Evaluation Warning: The document was created with Spire.Doc for Python.

**熊猫社区（ 1.3.8版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 熊猫社区 |
| 版本 | 1.3.8 |
| 包名 | uni.UNI895DA06 |
| 域名线索 | 82条 |
| URL线索 | 23条 |
| APP图标 |  |
| 分析日期 | 2025年6月21日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | 必备组件.apk |
| 文件大小 | 24.89MB |
| MD5值 | 69bd8bbc13173947cfb9ef97c1f5ac4c |
| SHA1值 | 684c9585b8e8c58509fb06df6e89f8818bb4ad47 |
| SHA256值 | 65944815b5a9e10a49b93cee039e13bcb0241ce135d8c3e592651a2e2cabe911 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 熊猫社区 |
| 包名 | uni.UNI895DA06 |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 1.3.8 |
| 安卓版本 | 108 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| tex.stackexchange.com | IP: 104.18.43.226 所属国家: United States of America 地区: California 城市: San Francisco  |
| fanst-1309537472.cos.ap-chongqing.myqcloud.com | IP: 58.144.165.234 所属国家: China 地区: Chongqing 城市: Chongqing  |
| cravatar.cn | IP: 43.161.244.251 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| h5.xiaohaoym.com.cn | 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  |
| dev.mi.com | IP: 123.125.102.202 所属国家: China 地区: Beijing 城市: Beijing  |
| opencloud.wostore.cn | IP: 116.128.209.136 所属国家: China 地区: Beijing 城市: Beijing  |
| doc.sigmob.com | IP: 39.107.65.119 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| render.alipay.com | IP: 27.221.78.203 所属国家: China 地区: Shandong 城市: Qingdao  |
| dev.vivo.com.cn | IP: 221.15.69.48 所属国家: China 地区: Henan 城市: Luoyang  |
| flow.org | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| cn.gravatar.com | IP: 31.13.87.19 所属国家: Taiwan (Province of China) 地区: Taipei 城市: Taipei  |
| www.msa-alliance.cn | IP: 106.75.154.231 所属国家: China 地区: Shanghai 城市: Shanghai  |
| img0.baidu.com | IP: 221.204.61.38 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| tnuiimage.tnkjapp.com | 没有服务器地理信息.  |
| docs.getui.com | IP: 124.160.116.170 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| code.google.com | IP: 142.250.99.113 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.tug.org | IP: 46.4.94.215 所属国家: Germany 地区: Bayern 城市: Gunzenhausen  |
| doc.dcloud.net.cn | IP: 116.196.150.248 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| www.pexels.com | IP: 104.18.67.220 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.xiaohaoym.com.cn | IP: 61.182.138.70 所属国家: China 地区: Hebei 城市: Xingtai  |
| resource.tuniaokj.com | IP: 115.56.90.188 所属国家: China 地区: Henan 城市: Jiaozuo  |
| prismjs.com | IP: 3.33.186.135 所属国家: United States of America 地区: Washington 城市: Seattle  |
| map.baidu.com | IP: 111.206.208.32 所属国家: China 地区: Beijing 城市: Beijing  |
| www.math.lsu.edu | IP: 130.39.247.205 所属国家: United States of America 地区: Louisiana 城市: Baton Rouge  |
| yun.tuia.cn | IP: 116.196.150.248 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| ask.dcloud.net.cn | IP: 124.163.195.89 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| ctan.math.washington.edu | IP: 128.95.224.254 所属国家: United States of America 地区: Washington 城市: Seattle  |
| wap.cmpassport.com | IP: 112.33.111.233 所属国家: China 地区: Anhui 城市: Hefei  |
| gist.github.com | IP: 37.61.54.158 所属国家: Azerbaijan 地区: Baki 城市: Baku  |
| en.wikipedia.org | IP: 31.13.94.10 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires  |
