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

**葫芦侠（ 3.5.1.89.1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 | 葫芦侠 |
| 版本 | 3.5.1.89.1 |
| 包名 | com.huluxia.gametools |
| 域名线索 | 106条 |
| URL线索 | 91条 |
| APP图标 |  |
| 分析日期 | 2025年7月9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 | 葫芦侠 - v3.5.1.89.1.apk |
| 文件大小 | 19.43MB |
| MD5值 | 8605566a63e074e10da394bf59108fbe |
| SHA1值 | ee71cbf0c033947cb44a82cd9f560d477fe3399b |
| SHA256值 | d1999e3281d5bf89e6194265852240303ced060756f7daca6d8ef7eed2602a6b |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 葫芦侠 |
| 包名 | com.huluxia.gametools |
| 主活动Activity | com.huluxia.gametools.ui.MainActivity.AppStart |
| 安卓版本名称 | 3.5.1.89.1 |
| 安卓版本 | 248 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| pan.baidu.com | IP: 110.242.69.176  所属国家: China  地区: Hebei  城市: Baoding |
| qzs.qq.com | IP: 116.148.164.9  所属国家: China  地区: Beijing  城市: Beijing |
| app.html5.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| cdn.ws.huluxia.com | IP: 116.114.190.202  所属国家: China  地区: Nei Mongol  城市: Baotou |
| bb.huluxia.com | IP: 60.28.100.28  所属国家: China  地区: Tianjin  城市: Tianjin |
| debugx5.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| www.gnu.org | IP: 209.51.188.116  所属国家: United States of America  地区: Massachusetts  城市: Somerville |
| restapi.amap.com | IP: 203.119.169.174  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| version.huluxia.com | IP: 134.175.40.11  所属国家: China  地区: Beijing  城市: Beijing |
| map.baidu.com | IP: 111.206.208.32  所属国家: China  地区: Beijing  城市: Beijing |
| cmnsguider.yunos.com | IP: 203.119.169.246  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| test.floor.huluxia.com | IP: 61.182.142.22  所属国家: China  地区: Hebei  城市: Hengshui |
| mqqad.html5.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| cdn.jcloud.huluxia.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| stat.huluxia.com.wswebpic.com | IP: 123.125.46.43  所属国家: China  地区: Beijing  城市: Beijing |
| www.json.org | IP: 74.208.236.169  所属国家: United States of America  地区: Pennsylvania  城市: Philadelphia |
| uplog.qbox.me | IP: 101.251.144.177  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| test2.bbs.huluxia.net | IP: 14.152.50.98  所属国家: China  地区: Guangdong  城市: Foshan |
| gray.floor.huluxia.com | IP: 110.242.21.78  所属国家: China  地区: Hebei  城市: Baoding |
| www.opensource.org | IP: 104.21.84.214  所属国家: United States of America  地区: California  城市: San Francisco |
| fusion.qq.com | IP: 116.130.228.157  所属国家: China  地区: Beijing  城市: Beijing |
| tools.huluxia.com.wswebcdn.com | IP: 123.126.74.16  所属国家: China  地区: Beijing  城市: Beijing |
| www.openssl.org | IP: 34.49.79.89  所属国家: United States of America  地区: California  城市: Mountain View |
| javascript.crockford.com | IP: 217.160.0.111  所属国家: Germany  地区: Nordrhein-Westfalen  城市: Strang |
| register.xmpush.xiaomi.com | IP: 221.194.179.52  所属国家: China  地区: Hebei  城市: Langfang |
| test.tools.huluxia.net | 没有服务器地理信息. |
| abroad.apilocate.amap.com | IP: 59.82.44.11  所属国家: China  地区: Shanghai  城市: Shanghai |
| cdn2.huluxia.com | IP: 39.91.174.14  所属国家: China  地区: Shandong  城市: Linyi |
| wifi.huluxia.net | IP: 112.81.148.49  所属国家: China  地区: Jiangsu  城市: Wuxi |
| st.tools.huluxia.net | IP: 112.90.227.133  所属国家: China  地区: Guangdong  城市: Shanwei |
| api.map.baidu.com | IP: 111.206.208.72  所属国家: China  地区: Beijing  城市: Beijing |
