



MoGua

原田易购 1.0.1.APK 分析报告



APP名称:

原田易购

包名:	com.zjytx.auction
域名线索:	23条
URL线索:	84条
邮箱线索:	0条
分析日期:	2025年5月8日
分析平台:	摸瓜APK反编译平台

文件名: yuantianv1.apk
文件大小: 24.44MB
MD5值: 464974959367fa02f25cf4d069352d8f
SHA1值: 1ec0b6bde740db22ff5cf47b2d78452e00f17d4d
SHA256值: c597da72e1f56347de274d67ebba666f294c2d9e1d5480e3ccaf48d4ec638c9

i APP 信息

App名称: 原田易购
包名: com.zjytx.auction
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0.1
安卓版本: 102

🔍 域名线索

域名	服务器信息
ns.adobe.com	没有服务器地理信息.
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
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

mclient.alipay.com	IP: 122.156.129.93 所属国家: China 地区: Heilongjiang 城市: Heihe 纬度: 50.266670 经度: 127.466667
loggw-exsdk.alipay.com	IP: 119.42.231.33 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
er.dcloud.net.cn	IP: 43.142.57.168 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
mcgw.alipay.com	IP: 27.221.79.16 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
m3w.cn	IP: 221.204.51.18 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438

	经度: 112.561508
ytapp.bbmai8.com	IP: 116.62.103.118 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
er.dcloud.io	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
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
render.alipay.com	IP: 122.156.129.94 所属国家: China 地区: Heilongjiang 城市: Heihe 纬度: 50.266670 经度: 127.466667
wappaygw.alipay.com	IP: 27.221.79.17 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941

mobilegw.alipay.com	IP: 203.209.243.27 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
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
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
schemas.android.com	没有服务器地理信息.
h5.m.taobao.com	IP: 125.38.11.131 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
www.google.com	IP: 31.13.73.169 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
	IP: 120.53.45.24 所属国家: China

bear.81webren.cn	地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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

 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://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://ytapp.bbmai8.com/uploads/yuantianv1.apk	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2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://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://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎

https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎

https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://bear.81webren.cn/uploads/static/order/detail/location.png	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
http://ytapp.bbmai8.com/static/manage/images/zhizhao.png	摸瓜V2引擎
http://ytapp.bbmai8.com/static/manage/images/dianban.jpg	摸瓜V2引擎
http://ytapp.bbmai8.com/static/manage/images/dianruan.jpg	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎

https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://ytapp.bbmai8.com/index	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

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, ST=zhejiang, L=zhejiang, O=yuantian, OU=yuantianyigou, CN=wang
签名算法: rsassa_pkcs1v15
有效期自: 2022-09-28 09:18:42+00:00
有效期至: 2122-09-04 09:18:42+00:00
发行人: C=cn, ST=zhejiang, L=zhejiang, O=yuantian, OU=yuantianyigou, CN=wang

序列号: 0x29095246
哈希算法: sha256
md5值: 5b9ac4cede17caedaa972fac59f64fb4
sha1值: c65e2eaf7fc35b1916597f56d36c4cc3783fa87d
sha256值: d5d377c926ff23b19da6081b47e50556e2ac28523793aa26b23bc79c3d794998
sha512值: b2c5e5480a8d445d081826778302676a21f7383a857a51beca611965c5947cae23b054f35e525325aa247675434d00dcf1ee64ef33db5ebd91775ea17d8c86cd
公钥算法: rsa
密钥长度: 2048
指纹: 2e8a5f8e8974cae9a2471730cc95923c2bd98a27be15864dcee04ba2577b8d5c

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_feature_confusion_exception_no_private_key_input" : "no private key input"
"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_feature_confusion_exception_no_private_key_input" : "私钥数据为空"
"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

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
		在应用程序上	

com.huawei.android.launcher.permission.CHANGE_BADGE	正常	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.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
com.zjytx.auction.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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