| ctan.math.illinois.edu | IP: 192.17.3.223 所属国家: United States of America 地区: Illinois 城市: Urbana  |
| login.t.cn | IP: 123.56.139.83 所属国家: China 地区: Beijing 城市: Beijing  |
| www.google.com | IP: 31.13.68.169 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| www.pangle.cn | IP: 116.136.186.205 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| stackoverflow.com | IP: 172.64.155.249 所属国家: United States of America 地区: California 城市: San Francisco  |
| qm.qq.com | IP: 125.39.104.69 所属国家: China 地区: Tianjin 城市: Tianjin  |
| bumptech.github.io | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| static.meizu.com | IP: 119.167.193.10 所属国家: China 地区: Shandong 城市: Qingdao  |
| wiki.connect.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| scripts.sil.org | IP: 172.67.29.248 所属国家: United States of America 地区: California 城市: San Francisco  |
| apis.map.qq.com | IP: 116.130.224.140 所属国家: China 地区: Beijing 城市: Beijing  |
| u.kuaishou.com | IP: 103.102.202.80 所属国家: China 地区: Beijing 城市: Beijing  |
| open.oppomobile.com | IP: 123.58.104.1 所属国家: China 地区: Beijing 城市: Beijing  |
| www.unicode.org | IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas  |
| www.yuque.com | IP: 203.107.62.20 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| union.baidu.com | IP: 111.206.208.169 所属国家: China 地区: Beijing 城市: Beijing  |
| www.kuaishou.com | IP: 103.102.202.106 所属国家: China 地区: Beijing 城市: Beijing  |
| weibo.com | IP: 123.125.107.14 所属国家: China 地区: Beijing 城市: Beijing  |
| www.foreverblog.cn | IP: 60.28.220.101 所属国家: China 地区: Tianjin 城市: Tianjin  |
| at.alicdn.com | IP: 221.194.182.10 所属国家: China 地区: Hebei 城市: Langfang  |
| www.fresco-cn.org | IP: 8.212.40.144 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| lbs.amap.com | IP: 110.253.189.212 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| x5.tencent.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| marked.js.org | IP: 66.33.60.34 所属国家: Canada 地区: Ontario 城市: Etobicoke  |
| www.w3schools.com | IP: 23.208.31.24 所属国家: Nigeria 地区: Lagos 城市: Lagos  |
| developer.huawei.com | IP: 120.52.95.238 所属国家: China 地区: Hebei 城市: Langfang  |
| weixin.qq.com | IP: 140.207.122.206 所属国家: China 地区: Shanghai 城市: Shanghai  |
| img.ia14.cn | IP: 103.39.152.8 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.matts411.com | IP: 199.59.243.228 所属国家: United States of America 地区: Florida 城市: Tampa  |
| starimg.starpro.site | IP: 192.229.85.218 所属国家: United States of America 地区: California 城市: Westlake Village  |
| e.qq.com | IP: 220.194.116.85 所属国家: China 地区: Tianjin 城市: Tianjin  |
| vuejs.org | IP: 3.33.186.135 所属国家: United States of America 地区: Washington 城市: Seattle  |
| quilljs.com | IP: 172.66.43.93 所属国家: United States of America 地区: California 城市: San Francisco  |
| en.wikibooks.org | IP: 31.13.106.4 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| app.xiaohaoym.com.cn | 没有服务器地理信息.  |
| connect.microsoft.com | IP: 20.231.239.246 所属国家: United States of America 地区: Virginia 城市: Washington  |
| mirrors.concertpass.com | IP: 162.219.248.112 所属国家: United States of America 地区: California 城市: Chatsworth  |
| neil.fraser.name | IP: 51.195.151.70 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: London  |
| html.spec.whatwg.org | IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| highlightjs.org | IP: 75.2.60.5 所属国家: United States of America 地区: Washington 城市: Seattle  |