| mta.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| logs.amap.com | IP: 110.253.189.211  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| server.chat.huluxia.com | 没有服务器地理信息. |
| alog.umengcloud.com | IP: 223.109.148.179  所属国家: China  地区: Jiangsu  城市: Nanjing |
| test.search.huluxia.net | IP: 119.29.85.235  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| open.hicloud.com | 没有服务器地理信息. |
| 192.168.0.116 | IP: 192.168.0.116  所属国家: -  地区: -  城市: - |
| www.jivesoftware.com | IP: 23.235.209.143  所属国家: United States of America  地区: Virginia  城市: Virginia Beach |
| logtbs.sparta.mig.tencent-cloud.net | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| st.search.huluxia.net | IP: 119.146.201.133  所属国家: China  地区: Guangdong  城市: Shanwei |
| tools.huluxia.com | IP: 123.126.74.16  所属国家: China  地区: Beijing  城市: Beijing |
| service.bbs.huluxia.com | IP: 119.134.255.183  所属国家: China  地区: Guangdong  城市: Shanwei |
| debugtbs.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| apilocatesrc.amap.com | IP: 106.11.43.81  所属国家: China  地区: Beijing  城市: Beijing |
| cgi.connect.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| test.version.huluxia.com | IP: 14.152.50.98  所属国家: China  地区: Guangdong  城市: Foshan |
| wup.imtt.qq.com | IP: 116.130.230.62  所属国家: China  地区: Beijing  城市: Beijing |
| ns.adobe.com | 没有服务器地理信息. |
| c.isdspeed.qq.com | 没有服务器地理信息. |
| floor.huluxia.com | IP: 219.157.125.31  所属国家: China  地区: Henan  城市: Luohe |
| reg.ksyun.huluxia.com | IP: 121.17.252.9  所属国家: China  地区: Hebei  城市: Hengshui |
| my.tv.sohu.com | IP: 116.130.217.2  所属国家: China  地区: Beijing  城市: Beijing |
| search.huluxia.com | IP: 123.125.46.38  所属国家: China  地区: Beijing  城市: Beijing |
| alog.umeng.com | IP: 223.109.148.176  所属国家: China  地区: Jiangsu  城市: Nanjing |
| 10.237.14.141 | IP: 10.237.14.141  所属国家: -  地区: -  城市: - |
| mdc.html5.qq.com | IP: 125.39.196.199  所属国家: China  地区: Tianjin  城市: Tianjin |
| data.hicloud.com | IP: 118.194.33.124  所属国家: China  地区: Shanghai  城市: Shanghai |
| reg.huluxia.com | IP: 121.17.252.9  所属国家: China  地区: Hebei  城市: Hengshui |
| bb.huluxia.net | IP: 183.129.249.120  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| jquery.eisbehr.de | IP: 212.90.148.124  所属国家: Germany  地区: Rheinland-Pfalz  城市: Minden |
| lkme.cc | IP: 43.137.70.64  所属国家: China  地区: Beijing  城市: Beijing |
| www.baidu.com | IP: 110.242.68.3  所属国家: China  地区: Hebei  城市: Baoding |
| yunpan.cn | IP: 101.199.254.53  所属国家: China  地区: Beijing  城市: Beijing |
| log.tbs.qq.com | IP: 124.95.231.218  所属国家: China  地区: Liaoning  城市: Shenyang |
| openmobile.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| cdn.u2.huluxia.com | IP: 39.91.174.14  所属国家: China  地区: Shandong  城市: Linyi |
| tools.huluxia.net | IP: 110.242.21.78  所属国家: China  地区: Hebei  城市: Baoding |
| 119.29.29.29 | IP: 119.29.29.29  所属国家: Singapore  地区: Singapore  城市: Singapore |
| v.youku.com | IP: 106.11.40.57  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.huluxia.com | IP: 129.204.12.158  所属国家: China  地区: Beijing  城市: Beijing |
| server.news.huluxia.com | IP: 60.28.100.28  所属国家: China  地区: Tianjin  城市: Tianjin |
| cgicol.amap.com | IP: 110.253.189.212  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| service.tools.huluxia.net | IP: 119.134.255.184  所属国家: China  地区: Guangdong  城市: Shanwei |
