



MoGua

订货系统 1.1.1.APK 分析报告



APP名称:

订货系统

包名:	uni.UNIAA82D7D
域名线索:	17条
URL线索:	24条
邮箱线索:	1条
分析日期:	2025年6月14日
分析平台:	摸瓜APK反编译平台

文件名: oneMallSystem1-v1.1.1(1).apk
文件大小: 16.94MB
MD5值: 01f9eb96a7602d97e26d938372968112
SHA1值: d35b8f783b78d3b8155a60d02fd8b6e47dbc3606
SHA256值: 37831110721146b9c5ab6d8df05f25dcfaf90a0dc23a69bc78abfd3e7528f2ee

i APP 信息

App名称: 订货系统
包名: uni.UNIAA82D7D
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.1.1
安卓版本: 111

🔍 域名线索

域名	服务器信息
ns.adobe.com	没有服务器地理信息.
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
acc.svc.msmlife.com	IP: 39.108.119.255 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545673 经度: 114.068108

ask.dcloud.net.cn	IP: 61.162.174.86 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
www.google.com	IP: 192.133.77.133 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
classonejava.jinmu11.com.cn	IP: 47.99.206.144 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
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
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
er.dcloud.io	没有服务器地理信息.
	IP: 47.99.206.144 所属国家: China

api.jinmu11.com.cn	地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
er.dcloud.net.cn	IP: 43.142.131.213 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
service.dcloud.net.cn	IP: 111.229.199.57 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
schemas.android.com	没有服务器地理信息.
m3w.cn	IP: 27.221.71.65 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223
at.alicdn.com	IP: 218.11.11.173 所属国家: China 地区: Hebei 城市: Shijiazhuang

	纬度: 38.041599 经度: 114.478081
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
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/e/b/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/e/b/a.java
https://er.dcloud.io/rv	io/dcloud/e/c/h/c.java
https://er.dcloud.net.cn/rv	io/dcloud/e/c/h/c.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.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/283	io/dcloud/g/b.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/GifTextView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
https://ask.dcloud.net.cn/article/36199	Mogua Engine V1
http://www.w3.org/2000/svg	Mogua Engine V2
">http://www.w3.org/2000/svg'>	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2
https://acc.svc.msmlife.com/	Mogua Engine V2
https://feross.org/opensource >	Mogua Engine V2
http://api.jinmu11.com.cn/api/	Mogua Engine V2
http://classonejava.jinmu11.com.cn/api/	Mogua Engine V2
http://feross.org >	Mogua Engine V2
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf)	Mogua Engine V2

https://service.dcloud.net.cn/uniapp/feedback.html	Mogua Engine V2
http://www.w3.org/1999/xlink	Mogua Engine V2
http://www.w3.org/2000/svg	Mogua Engine V2
http://www.w3.org/1998/Math/MathML	Mogua Engine V2
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=	Mogua Engine V2
https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=	Mogua Engine V2
https://www.google.com/maps/?daddr=	Mogua Engine V2
https://www.google.com/maps/	Mogua Engine V2
https://quilljs.com/	Mogua Engine V2
https://quilljs.com	Mogua Engine V2

 邮箱线索

邮箱地址	所在文件
jhruby.web@gmail.com	Mogua Engine V2

 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=BJ, L=HD, O=Android, OU=Android, CN=Android Debug
签名算法: rsassa_pkcs1v15
有效期自: 2021-04-12 08:27:53+00:00
有效期至: 2121-03-19 08:27:53+00:00
发行人: C=CN, ST=BJ, L=HD, O=Android, OU=Android, CN=Android Debug
序列号: 0x363bc393
哈希算法: sha256
md5值: 06838cc840093b9d4689fc419ba1a3f3
sha1值: 97c84101b9141c130dd75d7428a2922518c36dcd
sha256值: b01d06180d003e79c7b9088993b8e5ae7a19b0da1161aa097c7f398a6f514fa7
sha512值: 67720eb20639d1f5f9c8b7b201b185ea4364f6a89bedd35aad273002c16d65a7739f59679510d3b96c1f2c3dd3136d9a34451cb679251a86ff4cafdc18314bf
公钥算法: rsa
密钥长度: 2048
指纹: b27ac6d7a4586417c251be6e44179616262379e57da2d1e19db0995be0ddf509

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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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.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.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。
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
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

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。