| feross.org | IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont  |
| weexapp.com | IP: 203.119.146.33 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| fengyuanchen.github.io | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| service.dcloud.net.cn | IP: 110.40.181.119 所属国家: China 地区: Beijing 城市: Beijing  |
| sq.xiaohaoym.com.cn | IP: 61.182.138.70 所属国家: China 地区: Hebei 城市: Xingtai  |
| facebook.github.io | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| tongji.dcloud.io | IP: 118.25.50.251 所属国家: China 地区: Beijing 城市: Beijing  |
| www.wuruijin.cn | IP: 172.232.112.221 所属国家: India 地区: Maharashtra 城市: Mumbai  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://ask.dcloud.net.cn/article/36199  | 摸瓜V1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://cn.gravatar.com/  | 摸瓜V2引擎  |
| http://feross.org>  | 摸瓜V2引擎  |
| https://img.ia14.cn/upload/2024/7/16/2ea19fa3-0f61-4ffe-8cae-74055bfc41db.png  | 摸瓜V2引擎  |
| https://img.ia14.cn/upload/2024/7/16/0f2d2004-e549-4340-9cbd-c3e8179f842b.png  | 摸瓜V2引擎  |
| https://api.xiaohaoym.com.cn/  | 摸瓜V2引擎  |
| https://sq.xiaohaoym.com.cn/  | 摸瓜V2引擎  |
| https://h5.xiaohaoym.com.cn/  | 摸瓜V2引擎  |
| https://app.xiaohaoym.com.cn/  | 摸瓜V2引擎  |
| https://qm.qq.com/cgi-bin/qm/qr?k=5NH62ptFCVU41qqh-xEHdpx-pkb3Rmog&jump\_from=webapi&authKey=Bo8nkWpFcRLzEKmr/zJAqlst5st8p6fYWhedw/VDd/cQdYw9Zrs8VuGIOXDn/qc1  | 摸瓜V2引擎  |
| http://login.t.cn/A6TVGmxo  | 摸瓜V2引擎  |
| https://h5.xiaohaoym.com.cn/h5/  | 摸瓜V2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://www.foreverblog.cn  | 摸瓜V2引擎  |
| https://github.com/facebook/regenerator/blob/main/LICENSE  | 摸瓜V2引擎  |
| https://prismjs.com/download.html  | 摸瓜V2引擎  |
| https://feross.org/opensource>  | 摸瓜V2引擎  |
| http://qm.qq.com/cgi-bin/qm/qr?\_wv=1027&k=Ugxbp8mgVuunGh9ONjFKRYbNcu9ERMmo&authKey=7JAOX6RODw6EPDWrbGkHKuJb1%2BT4s%2F09NhveJthXAykhL6gMZr%2Bdje7vpbtgW6%2BT&noverify=0&group\_code=570762080  | 摸瓜V2引擎  |
| https://www.yuque.com/senyun-ev0j3/starpro  | 摸瓜V2引擎  |
| https://img0.baidu.com/it/u=1010312865,580100376&fm=253&fmt=auto&app=120&f=JPEG?w=242&h=262  | 摸瓜V2引擎  |
| https://tongji.dcloud.io/uni/stat  | 摸瓜V2引擎  |
| https://tongji.dcloud.io/uni/stat.gif?  | 摸瓜V2引擎  |
| https://resource.tuniaokj.com/images/blogger/avatar\_1.jpeg  | 摸瓜V2引擎  |
| https://resource.tuniaokj.com/images/blogger/avatar\_3.jpeg  | 摸瓜V2引擎  |
| https://resource.tuniaokj.com/images/blogger/avatar\_4.jpeg  | 摸瓜V2引擎  |
| https://resource.tuniaokj.com/images/blogger/avatar\_2.jpeg  | 摸瓜V2引擎  |
| https://www.pexels.com/  | 摸瓜V2引擎  |
| https://starimg.starpro.site/upload/2024/1/27/51139d81-1c5b-4568-a50b-79dae4656a31.png  | 摸瓜V2引擎  |
| https://fanst-1309537472.cos.ap-chongqing.myqcloud.com/headBg.png  | 摸瓜V2引擎  |
| https://cravatar.cn/wp-content/themes/cravatar/assets/img/img1.png  | 摸瓜V2引擎  |
| https://tnuiimage.tnkjapp.com/cool\_bg\_image/icon\_bg2.png)  | 摸瓜V2引擎  |
| https://tnuiimage.tnkjapp.com/cool\_bg\_image/icon\_bg5.png)  | 摸瓜V2引擎  |
| https://tnuiimage.tnkjapp.com/cool\_bg\_image/arc4.png)  | 摸瓜V2引擎  |
| https://resource.tuniaokj.com/images/cool\_bg\_image/1.png)  | 摸瓜V2引擎  |
| https://resource.tuniaokj.com/images/cool\_bg\_image/2.png)  | 摸瓜V2引擎  |
| https://resource.tuniaokj.com/images/cool\_bg\_image/3.png)  | 摸瓜V2引擎  |