| apilocate.amap.com | IP: 59.82.31.183  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| cdn.u1.huluxia.com | IP: 39.91.174.18  所属国家: China  地区: Shandong  城市: Linyi |
| lbs.amap.com | IP: 110.253.188.148  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| uop.umeng.com | 没有服务器地理信息. |
| api.g.huluxia.com | IP: 110.242.21.78  所属国家: China  地区: Hebei  城市: Baoding |
| test.bbs.huluxia.net | 没有服务器地理信息. |
| cfg.imtt.qq.com | IP: 60.28.172.238  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 |
| uc.qbox.me | IP: 153.99.246.132  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| v.qq.com | IP: 123.6.40.249  所属国家: China  地区: Henan  城市: Zhengzhou |
| version.check.huluxia.com | IP: 134.175.40.11  所属国家: China  地区: Beijing  城市: Beijing |
| tieba.baidu.com | IP: 111.206.209.41  所属国家: China  地区: Beijing  城市: Beijing |
| dl.vmall.com | 没有服务器地理信息. |
| test.server.news.huluxia.net | IP: 119.29.85.235  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| xmlpull.org | IP: 185.199.110.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| appsupport.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| goo.gl | IP: 142.250.217.110  所属国家: United States of America  地区: California  城市: Mountain View |
| 192.168.0.107 | IP: 192.168.0.107  所属国家: -  地区: -  城市: - |
| upload.huluxia.com | IP: 129.204.46.114  所属国家: China  地区: Beijing  城市: Beijing |
| wap.huluxia.com | IP: 61.182.142.22  所属国家: China  地区: Hebei  城市: Hengshui |
| pingma.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| cdn.dnion.huluxia.com | 没有服务器地理信息. |
| hlx.iweju.com | IP: 120.132.37.251  所属国家: China  地区: Beijing  城市: Beijing |
| mta.oa.com | IP: 141.144.196.217  所属国家: Netherlands  地区: Noord-Holland  城市: Amsterdam |
| resolver.msg.xiaomi.net | IP: 114.247.154.13  所属国家: China  地区: Beijing  城市: Beijing |
| stat.huluxia.com | IP: 61.182.142.22  所属国家: China  地区: Hebei  城市: Hengshui |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86  所属国家: China  地区: Shandong  城市: Qingdao |
| bbs.huluxia.com | IP: 60.28.100.28  所属国家: China  地区: Tianjin  城市: Tianjin |
| img0.bdstatic.com | IP: 123.117.132.38  所属国家: China  地区: Beijing  城市: Beijing |
| log.umsns.com | IP: 59.82.31.92  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| v.huluxia.com | IP: 183.129.249.120  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ulog.imap.baidu.com | IP: 111.206.209.119  所属国家: China  地区: Beijing  城市: Beijing |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://map.baidu.com/fwmap/upload/place/icon/ | com/baidu/mapapi/h.java |
| http://ulog.imap.baidu.com/up | com/baidu/mapapi/s.java |
| http://api.map.baidu.com/geosearch/poi | com/baidu/mapapi/cloud/GeoSearchManager.java |
| http://api.map.baidu.com/geosearch/detail | com/baidu/mapapi/cloud/GeoSearchManager.java |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/ | com/amap/api/location/AMapLocation.java |
| http://open.hicloud.com/android/push1.0.js | com/huawei/android/pushselfshow/richpush/html/HtmlViewer.java |
| http://open.hicloud.com/android/push1.0.js\ | com/huawei/android/pushselfshow/richpush/html/e.java |
| http://data.hicloud.com:8089/sdkv1 | com/hianalytics/android/a/a/a.java |
| http://stat.huluxia.com/downstat/down/begin | com/huluxia/aa.java |
| http://stat.huluxia.com/downstat/down/downcount | com/huluxia/aa.java |
| http://stat.huluxia.com/downstat/down/complete | com/huluxia/aa.java |
| http://stat.huluxia.com/downstat/install/begin | com/huluxia/aa.java |
