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

**洋葱学园教师版（ 2.13.0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 | 洋葱学园教师版 |
| 版本 | 2.13.0 |
| 包名 | com.yangcong345.teacher |
| 域名线索 | 138条 |
| URL线索 | 112条 |
| APP图标 |  |
| 分析日期 | 2025年7月1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 | 洋葱学园教师版.apk |
| 文件大小 | 65.8MB |
| MD5值 | 749c8231b3d0eed314a5562abe595107 |
| SHA1值 | 7ccd5f0d2b41c8e724f626b4a71ed911b3e16696 |
| SHA256值 | 31658d0e55ffa5b4aed68c2f1ab447c255a0d049fd6daa7b3e7e3dcfcaccc643 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 洋葱学园教师版 |
| 包名 | com.yangcong345.teacher |
| 主活动Activity | com.yangcong345.teacher.feature.splash.SplashActivity |
| 安卓版本名称 | 2.13.0 |
| 安卓版本 | 2130 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| alogsus.umeng.com | IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| www.95516.com | IP: 123.125.46.38 所属国家: China 地区: Beijing 城市: Beijing  |
| xmlpull.org | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| www.c | 没有服务器地理信息.  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| www.math.lsu.edu | IP: 130.39.247.205 所属国家: United States of America 地区: Louisiana 城市: Baton Rouge  |
| search.maven.org | IP: 34.197.231.96 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| open.weibo.cn | IP: 123.125.107.13 所属国家: China 地区: Beijing 城市: Beijing  |
| www.text-decoration | 没有服务器地理信息.  |
| wappaygw.alipay.com | IP: 116.142.245.206 所属国家: China 地区: Beijing 城市: Beijing  |
| api-push.meizu.com | IP: 221.5.93.66 所属国家: China 地区: Guangdong 城市: Foshan  |
| www.interpretation | 没有服务器地理信息.  |
| www.css | 没有服务器地理信息.  |
| www.huawei.com | IP: 120.52.95.238 所属国家: China 地区: Hebei 城市: Langfang  |
| tex.stackexchange.com | IP: 172.64.144.30 所属国家: United States of America 地区: California 城市: San Francisco  |
| plbslog.umeng.com | IP: 36.156.202.78 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| imgcache.qq.com | IP: 119.188.44.140 所属国家: China 地区: Shandong 城市: Jinan  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| grs.dbankcloud.cn | IP: 124.70.116.153 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| .css | 没有服务器地理信息.  |
| en.wikibooks.org | IP: 199.59.148.96 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.oracle.com | IP: 23.219.69.212 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| xml.org | IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| metrics1-drcn.dt.dbankcloud.cn | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| 10.38.162.35 | IP: 10.38.162.35 所属国家: - 地区: - 城市: -  |
| img.sobot.com | IP: 116.140.34.223 所属国家: China 地区: Liaoning 城市: Shenyang  |
| www.dbunit.org | IP: 74.220.199.51 所属国家: United States of America 地区: Utah 城市: Provo  |
| stage.yangcong345.com | IP: 180.184.65.79 所属国家: China 地区: Beijing 城市: Beijing  |
| loggw-exsdk.alipay.com | IP: 110.76.6.68 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.unicode.org | IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas  |
| 7to12-test.yangcong345.com | IP: 180.184.76.239 所属国家: China 地区: Beijing 城市: Beijing  |
| en.wikipedia.org | IP: 31.13.73.9 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| projectlombok.org | IP: 104.21.64.1 所属国家: United States of America 地区: California 城市: San Francisco  |
| stackoverflow.com | IP: 104.18.32.7 所属国家: United States of America 地区: California 城市: San Francisco  |
| api-push.in.meizu.com | IP: 206.161.233.191 所属国家: United States of America 地区: Virginia 城市: Herndon  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| purl.org | IP: 207.241.225.157 所属国家: United States of America 地区: California 城市: San Francisco  |
| long.open.weixin.qq.com | IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai  |
| cfg.imtt.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.style | IP: 75.2.38.108 所属国家: United States of America 地区: Washington 城市: Seattle  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| debugtbs.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| log.tbs.qq.com | IP: 124.95.231.218 所属国家: China 地区: Liaoning 城市: Shenyang  |
| tbs.imtt.qq.com | IP: 36.248.43.57 所属国家: China 地区: Fujian 城市: Fuzhou  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.tug.org | IP: 46.4.94.215 所属国家: Germany 地区: Bayern 城市: Gunzenhausen  |
| mdc.html5.qq.com | IP: 116.130.223.178 所属国家: China 地区: Beijing 城市: Beijing  |
| mobile.unionpay.com | 没有服务器地理信息.  |
| mclient.alipay.com | IP: 116.142.235.204 所属国家: China 地区: Beijing 城市: Beijing  |
| appsupport.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| open.weixin.qq.com | IP: 116.128.171.214 所属国家: China 地区: Shanghai 城市: Shanghai  |