| https://resource.tuniaokj.com/images/cool\_bg\_image/4.png)  | 摸瓜V2引擎  |
| https://resource.tuniaokj.com/images/cool\_bg\_image/5.png)  | 摸瓜V2引擎  |
| https://resource.tuniaokj.com/images/cool\_bg\_image/6.png)  | 摸瓜V2引擎  |
| https://ask.dcloud.net.cn/protocol.html  | 摸瓜V2引擎  |
| https://weexapp.com/zh/  | 摸瓜V2引擎  |
| https://www.fresco-cn.org/  | 摸瓜V2引擎  |
| http://bumptech.github.io/glide/  | 摸瓜V2引擎  |
| https://github.com/alibaba/fastjson  | 摸瓜V2引擎  |
| https://github.com/koral--/android-gif-drawable  | 摸瓜V2引擎  |
| http://www.msa-alliance.cn/col.jsp?id=122  | 摸瓜V2引擎  |
| http://docs.getui.com/privacy  | 摸瓜V2引擎  |
| https://developer.huawei.com/consumer/cn/doc/HMSCore-Guides/sdk-data-security-0000001050042177  | 摸瓜V2引擎  |
| http://static.meizu.com/resources/term/privacy8.html  | 摸瓜V2引擎  |
| https://open.oppomobile.com/new/developmentDoc/info?id=10288  | 摸瓜V2引擎  |
| https://dev.vivo.com.cn/documentCenter/doc/652  | 摸瓜V2引擎  |
| https://dev.mi.com/distribute/doc/details?pId=1534  | 摸瓜V2引擎  |
| https://weixin.qq.com/cgi-bin/readtemplate?lang=zh\_CN&t=weixin\_agreement&s=privacy  | 摸瓜V2引擎  |
| https://weibo.com/signup/v5/privacy?spm=a1zaa.8161610.0.0.4f8776217Wu8R1  | 摸瓜V2引擎  |
| https://wiki.connect.qq.com/qq%e4%ba%92%e8%81%94sdk%e9%9a%90%e7%a7%81%e4%bf%9d%e6%8a%a4%e5%a3%b0%e6%98%8e  | 摸瓜V2引擎  |
| https://render.alipay.com/p/c/k2cx0tg8  | 摸瓜V2引擎  |
| https://lbs.amap.com/pages/privacy/  | 摸瓜V2引擎  |
| https://map.baidu.com/zt/client/privacy/index.html  | 摸瓜V2引擎  |
| https://doc.dcloud.net.cn/markdown-share-docs/1d821cdd3cdf2681045ec4be94bc8404/  | 摸瓜V2引擎  |
| https://yun.tuia.cn/tuia/sdk/agreement/index.html  | 摸瓜V2引擎  |
| https://www.kuaishou.com/about/policy  | 摸瓜V2引擎  |
| https://u.kuaishou.com/home/detail/1220  | 摸瓜V2引擎  |
| https://e.qq.com/dev/help\_detail.html?cid=2005&pid=5983  | 摸瓜V2引擎  |
| https://www.pangle.cn/privacy/partner  | 摸瓜V2引擎  |
| https://doc.sigmob.com/  | 摸瓜V2引擎  |
| https://union.baidu.com/bqt/  | 摸瓜V2引擎  |
| https://developer.huawei.com/consumer/cn/doc/HMSCore-Guides/whale-hong-kinetic-energy-sdk-privacy-statement-0000001658283582  | 摸瓜V2引擎  |
| https://developer.huawei.com/consumer/cn/doc/development/HMSCore-Guides/publisher-service-personal-data-0000001050066921  | 摸瓜V2引擎  |
| https://x5.tencent.com/docs/privacy.html  | 摸瓜V2引擎  |
| https://docs.getui.com/privacy/  | 摸瓜V2引擎  |
| https://wap.cmpassport.com/resources/html/contract.html  | 摸瓜V2引擎  |
| https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true  | 摸瓜V2引擎  |
| https://tnuiimage.tnkjapp.com/cool\_bg\_image/icon\_bg.png)  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_2843597\_kx4g4k3cyrh.woff2?t=1633846789896)  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_2843597\_kx4g4k3cyrh.woff?t=1633846789896)  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_2843597\_kx4g4k3cyrh.ttf?t=1633846789896)  | 摸瓜V2引擎  |
| https://img0.baidu.com/it/u=1010312865,580100376&fm=253&fmt=auto&app=120&f=JPEG?w=242&h=262  | 摸瓜V2引擎  |
| https://service.dcloud.net.cn/uniapp/feedback.html  | 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://quilljs.com/  | 摸瓜V2引擎  |
| https://connect.microsoft.com/IE/feedback/details/780874/node-contains-is-incorrect  | 摸瓜V2引擎  |
| http://code.google.com/p/google-diff-match-patch/  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://neil.fraser.name/news/2007/10/09/  | 摸瓜V2引擎  |