| http://stat.huluxia.com/downstat/install/complete | com/huluxia/aa.java |
| http://stat.huluxia.com/downstat/error | com/huluxia/aa.java |
| http://stat.huluxia.com/stat/nodeerror | com/huluxia/aa.java |
| http://stat.huluxia.com/stat/gamedown | com/huluxia/aa.java |
| http://stat.huluxia.com/stat/service/event | com/huluxia/aa.java |
| http://upload.huluxia.com/upload/file | com/huluxia/f.java |
| http://cdn.u1.huluxia.com/g1/M00/CB/04/wKgBB1XgSe-AG3mhAAALwQuN1SE568.png | com/huluxia/data/game/GameCateItem.java |
| http://cdn.u1.huluxia.com/g1/M00/CB/04/wKgBB1XgSgaAaO7AAAATdzek9P8465.png | com/huluxia/data/game/GameCateItem.java |
| http://pan.baidu.com/ | com/huluxia/module/GameInfo.java |
| http://dl.vmall.com/ | com/huluxia/module/GameInfo.java |
| http://yunpan.cn/ | com/huluxia/module/GameInfo.java |
| http://v.youku.com/ | com/huluxia/module/GameInfo.java |
| http://my.tv.sohu.com/ | com/huluxia/module/GameInfo.java |
| http://v.qq.com/ | com/huluxia/module/GameInfo.java |
| http://pan.baidu.com/ | com/huluxia/module/SubscribeResourceInfo.java |
| http://dl.vmall.com/ | com/huluxia/module/SubscribeResourceInfo.java |
| http://yunpan.cn/ | com/huluxia/module/SubscribeResourceInfo.java |
| http://v.youku.com/ | com/huluxia/module/SubscribeResourceInfo.java |
| http://my.tv.sohu.com/ | com/huluxia/module/SubscribeResourceInfo.java |
| http://v.qq.com/ | com/huluxia/module/SubscribeResourceInfo.java |
| http://test.tools.huluxia.net | com/huluxia/module/c.java |
| http://service.tools.huluxia.net | com/huluxia/module/c.java |
| http://test.bbs.huluxia.net | com/huluxia/module/c.java |
| http://test2.bbs.huluxia.net | com/huluxia/module/c.java |
| http://service.bbs.huluxia.com | com/huluxia/module/c.java |
| http://test.floor.huluxia.com | com/huluxia/module/c.java |
| http://st.tools.huluxia.net | com/huluxia/module/c.java |
| http://test.server.news.huluxia.net | com/huluxia/module/c.java |
| https://gray.floor.huluxia.com | com/huluxia/module/c.java |
| https://test.bbs.huluxia.net | com/huluxia/module/c.java |
| http://www.huluxia.com | com/huluxia/module/c.java |
| http://floor.huluxia.com/friendship/follow | com/huluxia/module/c.java |
| http://reg.huluxia.com/game/downloadlimitsize.txt | com/huluxia/module/c.java |
| https://graph.qq.com/user/get\_user\_info | com/huluxia/module/c.java |
| http://server.chat.huluxia.com | com/huluxia/module/c.java |
| http://api.g.huluxia.com/get/v1 | com/huluxia/module/c.java |
| http://tools.huluxia.com | com/huluxia/module/c.java |
| http://floor.huluxia.com | com/huluxia/module/c.java |
| http://server.news.huluxia.com | com/huluxia/module/c.java |
| https://floor.huluxia.com | com/huluxia/module/c.java |
| http://upload.huluxia.com/upload/token | com/huluxia/module/c.java |
| http://upload.huluxia.com | com/huluxia/module/c.java |
| http://search.huluxia.com | com/huluxia/module/c.java |
| http://st.search.huluxia.net | com/huluxia/module/c.java |
| http://test.search.huluxia.net | com/huluxia/module/c.java |
| http://192.168.0.116 | com/huluxia/module/c.java |
| http://192.168.0.107 | com/huluxia/module/c.java |
| http://tools.huluxia.net) | com/huluxia/module/c.java |
| http://test.tools.huluxia.net) | com/huluxia/module/c.java |
| http://service.tools.huluxia.net) | com/huluxia/module/c.java |
| http://floor.huluxia.com) | com/huluxia/module/c.java |
| http://test.bbs.huluxia.net) | com/huluxia/module/c.java |