| store.hispace.hicloud.com | IP: 123.249.62.130 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| www.sec.co.kr | IP: 112.106.187.200 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul  |
| schemas.android.com | 没有服务器地理信息.  |
| ctan.math.washington.edu | IP: 128.95.224.254 所属国家: United States of America 地区: Washington 城市: Seattle  |
| store2.hispace.hicloud.com | IP: 18.155.68.98 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| astat.bugly.cros.wr.pvp.net | IP: 170.106.118.26 所属国家: United States of America 地区: California 城市: San Francisco  |
| mobilegw.alipay.com | IP: 203.209.243.98 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| ccs.umeng.com | IP: 36.143.252.41 所属国家: China 地区: Beijing 城市: Beijing  |
| gist.github.com | IP: 243.185.187.39 所属国家: - 地区: - 城市: -  |
| www.slf4j.org | IP: 195.15.222.169 所属国家: Switzerland 地区: Geneve 城市: Carouge  |
| store-at-dre.hispace.dbankcloud.com | 没有服务器地理信息.  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| 7to12.yangcong345.com | IP: 180.184.75.103 所属国家: China 地区: Beijing 城市: Beijing  |
| api.weibo.com | IP: 116.133.8.18 所属国家: China 地区: Beijing 城市: Beijing  |
| utoken.umeng.com | IP: 223.109.148.139 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| mcgw.alipay.com | IP: 116.142.245.206 所属国家: China 地区: Beijing 城市: Beijing  |
| mirrors.concertpass.com | IP: 162.219.248.112 所属国家: United States of America 地区: California 城市: Chatsworth  |
| pms.mb.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |
| developer.umeng.com | IP: 59.82.31.210 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| grs.dbankcloud.asia | IP: 49.4.35.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| cgi.qplus.com | 没有服务器地理信息.  |
| api.sobot.com | IP: 203.107.41.32 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| data-drcn.push.dbankcloud.com | IP: 118.194.33.160 所属国家: China 地区: Shanghai 城市: Shanghai  |
| openmobile.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| pslog.umeng.com | IP: 59.82.29.162 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| alogus.umeng.com | IP: 223.109.148.177 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| www.years | 没有服务器地理信息.  |
| www.a | 没有服务器地理信息.  |
| debugx5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.umeng.com | IP: 59.82.29.249 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| ctan.math.illinois.edu | IP: 192.17.3.223 所属国家: United States of America 地区: Illinois 城市: Urbana  |
| cn.register.xmpush.xiaomi.com | IP: 221.194.179.52 所属国家: China 地区: Hebei 城市: Langfang  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.com | IP: 60.28.200.159 所属国家: China 地区: Tianjin 城市: Tianjin  |
| store3.hispace.hicloud.com | IP: 23.210.26.177 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| schemas.xmlsoap.org | IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| log.umsns.com | IP: 59.82.31.210 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.recent | 没有服务器地理信息.  |
| x.y | 没有服务器地理信息.  |
| resolver.msg.xiaomi.net | IP: 110.43.0.169 所属国家: China 地区: Beijing 城市: Beijing  |
| pre-c.umsns.com | IP: 203.119.252.86 所属国家: China 地区: Beijing 城市: Beijing  |
| store1.hispace.hicloud.com | IP: 49.4.47.241 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| h.trace.qq.com | IP: 113.56.189.246 所属国家: China 地区: Hubei 城市: Huangshi  |
| ai.login.umeng.com | IP: 59.82.31.154 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| astat.bugly.qcloud.com | IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| sss.umeng.com | IP: 59.82.31.160 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| metrics2.data.hicloud.com | IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| store-drru.hispace.hicloud.com | IP: 159.138.201.153 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| mobilegw.alipaydev.com | IP: 110.75.132.131 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.4thline.org | IP: 51.15.52.165 所属国家: Netherlands 地区: Noord-Holland 城市: Haarlem  |
| mobile.umeng.com | IP: 59.82.31.92 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| norma-external-collect.meizu.com | 没有服务器地理信息.  |
| www.lia | 没有服务器地理信息.  |
| fp.yangcong345.com | IP: 218.68.136.41 所属国家: China 地区: Tianjin 城市: Tianjin  |
| .jpg | 没有服务器地理信息.  |
| mobilegwpre.alipay.com | IP: 110.75.138.35 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| groups.google.com | IP: 199.16.158.9 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.icon | 没有服务器地理信息.  |
| ulogs.umeng.com | IP: 223.109.148.177 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| yangcong345.com | IP: 180.184.75.103 所属国家: China 地区: Beijing 城市: Beijing  |
| www.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.wencodeuricomponent | 没有服务器地理信息.  |