| https://quilljs.com/  | 摸瓜V2引擎  |
| https://connect.microsoft.com/IE/feedback/details/780874/node-contains-is-incorrect  | 摸瓜V2引擎  |
| http://code.google.com/p/google-diff-match-patch/  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://neil.fraser.name/news/2007/10/09/  | 摸瓜V2引擎  |
| https://quilljs.com  | 摸瓜V2引擎  |
| https://quilljs.com/  | 摸瓜V2引擎  |
| https://quilljs.com  | 摸瓜V2引擎  |
| https://quilljs.com/\n  | 摸瓜V2引擎  |
| https://connect.microsoft.com/IE/feedback/details/780874/node-contains-is-incorrect\n  | 摸瓜V2引擎  |
| http://code.google.com/p/google-diff-match-patch/\n  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0\n  | 摸瓜V2引擎  |
| http://neil.fraser.name/news/2007/10/09/\n  | 摸瓜V2引擎  |
| https://quilljs.com\  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2827  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2833  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2880  | 摸瓜V2引擎  |
| https://highlightjs.org/  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/1086  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2277  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/3149  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2140  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/wiki/security  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2277  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/wiki/security  | 摸瓜V2引擎  |
| https://highlightjs.org/  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2827  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2833  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2880  | 摸瓜V2引擎  |
| https://highlightjs.org/  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/1086  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2277  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/3149  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2140  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/wiki/security  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2277  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/wiki/security  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2827  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2833  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2880  | 摸瓜V2引擎  |
| https://highlightjs.org/  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/1086  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2277  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/3149  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2140  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/wiki/security  | 摸瓜V2引擎  |
| http://stackoverflow.com/a/8460753  | 摸瓜V2引擎  |
| https://tex.stackexchange.com/questions/22350/difference-between-textrm-and-mathrm  | 摸瓜V2引擎  |
| https://en.wikibooks.org/wiki/LaTeX/Lengths  | 摸瓜V2引擎  |
| https://tex.stackexchange.com/a/8263  | 摸瓜V2引擎  |
| https://tex.stackexchange.com/a/41371  | 摸瓜V2引擎  |
| https://github.com/KaTeX/KaTeX/pull/2460.  | 摸瓜V2引擎  |
| https://github.com/facebook/flow/issues/4582  | 摸瓜V2引擎  |
| https://github.com/facebook/flow/issues/5688  | 摸瓜V2引擎  |
| https://github.com/KaTeX/KaTeX/wiki/Examining-TeX  | 摸瓜V2引擎  |
| https://www.unicode.org/charts/PDF/U1D400.pdf  | 摸瓜V2引擎  |
| https://github.com/facebook/flow/issues/3663.  | 摸瓜V2引擎  |