| http://test2.bbs.huluxia.net) | com/huluxia/module/c.java |
| http://service.bbs.huluxia.com) | com/huluxia/module/c.java |
| http://test.floor.huluxia.com) | com/huluxia/module/c.java |
| http://server.news.huluxia.com) | com/huluxia/module/c.java |
| http://test.server.news.huluxia.net) | com/huluxia/module/c.java |
| https://floor.huluxia.com) | com/huluxia/module/c.java |
| https://gray.floor.huluxia.com) | com/huluxia/module/c.java |
| https://test.bbs.huluxia.net) | com/huluxia/module/c.java |
| http://search.huluxia.com) | com/huluxia/module/c.java |
| http://test.search.huluxia.net) | com/huluxia/module/c.java |
| http://img0.bdstatic.com/img/image/shouye/mntsc-11681494554.jpg | com/huluxia/module/area/spec/a.java |
| http://img0.bdstatic.com/img/image/shouye/mntsc-11681494554.jpg | com/huluxia/module/area/detail/a.java |
| http://img0.bdstatic.com/img/image/shouye/mnqz-11867945883.jpg | com/huluxia/module/area/detail/a.java |
| http://stat.huluxia.com/stat/nodeerror | com/huluxia/module/home/a.java |
| http://upload.huluxia.com/upload/file | com/huluxia/module/feedback/a.java |
| http://xmlpull.org/v1/doc/features.html | com/huluxia/parallel/helper/utils/g.java |
| http://xmlpull.org/v1/doc/features.html | com/huluxia/parallel/server/pm/g.java |
| http://bb.huluxia.net/tool/help/ | com/huluxia/ui/tools/uictrl/j.java |
| http://bb.huluxia.net/idol | com/huluxia/ui/tools/uictrl/j.java |
| http://bb.huluxia.net/tool/help/ | com/huluxia/ui/tools/uictrl/i.java |
| http://bb.huluxia.net/idol | com/huluxia/ui/tools/uictrl/i.java |
| http://cdn.jcloud.huluxia.com/file/libs/video-lib-20180918.zip | com/huluxia/ui/bbs/PublishTopicActivity.java |
| http://bb.huluxia.net/h5game/ | com/huluxia/ui/home/DiscoveryLayout.java |
| http://v.huluxia.com | com/huluxia/ui/home/DiscoveryLayout.java |
| https://www.baidu.com/ | com/huluxia/ui/profile/LevelActivity.java |
| http://bb.huluxia.com/bbs/jifen.html | com/huluxia/ui/profile/ProfileScoreActivity.java |
| http://bb.huluxia.com/bbs/hulu.html | com/huluxia/ui/profile/ProfileScoreActivity.java |
| http://bbs.huluxia.com/iccjifen.html | com/huluxia/ui/profile/ProfileScoreActivity.java |
| http://cdn.ws.huluxia.com/game/2016/12/06/GG\_8166(1.22).rpk | com/huluxia/ui/test/TestDownloadChannelActivity.java |
| http://cdn.dnion.huluxia.com/game/2016/12/06/GG\_8166(1.22).rpk | com/huluxia/ui/test/TestDownloadChannelActivity.java |
| http://cdn.ws.huluxia.com/game/2016/12/06/GG\_8166(1.22).apk | com/huluxia/ui/test/TestDownloadChannelActivity.java |
| http://cdn.ws.huluxia.com/game/2014/10/11hpk/1tiantangdao.hpk | com/huluxia/ui/test/TestDownloadChannelActivity.java |
| http://cdn.ws.huluxia.com/game/Rom/GBA/1100323.gba | com/huluxia/ui/test/TestDownloadChannelActivity.java |
| http://stat.huluxia.com/stat/networkerror | com/huluxia/resource/j.java |
| http://stat.huluxia.com/stat/networkspeed | com/huluxia/resource/j.java |
| http://stat.huluxia.com/stat/networkspeed/total | com/huluxia/resource/j.java |
| http://stat.huluxia.com/stat/networkspeed/eachlink | com/huluxia/resource/j.java |
| http://stat.huluxia.com/stat/networkrequest | com/huluxia/resource/j.java |
| http://test.version.huluxia.com | com/huluxia/version/e.java |
| http://version.check.huluxia.com/hlx\_tool/config.txt | com/huluxia/version/e.java |
| http://version.huluxia.com | com/huluxia/version/e.java |