| scripts.sil.org | IP: 104.22.10.254 所属国家: United States of America 地区: California 城市: San Francisco  |
| 7to12-stage.yangcong345.com | IP: 180.184.65.79 所属国家: China 地区: Beijing 城市: Beijing  |
| oauth2.umeng.com | IP: 59.82.31.210 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.language | 没有服务器地理信息.  |
| api.weixin.qq.com | IP: 116.128.170.42 所属国家: China 地区: Shanghai 城市: Shanghai  |
| www.world | IP: 99.83.155.228 所属国家: United States of America 地区: Washington 城市: Seattle  |
| ulogs.umengcloud.com | IP: 223.109.148.130 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| h5.m.taobao.com | IP: 125.38.11.98 所属国家: China 地区: Tianjin 城市: Tianjin  |
| graph.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| facebook.github.io | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| www.w3schools.com | IP: 23.220.70.38 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| c.umsns.com | IP: 59.82.29.163 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| android.bugly.qq.com | IP: 124.95.225.146 所属国家: China 地区: Liaoning 城市: Shenyang  |
| render.alipay.com | IP: 124.165.219.238 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| cgi.connect.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| javax.xml.xmlconstants | 没有服务器地理信息.  |
| www.hortcut | 没有服务器地理信息.  |
| service.weibo.com | IP: 123.125.107.13 所属国家: China 地区: Beijing 城市: Beijing  |
| test.yangcong345.com | IP: 180.184.76.239 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| 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  |
| https://mobilegw.alipay.com/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| https://mobilegwpre.alipay.com/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| http://javax.xml.XMLConstants/feature/secure-processing  | com/fasterxml/jackson/databind/ext/DOMDeserializer.java  |
| http://apache.org/xml/features/disallow-doctype-decl  | com/fasterxml/jackson/databind/ext/DOMDeserializer.java  |
| http://apache.org/xml/features/nonvalidating/load-external-dtd  | com/fasterxml/jackson/databind/ext/DOMDeserializer.java  |
| http://schemas.android.com/apk/res/android  | com/huawei/appmarket/component/buoycircle/impl/view/GifImageView.java  |
| https://www.huawei.com/auth/drive.appdata  | com/huawei/hms/jos/games/GameScopes.java  |
| https://www.huawei.com/game/services.lite  | com/huawei/hms/jos/games/GameScopes.java  |
| https://www.huawei.com/auth/jos/checkmobile  | com/huawei/hms/jos/games/GameScopes.java  |
| https://www.huawei.com/auth/account/nonincludegranted  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/base.profile/accesstoken  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/carrierid  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/base.profile/serviceauthcode  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/base.profile  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/country  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/games  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/shipping.address  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/age.range  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/assisttoken  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/homezone  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/age.groupflag  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/mobile.flag  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/mobile.number  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/realname.anonymous  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://api-push.meizu.com/garcia/api/server/getPublicKey  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.meizu.com/garcia/api/server/getPushConf  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.in.meizu.com  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.meizu.com  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://norma-external-collect.meizu.com/android/exchange/getpublickey.do  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://norma-external-collect.meizu.com/push/android/external/add.do  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://service.weibo.com/share/mobilesdk\_uppic.php  | com/sina/weibo/sdk/a/d.java  |
| https://api.weibo.com/oauth2/access\_token  | com/sina/weibo/sdk/a/e.java  |
| https://service.weibo.com/share/mobilesdk.php  | com/sina/weibo/sdk/web/WebActivity.java  |
| https://open.weibo.cn/oauth2/authorize?  | com/sina/weibo/sdk/web/WebActivity.java  |
| https://service.weibo.com/share/mobilesdk.php  | com/sina/weibo/sdk/web/b/d.java  |
| https://open.weibo.cn/oauth2/authorize?  | com/sina/weibo/sdk/auth/a.java  |
| https://api.sobot.com/  | com/sobot/chat/api/apiUtils/SobotBaseUrl.java  |
