc-1333766888.cos.ap-nanjing.myqcloud.com/jxsc.json	摸瓜V2引擎
https://jxsc-1333762715.cos.ap-beijing.myqcloud.com/jxsc.json	摸瓜V2引擎
https://api.xn--fiq108educ35c.com/api/v1	摸瓜V2引擎

https://tupian.xn--isz43i555a.cn	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://www.txjcishan.com/	摸瓜V2引擎
https://mths.be/punycode	摸瓜V2引擎
http://goo.gl/MqrFmX\n	摸瓜V2引擎
http://goo.gl/rRqMUw	摸瓜V2引擎
http://goo.gl/MqrFmX\n\n	摸瓜V2引擎
https://discourse.threejs.org/t/updates-to-lighting-in-three-js-r155/53733.	摸瓜V2引擎
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf)	摸瓜V2引擎
https://mdkhk1.kefuzixun.cn/web/im?cptid=487598110ca2	摸瓜V2引擎
https://chatlink.mstatik.com/widget/standalone.html?eid=458090a34d565cb012760ca1cbae370b	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
https://github.com/ecomfe/zrender/blob/master/LICENSE.txt	摸瓜V2引擎
https://api.tianxingjian1.com/api/v1	摸瓜V2引擎
https://admin.tianxingjian6.com/uploads/	摸瓜V2引擎
http://www.d-project.com/	摸瓜V2引擎
	摸瓜V2引擎

http://jeromeetienne.github.com/jquery-qrcode/	摸瓜V2引擎
	摸瓜V2引擎
http://www.opensource.org/licenses/mit-license.php	摸瓜V2引擎
http://www.denso-wave.com/qrcode/faqpatent-e.html	摸瓜V2引擎
http://code.google.com/p/android/issues/detail?id=5141	摸瓜V2引擎
http://jindo.dev.naver.com/collie	摸瓜V2引擎
http://naver.com	摸瓜V2引擎
http://map.naver.com	摸瓜V2引擎
http://dev.dcloud.net.cn/mui	摸瓜V2引擎
http://www.codefans.net	摸瓜V2引擎
https://zenorocha.github.io/clipboard.js	摸瓜V2引擎
https://laravel.com/docs/csrf	摸瓜V2引擎
https://npms.io/search?q=ponyfill .	摸瓜V2引擎
https://popper.js.org)	摸瓜V2引擎
http://layer.layui.com/	摸瓜V2引擎
http://layer.layui.com	摸瓜V2引擎
http://layer.layui.com/mobile	摸瓜V2引擎

https://www.layui.com	摸瓜V2引擎
https://www.layui.com	摸瓜V2引擎
https://www.layui.com	摸瓜V2引擎
https://www.layui.com	摸瓜V2引擎
https://www.layui.com	摸瓜V2引擎
http://www.layui.com/about/layedit/help.html	摸瓜V2引擎
https://www.layui.com	摸瓜V2引擎
https://www.layui.com	摸瓜V2引擎
https://crbug.com/v8/8520	lib/x86/libweexjss.so
http://lame.sf.net	lib/x86/liblamemp3.so
http://www.openssl.org/support/faq.html	lib/x86/libijkffmpegpeg.so
https://crbug.com/v8/8520	lib/arm64-v8a/libweexjss.so

 邮箱线索

邮箱地址	所在文件
jhruby.web@gmail.com	摸瓜V2引擎
icon-ipad-app@2x.png	

on-ipad-notification@2x.png icon-ipad-proapp@2x.png icon-ipad-settings@2x.png icon-ipad-spotlight@2x.png icon-iphone-app@2x.png icon-iphone-app@3x.png -iphone-notification@2x.png -iphone-notification@3x.png icon-iphone-settings@2x.png icon-iphone-settings@3x.png con-iphone-spotlight@2x.png con-iphone-spotlight@3x.png	摸瓜V2引擎
ffmpeg-devel@ffmpeg.org	lib/x86/libijkplayer.so

 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=beijing, ST=beijing, L=beijing, O=cg1740614668979, OU=lo1740614668979, CN=rzgd
签名算法: rsassa_pkcs1v15
有效期自: 2025-02-27 00:04:32+00:00
有效期至: 2075-02-15 00:04:32+00:00
发行人: C=beijing, ST=beijing, L=beijing, O=cg1740614668979, OU=lo1740614668979, CN=rzgd
序列号: 0x257d8ae7

哈希算法: sha512
md5值: 3866831a9248b0bbdfe1a673a8855839
sha1值: d6e819eee0dc95ba78307c017e5c0d421c295abd
sha256值: c9db805d67a75eb9c0fc05449f1265698bfc16c000975221b81acccd06b9d093
sha512值: d7882cc1df694f444020e267eed408e5f0e9b10b64915ec0bf1a5e5c13fce5f7fa8fc8163e3c6ba525c64409a8e6dfacebb835cccefd3fb7415d7b64365e876d
公钥算法: rsa
密钥长度: 4096
指纹: 05eb002d8bce74201c991cb0170235d8e51e643c96afdb702e8f6328b6321b20

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。

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。