| http://reg.ksyun.huluxia.com/game/update/flooricon.jpg | com/huluxia/service/g.java |
| http://tieba.baidu.com/p/3219122263 | com/huluxia/widget/Constants.java |
| http://app.html5.qq.com/navi/index | com/huluxia/widget/x5web/RefreshActivity.java |
| http://www.huluxia.com | com/huluxia/widget/x5web/BrowserActivity.java |
| http://pan.baidu.com/api/sharedownload | com/huluxia/utils/q.java |
| http://pan.baidu.com/api/getcaptcha | com/huluxia/utils/q.java |
| http://cdn.u2.huluxia.com/ | com/huluxia/utils/z.java |
| http://pan.baidu.com/api/sharedownload | com/huluxia/utils/ah.java |
| http://pan.baidu.com/api/getcaptcha | com/huluxia/utils/ah.java |
| http://wap.huluxia.com | com/huluxia/utils/ab.java |
| http://cdn2.huluxia.com/avatar/1/201406/19/07ceb0ca9fcbea5f84f528b1be9535fc.png\_80x80.jpeg | com/huluxia/utils/ab.java |
| http://bb.huluxia.net/idol | com/huluxia/utils/gameplugin/b.java |
| http://bb.huluxia.net/tool/help/ | com/huluxia/utils/gameplugin/b.java |
| http://bb.huluxia.net/idol | com/huluxia/utils/gameplugin/a.java |
| http://bb.huluxia.net/tool/help/ | com/huluxia/utils/gameplugin/a.java |
| http://reg.huluxia.com/game/2014/11/root/BoomBeachPatch.json | com/huluxia/utils/gameplugin/a.java |
| http://wifi.huluxia.net/wifi/saveBatch | com/huluxia/wifi/WifiDatabase.java |
| http://hlx.iweju.com | com/huluxia/http/base/b.java |
| http://version.check.huluxia.com/hlx\_iccgame | com/huluxia/http/other/h.java |
| http://version.check.huluxia.com/hlx\_tool | com/huluxia/http/other/h.java |
| http://version.check.huluxia.com/hlx\_floor | com/huluxia/http/other/h.java |
| http://version.check.huluxia.com/test | com/huluxia/http/other/h.java |
| http://logs.amap.com/ws/log/upload?product=%s&type=%s&platform=%s&channel=%s&sign=%s | com/loc/da.java |
| http://restapi.amap.com | com/loc/cx.java |
| http://apilocate.amap.com/mobile/binary | com/loc/cd.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/cd.java |
| http://restapi.amap.com/v3/place/around? | com/loc/a.java |
| http://restapi.amap.com/v3/place/text? | com/loc/a.java |
| http://restapi.amap.com/v3/config/district? | com/loc/a.java |
| https://restapi.amap.com/v3/iasdkauth | com/loc/cs.java |
| http://restapi.amap.com/v3/iasdkauth | com/loc/cs.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/bw.java |
| http://apilocatesrc.amap.com/mobile/binary | com/loc/bw.java |
| http://cgicol.amap.com/collection/writedata?ver=v1.0\_ali& | com/loc/bn.java |
| http://restapi.amap.com/v3/geocode/regeo | com/loc/ba.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/d.java |
| http://lkme.cc/i/ | com/microquation/linkedme/android/b/j.java |
| http://lkme.cc | com/microquation/linkedme/android/referral/b.java |
| https://lkme.cc | com/microquation/linkedme/android/referral/b.java |
| http://lkme.cc/track/ | com/microquation/linkedme/android/referral/b.java |
| http://119.29.29.29/d?ttl=1&dn= | com/qiniu/android/dns/http/b.java |
| https://uc.qbox.me | com/qiniu/android/common/a.java |
| https://uplog.qbox.me/log | com/qiniu/android/collect/a.java |
| http://qzs.qq.com/open/mobile/request/sdk\_request.html? | com/tencent/open/SocialApiIml.java |
| http://qzs.qq.com/open/mobile/invite/sdk\_invite.html? | com/tencent/open/SocialApiIml.java |
| http://qzs.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html? | com/tencent/open/SocialApiIml.java |
| http://qzs.qq.com | com/tencent/open/SocialApiIml.java |