| http://scripts.sil.org/OFL  | 摸瓜V2引擎  |
| https://developer.mozilla.org/en-US/docs/Web/MathML/Element/mo  | 摸瓜V2引擎  |
| https://www.tug.org/TUGboat/tb09-3/tb22bechtolsheim.pdf  | 摸瓜V2引擎  |
| https://www.math.lsu.edu/  | 摸瓜V2引擎  |
| https://www.w3schools.com/charsets/ref\_html\_entities\_a.asp  | 摸瓜V2引擎  |
| http://mirrors.concertpass.com/tex-archive/macros/latex/required/amsmath/amsmath.pdf  | 摸瓜V2引擎  |
| https://en.wikipedia.org/wiki/Help:Displaying\_a\_formula  | 摸瓜V2引擎  |
| https://ctan.math.illinois.edu/macros/latex/contrib/statmath/statmath.pdf  | 摸瓜V2引擎  |
| http://ctan.math.washington.edu/tex-archive/macros/latex/contrib/braket/braket.pdf  | 摸瓜V2引擎  |
| https://github.com/facebook/flow/issues/4808  | 摸瓜V2引擎  |
| https://tex.stackexchange.com/questions/1930/when-should-one-  | 摸瓜V2引擎  |
| https://gist.github.com/lambdahands/d19e0da96285b749f0ef  | 摸瓜V2引擎  |
| https://facebook.github.io/jest/docs/en/webpack.html  | 摸瓜V2引擎  |
| https://github.com/Khan/perseus/blob/master/src/perseus-markdown.jsx  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.wuruijin.cn/wuui  | 摸瓜V2引擎  |
| https://github.com/wuruijin1996/wuui  | 摸瓜V2引擎  |
| https://fengyuanchen.github.io/cropperjs  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| 707598066@qq.com  | 摸瓜V2引擎  |
| hello@joshgoebel.com e.rogov@postgrespro.ru me@allejo.io maniac@softwaremaniacs.org sourdrums@gmail.com efimovov@gmail.com gidi@gidi.io git@idleberg.com xuanji@gmail.com marcos@marcosc.com sang.dang@polku.io  | 摸瓜V2引擎  |
| 840399345@qq.com wuruijin1996@163.com  | 摸瓜V2引擎  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=CN, ST=, L=, O=Android, OU=Android, CN=tNuDmU5zoX1BfU2irccwVF6dUebQsRk67EbE5%2Bddrl1EjRYH2GPgnQ4u00MwH737 签名算法: rsassa\_pkcs1v15 有效期自: 2024-02-11 08:11:06+00:00 有效期至: 2124-01-18 08:11:06+00:00 发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=tNuDmU5zoX1BfU2irccwVF6dUebQsRk67EbE5%2Bddrl1EjRYH2GPgnQ4u00MwH737 序列号: 0x312d6f1e 哈希算法: sha256 md5值: a616ec6a6c8eabbb6574a564ced0bf29 sha1值: 1a1c051ebcd9c9220f257802d341a94c6f38cbe0 sha256值: d2b3d69cb36db19c9b06cf002f558e3ced769392a01eb589bbd28f6f081a8ba9 sha512值: 01bbe73dab2ab9f1095a99ab8c007e500b0277ce2ba2dddf2db2b32142c6154c103ec9c54215468e6a7f8f2b5d8a5532f72219d75ccfd015bc46717eeb1b27a8 公钥算法: rsa 密钥长度: 2048 指纹: 8c42d368305ff0b2d47feaf4169dfcd9460bd0cb657fafd113bfeeca7356852f**

## **6. 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\_oauth\_univerify\_plugin\_description" : "onekey login"  |
| "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"  |
| "umcsdk\_oauth\_version\_name" : "v1.4.1"  |
| "dcloud\_common\_user\_refuse\_api" : "用户拒绝该API访问"  |
| "dcloud\_feature\_oauth\_univerify\_plugin\_description" : "一键登录"  |
| "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"  |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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.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.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 |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| uni.UNI895DA06.permission.GYRECEIVER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.MODIFY\_PHONE\_STATE | 系统需要 | 修改电话状态 | 允许应用程序控制设备的电话功能。具有此权限的应用程序可以切换网络,打开和关闭电话收音机等,而无需通知您 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent102098140://,  |

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**