



MoGua

未成年 2.2.18.APK 分析报告



APP名称:

未成年

包名:	yeye.YinShi.com
域名线索:	22条
URL线索:	16条
邮箱线索:	2条
分析日期:	2025年9月3日
分析平台:	摸瓜APK反编译平台

文件名: jshdc ugdfe.apk
文件大小: 31.44MB
MD5值: 8aefc17919d5cd976ea073a7b3a748f0
SHA1值: 42cedbf312b8e200d3c72e35a75cc99fb0041466
SHA256值: ad5115dd3f681cb48d4d35d10a98aa463e4cfab4cca4a20ef79b85bf32723b24

i APP 信息

App名称: 未 成 年
包名: yeye.YinShi.com
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 2.2.18
安卓版本: 2118

🔍 域名线索

域名	服务器信息
webapi.amap.com	IP: 221.204.10.231 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
api.map.baidu.com	IP: 111.206.208.72 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
marked.js.org	IP: 66.33.60.129 所属国家: Canada 地区: Ontario

	城市: Etobicoke 纬度: 43.623768 经度: -79.559723
prismjs.com	IP: 15.197.167.90 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
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
vuejs.org	IP: 15.197.167.90 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
html2canvas.hertzen.com	IP: 172.67.140.170 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.google.com	IP: 31.13.73.9 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
	IP: 116.130.223.114

apis.map.qq.com	所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
ask.dcloud.net.cn	IP: 123.125.244.31 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
vid-uscdn.aklsjud21oi3dmixo2j.com	IP: 137.175.37.4 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.333698 经度: -121.889297
www.baidu.com	IP: 110.242.69.21 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
map.qq.com	IP: 116.130.224.82 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

hertzen.com	IP: 172.67.140.170 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
maps.googleapis.com	IP: 142.251.215.234 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
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
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
ns.adobe.com	没有服务器地理信息.
	IP: 110.40.169.99

service.dcloud.net.cn	所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
lame.sf.net	IP: 104.18.20.237 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

 URL线索

URL信息	Url所在文件
https://ask.dcloud.net.cn/article/36199	摸瓜V1引擎
https://github.com/markedjs/marked	摸瓜V2引擎
https://marked.js.org/	摸瓜V2引擎
https://github.com/markedjs/marked.	摸瓜V2引擎
https://prismjs.com/download.html	摸瓜V2引擎
>	摸瓜V2引擎
>	摸瓜V2引擎
https://quilljs.com/	摸瓜V2引擎
https://quilljs.com	摸瓜V2引擎

https://vuejs.org/error-reference/	摸瓜V2引擎
https://service.dcloud.net.cn/uniapp/feedback.html	摸瓜V2引擎
https://map.qq.com/api/js?v=2.exp&	摸瓜V2引擎
https://maps.googleapis.com/maps/api/js?	摸瓜V2引擎
https://webapi.amap.com/maps?v=2.0&	摸瓜V2引擎
https://api.map.baidu.com/api?type=webgl&v=1.0&	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://github.com/uuidjs/uuid	摸瓜V2引擎
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=\$	摸瓜V2引擎
https://www.baidu.com/	摸瓜V2引擎
https://vid-uscdn.aklsjud21oi3dmixo2j.com:668/20250403/UsAlMgw1/index.m3u8	摸瓜V2引擎
https://vid-uscdn.aklsjud21oi3dmixo2j.com:668/20250403/UsAlMgw1/index.m3u8	摸瓜V2引擎
https://marked.js.org/	摸瓜V2引擎
https://github.com/markedjs/marked.	摸瓜V2引擎
https://github.com/markedjs/marked	摸瓜V2引擎

https://prismjs.com/download.html	摸瓜V2引擎
http://lame.sf.net	lib/armeabi-v7a/liblamemp3.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libnative-imagetranscoder.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libstatic-webp.so
https://crbug.com/v8/8520	lib/armeabi-v7a/libweexjs.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so

邮箱线索

邮箱地址	所在文件
jhruby.web@gmail.com	摸瓜V2引擎
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so

手机线索

签名证书

APK已签名
v1 签名: False
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=fAQCV, ST=ieFqV, L=DV3Ix, O=mq1753059602882, OU=un1753059602882, CN=dnke

签名算法: rsassa_pkcs1v15
 有效期自: 2025-07-21 01:00:03+00:00
 有效期至: 2075-07-09 01:00:03+00:00
 发行人: C=fAQCV, ST=ieFqV, L=DV3lx, O=mq1753059602882, OU=un1753059602882, CN=dnke
 序列号: 0x4f785ef6
 哈希算法: sha512
 md5值: 5d3bdd86fe5c98be98d964172640fb6f
 sha1值: eb8fa0b12b7ca74264e8b59692abf63d0b1e8aad
 sha256值: 5afccece5b95e0b8748e1ad879416f1af9318c44b7ecffd860e2e127c6bb291c
 sha512值: 730f9d79f9ca21607c7d4753119e6c450ac97cf32929afef5ffcbdb79facdefe64072a4a3ea94d969a52a997a2980b024555f75794c21328781c98842c0a5f24
 公钥算法: rsa
 密钥长度: 4096
 指纹: 9a2228cbbb1dc6a201d9ca175c8086c27e29400fc82ddcb6dce8beb513df2f23

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

yeye.YinShi.com_com.huawei.android.launcher.permission.CHANGE_BADGE	未知	Unknown permission	Unknown permission from android reference
yeye.YinShi.com_com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
yeye.YinShi.com_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
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.CHANGE_WIFI_MULTICAST_STATE	正常	允许Wi-Fi多播接收	允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率
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.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
yeye.YinShi.com.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
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	允许应用程序请求安装	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。

	危险	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.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
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.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: febkyy://,

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。