| http://c.isdspeed.qq.com/code.cgi | com/tencent/open/b/d.java |
| http://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf | com/tencent/open/utils/e.java |
| https://openmobile.qq.com/ | com/tencent/open/utils/HttpUtils.java |
| http://debugtbs.qq.com | com/tencent/smtt/sdk/WebView.java |
| http://debugx5.qq.com | com/tencent/smtt/sdk/WebView.java |
| http://debugtbs.qq.com?10000\ | com/tencent/smtt/sdk/WebView.java |
| http://mdc.html5.qq.com/mh?channel\_id=50079&u= | com/tencent/smtt/sdk/a/d.java |
| http://log.tbs.qq.com/ajax?c=pu&v=2&k= | com/tencent/smtt/utils/v.java |
| http://log.tbs.qq.com/ajax?c=pu&tk= | com/tencent/smtt/utils/v.java |
| http://wup.imtt.qq.com:8080 | com/tencent/smtt/utils/v.java |
| http://log.tbs.qq.com/ajax?c=dl&k= | com/tencent/smtt/utils/v.java |
| http://cfg.imtt.qq.com/tbs?v=2&mk= | com/tencent/smtt/utils/v.java |
| http://log.tbs.qq.com/ajax?c=ul&v=2&k= | com/tencent/smtt/utils/v.java |
| http://mqqad.html5.qq.com/adjs | com/tencent/smtt/utils/v.java |
| http://log.tbs.qq.com/ajax?c=ucfu&k= | com/tencent/smtt/utils/v.java |
| http://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs | com/tencent/smtt/utils/i.java |
| http://mta.qq.com/ | com/tencent/stat/StatServiceImpl.java |
| http://mta.oa.com/ | com/tencent/stat/StatServiceImpl.java |
| http://mta.qq.com/mta/api/ctr\_feedback/add\_feedback | com/tencent/stat/g.java |
| http://mta.qq.com/mta/api/ctr\_feedback/get\_feedback | com/tencent/stat/g.java |
| http://mta.qq.com/mta/api/ctr\_feedback/reply\_feedback | com/tencent/stat/g.java |
| http://mta.qq.com/mta/api/ctr\_feedback | com/tencent/stat/common/StatConstants.java |
| http://pingma.qq.com:80/mstat/report | com/tencent/stat/common/StatConstants.java |
| http://qzs.qq.com/open/mobile/login/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/user/user\_login\_statis | com/tencent/connect/auth/AuthAgent.java |
| https://openmobile.qq.com/v3/user/get\_info | com/tencent/connect/auth/AuthAgent.java |
| http://appsupport.qq.com/cgi-bin/qzapps/mapp\_addapp.cgi | com/tencent/connect/auth/AuthAgent.java |
| http://openmobile.qq.com/oauth2.0/m\_jump\_by\_version? | com/tencent/connect/common/BaseApi.java |
| http://qzs.qq.com/open/mobile/login/qzsjump.html? | com/tencent/connect/common/BaseApi.java |
| http://fusion.qq.com/cgi-bin/qzapps/unified\_jump?appid=%1$s&from=%2$s&isOpenAppID=1 | com/tencent/connect/share/QQShare.java |
| http://fusion.qq.com/cgi-bin/qzapps/unified\_jump?appid=%1$s&from=%2$s&isOpenAppID=1 | com/tencent/connect/share/QzoneShare.java |
| http://10.237.14.141:9085/pass/register | com/xiaomi/push/service/g.java |
| http://resolver.msg.xiaomi.net/psc/?t=a | com/xiaomi/push/service/ai.java |
| http://%1$s/gslb/gslb/getbucket.asp?ver=3.0 | com/xiaomi/network/HostManager.java |
| http://%1$s/gslb/?ver=3.0 | com/xiaomi/network/HostManagerV2.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/smack/j.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/smack/g.java |
| http://www.jivesoftware.com/xmlns/xmpp/properties\ | com/xiaomi/smack/packet/d.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/smack/provider/c.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/smack/util/c.java |
| https://uop.umeng.com | com/umeng/analytics/a.java |
| http://alog.umeng.com/app\_logs | com/umeng/analytics/a.java |
| http://alog.umengcloud.com/app\_logs | com/umeng/analytics/a.java |