| https://img.sobot.com/console/common/face/user.png  | com/sobot/chat/utils/ChatUtils.java  |
| https://h.trace.qq.com/kv  | com/tencent/bugly/proguard/ad.java  |
| https://astat.bugly.qcloud.com/rqd/async  | com/tencent/bugly/proguard/ac.java  |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async  | com/tencent/bugly/proguard/ac.java  |
| https://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| https://openmobile.qq.com/oauth2.0/me  | com/tencent/connect/UnionInfo.java  |
| https://cgi.qplus.com/report/report  | com/tencent/connect/avatar/ImageActivity.java  |
| https://openmobile.qq.com/oauth2.0/m\_jump\_by\_version?  | com/tencent/connect/common/BaseApi.java  |
| https://imgcache.qq.com/ptlogin/static/qzsjump.html?  | com/tencent/connect/common/BaseApi.java  |
| https://imgcache.qq.com/ptlogin/static/qzsjump.html?  | com/tencent/connect/auth/a.java  |
| https://openmobile.qq.com/oauth2.0/m\_authorize?  | com/tencent/connect/auth/AuthAgent.java  |
| https://openmobile.qq.com/v3/user/get\_info  | com/tencent/connect/auth/AuthAgent.java  |
| https://appsupport.qq.com/cgi-bin/qzapps/mapp\_addapp.cgi  | com/tencent/connect/auth/AuthAgent.java  |
| https://openmobile.qq.com/user/user\_login\_statis  | com/tencent/connect/auth/AuthAgent.java  |
| https://imgcache.qq.com/open/mobile/invite/sdk\_invite.html?  | com/tencent/open/SocialApiIml.java  |
| https://imgcache.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html?  | com/tencent/open/SocialApiIml.java  |
| https://imgcache.qq.com  | com/tencent/open/SocialApiIml.java  |
| https://imgcache.qq.com/open/mobile/request/sdk\_request.html?  | com/tencent/open/SocialApiIml.java  |
| https://openmobile.qq.com/cgi-bin/qunopensdk/check\_group  | com/tencent/open/SocialOperation.java  |
| https://openmobile.qq.com/cgi-bin/qunopensdk/unbind  | com/tencent/open/SocialOperation.java  |
| https://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf  | com/tencent/open/utils/i.java  |
| https://openmobile.qq.com/  | com/tencent/open/utils/HttpUtils.java  |
| https://appsupport.qq.com/cgi-bin/appstage/mstats\_batch\_report  | com/tencent/open/b/h.java  |
| https://h.trace.qq.com/kv  | com/tencent/open/b/b.java  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/c.java  |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s  | com/tencent/mm/opensdk/diffdev/a/b.java  |
| https://debugtbs.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| https://debugx5.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| https://debugtbs.qq.com?10000\  | com/tencent/smtt/sdk/WebView.java  |
| https://pms.mb.qq.com/rsp204  | com/tencent/smtt/sdk/k.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079  | com/tencent/smtt/sdk/stat/MttLoader.java  |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u=  | com/tencent/smtt/sdk/stat/MttLoader.java  |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k=  | com/tencent/smtt/utils/o.java  |
| https://log.tbs.qq.com/ajax?c=pu&tk=  | com/tencent/smtt/utils/o.java  |
| https://log.tbs.qq.com/ajax?c=dl&k=  | com/tencent/smtt/utils/o.java  |
| https://cfg.imtt.qq.com/tbs?v=2&mk=  | com/tencent/smtt/utils/o.java  |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k=  | com/tencent/smtt/utils/o.java  |
| https://tbs.imtt.qq.com/plugin/DebugPlugin\_v2.tbs  | com/tencent/smtt/utils/d.java  |
| https://c.umsns.com/ulink/getRTC  | com/umeng/socialize/tracker/a.java  |
| https://pre-c.umsns.com/ulink/getRTC  | com/umeng/socialize/tracker/a.java  |
| https://api.weibo.com/oauth2/revokeoauth2  | com/umeng/socialize/net/DeleteRequest.java  |
| https://api.weibo.com/2/users/show.json  | com/umeng/socialize/net/UserinfoRequest.java  |
| https://mobile.umeng.com/images/pic/home/social/img-1.png  | com/umeng/socialize/net/LinkcardRequest.java  |
| https://log.umsns.com/  | com/umeng/socialize/net/base/SocializeRequest.java  |
| https://ai.login.umeng.com/api/umed/event  | com/umeng/socialize/net/analytics/SocialAnalytics.java  |
| https://log.umsns.com/  | com/umeng/socialize/common/SocializeConstants.java  |
| https://log.umsns.com/link/qq/download/  | com/umeng/socialize/common/SocializeConstants.java  |
| https://log.umsns.com/link/weixin/download/  | com/umeng/socialize/common/SocializeConstants.java  |
| http://www.umeng.com/social  | com/umeng/socialize/common/SocializeConstants.java  |
| https://api.weixin.qq.com/sns/userinfo?access\_token=  | com/umeng/socialize/handler/UMWXHandler.java  |
| https://api.weixin.qq.com/sns/oauth2/access\_token?  | com/umeng/socialize/handler/UMWXHandler.java  |