| http://log.umsns.com/ | com/umeng/analytics/social/d.java |
| http://log.umsns.com/share/api/ | com/umeng/analytics/social/d.java |
| http://log.umsns.com/share/api/ | com/umeng/analytics/social/e.java |
| https://cmnsguider.yunos.com:443/genDeviceToken | u/aly/an.java |
| http://goo.gl/rb6C2Y | 摸瓜V1引擎 |
| http://www.JSON.org/json2.js | 摸瓜V2引擎 |
| http://www.JSON.org/js.html | 摸瓜V2引擎 |
| http://javascript.crockford.com/jsmin.html | 摸瓜V2引擎 |
| http://jquery.eisbehr.de/lazy/ | 摸瓜V2引擎 |
| http://www.opensource.org/licenses/mit-license.php | 摸瓜V2引擎 |
| http://www.gnu.org/licenses/gpl-2.0.html | 摸瓜V2引擎 |
| http://server.news.huluxia.com/news/detail/ANDROID/1.0'; | 摸瓜V2引擎 |
| version.huluxia.com | 摸瓜V3引擎 |
| log.tbs.qq.com | 摸瓜V3引擎 |
| floor.huluxia.com | 摸瓜V3引擎 |
| version.check.huluxia.com | 摸瓜V3引擎 |
| uop.umeng.com | 摸瓜V3引擎 |
| stat.huluxia.com | 摸瓜V3引擎 |
| register.xmpush.xiaomi.com | 摸瓜V3引擎 |
| logtbs.sparta.mig.tencent-cloud.net | 摸瓜V3引擎 |
| alog.umengcloud.com | 摸瓜V3引擎 |
| alog.umeng.com | 摸瓜V3引擎 |
| lkme.cc | 摸瓜V3引擎 |
| api.g.huluxia.com | 摸瓜V3引擎 |
| stat.huluxia.com.wswebpic.com | 摸瓜V3引擎 |
| tools.huluxia.com.wswebcdn.com | 摸瓜V3引擎 |
| tools.huluxia.com | 摸瓜V3引擎 |
| restapi.amap.com | 摸瓜V3引擎 |
| http://www.openssl.org/support/faq.html | lib/armeabi-v7a/libijkffmpeg.so |
| http://ns.adobe.com/xap/1.0/ | lib/armeabi-v7a/libimagepipeline.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| xxxx@xxxx.com | com/huawei/android/pushselfshow/utils/a.java |
| ypist@qq.com | com/huluxia/aa/c.java |
| -1@base.apk | com/huluxia/parallel/os/b.java |
| n请将投诉信息发送至邮箱xiaosong@huluxia.com | com/huluxia/ui/loginAndRegister/PolicyActivity.java |
| s-1@base.apk | com/huluxia/utils/w.java |
| eray.jiang@gmail.com | com/system/util/ap.java |
| ctwap@mycdma.cn | com/tencent/mid/a/a.java |
| ffmpeg-devel@ffmpeg.org | lib/armeabi-v7a/libijkplayer.so |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184 | org/bytedeco/javacpp/avutil.java |
| 17179869184 | tv/danmaku/ijk/media/player/IjkMediaMeta.java |

## **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=ch, ST=guangdong, L=guangzhou, O=hlx, OU=hlx, CN=kevinhuang 签名算法: rsassa\_pkcs1v15 有效期自: 2013-06-04 07:47:01+00:00 有效期至: 2040-10-20 07:47:01+00:00 发行人: C=ch, ST=guangdong, L=guangzhou, O=hlx, OU=hlx, CN=kevinhuang 序列号: 0x51ad9b75 哈希算法: sha1 md5值: 39791f34c818ddfa702360a9805d7930 sha1值: fa5a9cd5b88543662593518dd983b772856c0f62 sha256值: 8ddb9775208697a54ce2db9eb1c9acf868b2d69a1c6308489f999fe2fd247269 sha512值: 7336c4d78d2559a4d9488fa7e26d13371679bfd6c408daeffcbe617b2d3110f30bebc5037a0162d0f209a089bc36de0c0161c7bb3d3abe61594fbbb0b4e130ca 公钥算法: rsa 密钥长度: 1024 指纹: 067408b51e57091143ed7618daf77be6a4469e87904c4a42d36d1f955daceac3**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "send\_no\_user" : "暂无文件接收者" |
| "deleted\_key" : " %1$s deleted " |
| "forgetPassword" : "忘记密码" |
| "forget\_password" : "忘记密码？" |
| "go\_authorization" : "去授权" |
| "go\_authorization\_fail" : "跳转失败，请手动去应用管理设置！" |
| "root\_kinguser" : "使用kinguser工具获取手机权限" |
| "topic\_app\_author" : "作者: " |
| "topic\_auth" : "版主认证" |
| "topic\_auth\_failed" : "帖子认证失败" |
| "topic\_auth\_succ" : "帖子认证成功" |
| "send\_no\_user" : "Tidak ada koneksi" |
| "send\_no\_user" : "暂无文件接收者" |

## **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**

## **10. 应用内通信**

**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。**