| https://oauth2.umeng.com/oauth/token/acquire?  | com/umeng/socialize/handler/UMWXHandler.java  |
| https://api.weixin.qq.com/sns/oauth2/refresh\_token?appid=  | com/umeng/socialize/handler/UMWXHandler.java  |
| http://log.umsns.com/link/weixin/download/  | com/umeng/socialize/handler/UMWXHandler.java  |
| http://log.umsns.com/link/qq/download/  | com/umeng/socialize/handler/QZoneSsoHandler.java  |
| https://graph.qq.com/oauth2.0/me?access\_token=  | com/umeng/socialize/handler/UMQQSsoHandler.java  |
| https://api.weibo.com/2/users/show.json  | com/umeng/socialize/handler/SinaSsoHandler.java  |
| https://developer.umeng.com/docs/66632/detail/  | com/umeng/socialize/utils/UrlUtil.java  |
| https://ccs.umeng.com/sa  | com/umeng/socialize/a/a.java  |
| https://sss.umeng.com/api/v2/al  | com/umeng/socialize/a/a.java  |
| https://log.umsns.com/  | com/umeng/socialize/view/OauthDialog.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogsus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://ulogs.umengcloud.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://developer.umeng.com/docs/66632/detail/  | com/umeng/commonsdk/debug/UMLogUtils.java  |
| https://developer.umeng.com/docs/119267/detail/182050  | com/umeng/commonsdk/debug/UMLogCommon.java  |
| https://pslog.umeng.com  | com/umeng/commonsdk/vchannel/a.java  |
| https://pslog.umeng.com/  | com/umeng/commonsdk/vchannel/a.java  |
| https://plbslog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/j.java  |
| https://utoken.umeng.com/api/postZdata/v4  | com/umeng/umzid/ZIDManager.java  |
| https://utoken.umeng.com/api/updateZdata/v4  | com/umeng/umzid/ZIDManager.java  |
| https://mobile.unionpay.com/getclient?platform=android&type=securepayplugin\  | com/unionpay/UPPayAssistEx.java  |
| https://mobile.unionpay.com/getclient?platform=android&type=securepayplugin\  | com/unionpay/mobile/android/utils/c.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gv.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/hn.java  |
| https://%1$s/gslb/?ver=5.0  | com/xiaomi/push/dc.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/ho.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gj.java  |
| http://10.38.162.35:9085  | com/xiaomi/push/service/w.java  |
| https://cn.register.xmpush.xiaomi.com  | com/xiaomi/push/service/w.java  |
| https://resolver.msg.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/bx.java  |
| https://github.com/flutter/flutter/issues/2897).It  | io/flutter/plugin/platform/PlatformViewsController.java  |
| https://github.com/flutter/flutter/wiki/Upgrading-pre-1.12-Android-projects  | io/flutter/view/FlutterView.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Completable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Single.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Maybe.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Observable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Flowable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/rxjava3/exceptions/UndeliverableException.java  |
| https://projectlombok.org/LICENSE  | lombok/core/Main.java  |
| http://x.y/a/  | lombok/core/configuration/ConfigurationFile.java  |
| https://projectlombok.org/not/calculated  | lombok/javac/JavacAST.java  |
| https://projectlombok.org/features/experimental/FieldNameConstants  | lombok/javac/handlers/HandleFieldNameConstants.java  |
| https://projectlombok.org/not/calculated  | lombok/eclipse/EclipseAST.java  |
| https://projectlombok.org  | lombok/eclipse/agent/PatchFixesShadowLoaded.java  |
| https://projectlombok.org/  | lombok/eclipse/agent/PatchFixesShadowLoaded.java  |
| https://projectlombok.org/features/experimental/FieldNameConstants  | lombok/eclipse/handlers/HandleFieldNameConstants.java  |
| https://projectlombok.org  | lombok/installer/Installer.java  |
| http://groups.google.com/group/project-lombok  | lombok/installer/eclipse/EclipseProductLocation.java  |
| http://dictionaryperceptionrevolutionfoundationpx;height:successfulsupportersmillenniumhis  | org/brotli/dec/Dictionary.java  |
| http://mathematicsmargin-top:eventually  | org/brotli/dec/Dictionary.java  |
| http://Descriptionrelatively  | org/brotli/dec/Dictionary.java  |
| http://applicationslink\  | org/brotli/dec/Dictionary.java  |
| http://navigation\  | org/brotli/dec/Dictionary.java  |
| http://px;  | org/brotli/dec/Dictionary.java  |
| https://www.World  | org/brotli/dec/Dictionary.java  |
| http://www.years  | org/brotli/dec/Dictionary.java  |
| http://interested  | org/brotli/dec/Dictionary.java  |
| http://familiar  | org/brotli/dec/Dictionary.java  |
| https://was  | org/brotli/dec/Dictionary.java  |
| https://aIn  | org/brotli/dec/Dictionary.java  |
| http://whether  | org/brotli/dec/Dictionary.java  |
| http://interpreted  | org/brotli/dec/Dictionary.java  |
| http://\  | org/brotli/dec/Dictionary.java  |
| http://);  | org/brotli/dec/Dictionary.java  |
| http://addEventListenerresponsible  | org/brotli/dec/Dictionary.java  |
| http://.jpg  | org/brotli/dec/Dictionary.java  |
| http://<a  | org/brotli/dec/Dictionary.java  |
| https://<div  | org/brotli/dec/Dictionary.java  |
| http://according  | org/brotli/dec/Dictionary.java  |
| http://www.interpretation  | org/brotli/dec/Dictionary.java  |
| http://s;text-align:centerfont-weight:  | org/brotli/dec/Dictionary.java  |
| http://html4/loose.dtd\  | org/brotli/dec/Dictionary.java  |
| http://style=\  | org/brotli/dec/Dictionary.java  |
| http://staticsuggested  | org/brotli/dec/Dictionary.java  |
| http://www.a  | org/brotli/dec/Dictionary.java  |
| http://An  | org/brotli/dec/Dictionary.java  |
| https://www.recent  | org/brotli/dec/Dictionary.java  |
| http://In  | org/brotli/dec/Dictionary.java  |
| http://www./div></div><div  | org/brotli/dec/Dictionary.java  |
| http://cript\  | org/brotli/dec/Dictionary.java  |
| http://\n<script  | org/brotli/dec/Dictionary.java  |
| http://www.wencodeURIComponent(\  | org/brotli/dec/Dictionary.java  |
| http://encoding=\  | org/brotli/dec/Dictionary.java  |
| http://www.icon\  | org/brotli/dec/Dictionary.java  |
| http://imEnglish  | org/brotli/dec/Dictionary.java  |
| http://i  | org/brotli/dec/Dictionary.java  |
| http://www.<li><a  | org/brotli/dec/Dictionary.java  |
| http://site\_name\  | org/brotli/dec/Dictionary.java  |
| http://www.hortcut  | org/brotli/dec/Dictionary.java  |
| http://</a></li><li  | org/brotli/dec/Dictionary.java  |
| http://<div  | org/brotli/dec/Dictionary.java  |
| http://iparticipation  | org/brotli/dec/Dictionary.java  |
| http://www.\  | org/brotli/dec/Dictionary.java  |
| http://xt/css\  | org/brotli/dec/Dictionary.java  |
| http://link  | org/brotli/dec/Dictionary.java  |
| http://www.text-decoration:underthe  | org/brotli/dec/Dictionary.java  |
| http://option><option  | org/brotli/dec/Dictionary.java  |
| http://www</a><a  | org/brotli/dec/Dictionary.java  |
| http://w  | org/brotli/dec/Dictionary.java  |
| http://.css\  | org/brotli/dec/Dictionary.java  |
| http://www.style=\  | org/brotli/dec/Dictionary.java  |
| http://www.css\  | org/brotli/dec/Dictionary.java  |
| http://ator\  | org/brotli/dec/Dictionary.java  |
| http://www.language=\  | org/brotli/dec/Dictionary.java  |
| http://www-//W3C//DTD  | org/brotli/dec/Dictionary.java  |
| http://UA-Compatible\  | org/brotli/dec/Dictionary.java  |
| http://www.C//DTD  | org/brotli/dec/Dictionary.java  |
| http://www.  | org/brotli/dec/Dictionary.java  |
| http://www.sec.co.kr/dlna  | org/fourthline/cling/binding/xml/Descriptor.java  |
| http://schemas.xmlsoap.org/soap/envelope/  | org/fourthline/cling/model/Constants.java  |
| http://schemas.xmlsoap.org/soap/encoding/  | org/fourthline/cling/model/Constants.java  |
| http://www.4thline.org/projects/mailinglists-cling.html\n\n  | org/fourthline/cling/support/shared/Main.java  |
| http://purl.org/dc/elements/1.1/  | org/fourthline/cling/support/model/DIDLObject.java  |
| http://www.sec.co.kr/  | org/fourthline/cling/support/model/DIDLObject.java  |
| https://github.com/mockito/mockito/issues/685  | org/mockito/internal/creation/instance/ConstructorInstantiator.java  |
| https://github.com/mockito/mockito/issues/new  | org/mockito/internal/invocation/TypeSafeMatching.java  |
| http://search.maven.org/  | org/mockito/internal/util/Platform.java  |
| http://[  | org/seamless/util/URIUtil.java  |
| http://www.dbunit.org/properties/datatypeFactory  | org/seamless/util/dbunit/H2DBUnitOperations.java  |
| http://xmlpull.org/v1/doc/features.html  | org/seamless/xml/XmlPullParserUtils.java  |
| http://xml.org/sax/features/external-general-entities  | org/seamless/xml/SAXParser.java  |
| http://xml.org/sax/features/external-parameter-entities  | org/seamless/xml/SAXParser.java  |
| http://apache.org/xml/features/disallow-doctype-decl  | org/seamless/xml/SAXParser.java  |
| http://apache.org/xml/features/xinclude/fixup-base-uris  | org/seamless/xml/DOMParser.java  |
| http://apache.org/xml/features/xinclude/fixup-language  | org/seamless/xml/DOMParser.java  |
| http://apache.org/xml/features/disallow-doctype-decl  | org/seamless/xml/DOMParser.java  |
| http://xml.org/sax/features/external-general-entities  | org/seamless/xml/DOMParser.java  |
| http://xml.org/sax/features/external-parameter-entities  | org/seamless/xml/DOMParser.java  |
| http://apache.org/xml/features/nonvalidating/load-external-dtd  | org/seamless/xml/DOMParser.java  |
| http://apache.org/xml/features/validation/dynamic  | org/seamless/xml/DOMParser.java  |
| http://www.oracle.com/xml/is-standalone  | org/seamless/xml/DOMParser.java  |
| http://xml.apache.org/xslt  | org/seamless/xml/DOMParser.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/MDC.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/LoggerFactory.java  |
| https://www.95516.com/portal/open/init.do?entry=open  | 摸瓜V1引擎  |
| https://store.hispace.hicloud.com/hwmarket/api/  | 摸瓜V1引擎  |
| https://7to12.yangcong345.com  | 摸瓜V2引擎  |
| https://store-at-dre.hispace.dbankcloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://data-drcn.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dra.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dre.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-drru.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://metrics1-drcn.dt.dbankcloud.cn:443  | 摸瓜V2引擎  |
| https://metrics-dra.dt.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics2.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.dt.dbankcloud.ru:6447  | 摸瓜V2引擎  |
| https://store1.hispace.hicloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://store2.hispace.hicloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://store3.hispace.hicloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://store-drru.hispace.hicloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| https://grs.platform.dbankcloud.ru  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 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  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| https://7to12-test.yangcong345.com  | 摸瓜V2引擎  |
| https://7to12-stage.yangcong345.com  | 摸瓜V2引擎  |
| https://7to12.yangcong345.com  | 摸瓜V2引擎  |
| https://test.yangcong345.com  | 摸瓜V2引擎  |
| https://stage.yangcong345.com  | 摸瓜V2引擎  |
| https://yangcong345.com  | 摸瓜V2引擎  |
| https://fp.yangcong345.com/middle/1.0.0/network-inspection-v1.0-RC.0.html  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| x5tbs@tencent.com  | com/tencent/smtt/sdk/X5Downloader.java  |
| leaderboard\_ic\_like@1x.json  | 摸瓜V1引擎  |
| 椭圆形备份@3x.png  | 摸瓜V2引擎  |
| 渐变层@2x.png 高光@2x.png 蒙版@2x\_00001.png  | 摸瓜V2引擎  |
| 1@2x.png 2@2x.png 4@2x.png  | 摸瓜V2引擎  |
| icon\_hand@3x.png  | 摸瓜V2引擎  |
| 矩形@2x\_1.png  | 摸瓜V2引擎  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15060355040  | com/unionpay/UPPayAssistEx.java  |
| 17179869184  | lombok/javac/handlers/JavacHandlerUtil.java  |
| 17179869184  | lombok/javac/handlers/HandleDelegate.java  |
| 17179869184  | lombok/delombok/PrettyPrinter.java  |

## **5. 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=China, ST=BJ, L=BJ, O=GuangHeTV, OU=GuangHeTV, CN=kai chen 签名算法: rsassa\_pkcs1v15 有效期自: 2014-12-11 03:23:38+00:00 有效期至: 2044-12-03 03:23:38+00:00 发行人: C=China, ST=BJ, L=BJ, O=GuangHeTV, OU=GuangHeTV, CN=kai chen 序列号: 0x54890e3a 哈希算法: sha1 md5值: f25274a79f9fccdb70b83a043aae6f3c sha1值: 0fdb2ac459b2fbb9ef492542f11fe20901c19bfd sha256值: 809471cc443858556ad3d72799b88543ab173ce6cf5e83b34dbd829ed2c23375 sha512值: f09f5d764502b4f75e92a6b61816d3b511246b0d86839b9eb38cd41870f331155382c3adbb45b067d61810396713e0c85ede3b880ab3be2c2291f2d86d394043 公钥算法: rsa 密钥长度: 1024 指纹: 6de96407770cc68130ecb3ba9c56fe0e7a209b158355a68cb951c352f3e2a45f**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "account\_manage\_item\_password" : "密码管理"  |
| "err\_auth\_dented" : "认证被否决"  |
| "forget\_pwd" : "忘记密码"  |
| "input\_password" : "请输入有效的密码"  |
| "input\_username" : "请输入您的用户名"  |
| "login\_forget\_password" : "忘记密码？"  |
| "pos\_pwd\_display\_yiqianbao" : "请输入壹钱包支付密码:"  |
| "ppplugin\_dialog\_purse\_not\_get\_pwdinfo\_yiqianbao" : "壹钱包密码键盘无密文信息返回"  |
| "ppplugin\_forgetpwd\_prompt" : "忘记密码"  |
| "ppplugin\_input\_cardinfo\_cardpwd\_prompt" : "确认密码"  |
| "ppplugin\_inputpaypwd\_pos\_prompt" : "请输入6位全民付移动支付密码"  |
| "ppplugin\_inputpaypwd\_prompt" : "请输入6位支付密码"  |
| "ppplugin\_inputpwddialog\_accbalance\_prompt" : "账户余额"  |
| "ppplugin\_inputpwddialog\_coupon\_prompt" : "优惠券"  |
| "ppplugin\_microfreepwd\_amount\_prompt" : "免密金额"  |
| "ppplugin\_microfreepwd\_pay\_prompt" : "小额免密支付"  |
| "ppplugin\_microfreepwd\_prompt" : "小额免密"  |
| "ppplugin\_microfreepwd\_switchoff" : "关闭"  |
| "ppplugin\_microfreepwd\_switchon" : "已开启"  |
| "ppplugin\_microfreepwd\_use\_prompt" : "超过免密额度时，需要验证支付密码，并且系统会移除可疑交易。"  |
| "ppplugin\_modifypaypwd\_ok" : "支付密码修改成功"  |
| "ppplugin\_modifypwd\_prompt" : "修改支付密码"  |
| "ppplugin\_resetpaypwd\_ok" : "支付密码重置成功"  |
| "ppplugin\_session\_timeout\_prompt" : "由于您长时间未操作，请重新登录"  |
| "ppplugin\_set\_pwd\_prompt" : "设置密码"  |
| "security\_public\_key" : "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8hzUojzHX8jDL+97pqr7CaLiKSsZ0aOES7FUcX7vh9PoEDbCKNCTakRXdS5EiurPk3QpvsAGbfyIs7JWKm4py9KcIdJsZRh9onknVeAVlU++jnrGFGEYfQb8iKzClN059gYeeJBs9mwi7RGU9tj0KHUG659v5sMBxv7zNse3fJQIDAQAB"  |
| "session\_timeout" : "会话超时,请重新登录"  |
| "sobot\_ding\_cai\_sessionoff" : "会话结束，无法反馈"  |
| "tips\_amount\_free\_pwd" : "已为您开启200元额度小额免密，可在右上角设置"  |
| "tips\_input\_password" : "为了您的账号安全请输入支付密码"  |
| "xiao\_mi\_app\_key" : "5651817895860"  |
| "sobot\_ding\_cai\_sessionoff" : "Gespräch beendet, kein feedback"  |
| "sobot\_ding\_cai\_sessionoff" : "Percakapan berakhir, tidak ada umpan balik"  |
| "sobot\_ding\_cai\_sessionoff" : "انتهت المحادثة، لا يمكنك إرسال ملاحظاتك"  |
| "sobot\_ding\_cai\_sessionoff" : "Conversation terminée. Pas commentaire"  |
| "sobot\_ding\_cai\_sessionoff" : "Konuşma bitti,geri dönüt verilemez"  |
| "sobot\_ding\_cai\_sessionoff" : "La sesión terminó, no se puede comentar"  |
| "sobot\_ding\_cai\_sessionoff" : "Perbincangan tamat, tidak dapat maklumbalas"  |
| "sobot\_ding\_cai\_sessionoff" : "Fine della conversazione, nessun feedback"  |
| "sobot\_ding\_cai\_sessionoff" : "Fim da sessão, sem se poder dar feedback"  |
| "sobot\_ding\_cai\_sessionoff" : "會話結束，無法反饋"  |
| "sobot\_ding\_cai\_sessionoff" : "Percakapan berakhir, tidak ada umpan balik"  |
| "sobot\_ding\_cai\_sessionoff" : "Conversation ended, you can't send feedback"  |
| "sobot\_ding\_cai\_sessionoff" : "สนทนาจบลงแล้ว ไม่สามารถเสนอแนะได้"  |
| "sobot\_ding\_cai\_sessionoff" : "Wprowadź adres e-mail"  |
| "sobot\_ding\_cai\_sessionoff" : "Hội thoại kết thúc, không thể phản hồi"  |
| "sobot\_ding\_cai\_sessionoff" : "会話が終わりました。フィードバックできません"  |
| "sobot\_ding\_cai\_sessionoff" : "회화 종료, 피드백 없음"  |
| "sobot\_ding\_cai\_sessionoff" : "Разговор завершен, вы не можете отправить отзыв"  |

## **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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 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.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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.DOWNLOAD\_WITHOUT\_NOTIFICATION | 未知 | Unknown permission | Unknown permission from android reference |
| 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.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| 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.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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| com.yangcong345.teacher.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.apps.photos.permission.GOOGLE\_PHOTOS | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa.SECURITY\_ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| oplus.permission.settings.LAUNCH\_FOR\_EXPORT | 未知 | Unknown permission | Unknown permission from android reference |
| com.vivo.identifier.permission.OAID\_STATE\_DIALOG | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| 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.hihonor.android.launcher.permission.CHANGE\_BADGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.yangcong345.teacher.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.yangcong345.teacher.push.permission.MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.c2dm.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.yangcong345.teacher.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.yangcong345.teacher.permission.techain.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.yangcong345.teacher.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.yangcong345.teacher.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.push.permission.READ\_PUSH\_NOTIFICATION\_INFO | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.hwid.permission.gameservice.archive.access.provider | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.yangcong345.teacher.feature.splash.SplashActivity | **Schemes**: ycteacher://, **Hosts:** yangcong345.com,  |
| com.baidu.techain.push.VivoPushActivity | **Schemes**: vpushscheme://, **Hosts:** com.yangcong345.teacher, **Paths:** /detail,  |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent1107934310://,  |
| com.pingplusplus.android.PaymentActivity | **Schemes**: qwallet1107934310://,  |
| com.baidu.techain.push.HonorPushActivity | **Schemes**: honorps://, **Hosts:** com.yangcong345.teacher, **Paths:** /honor\_detail,  |
| com.yangcong345.pay.coupon.AlipayMiniProCallbackActivity | **Schemes**: ycunionpay://,  |

**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。**