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

**任性包（ 1.0.1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 | 任性包 |
| 版本 | 1.0.1 |
| 包名 | com.egh.flgvjsb |
| 域名线索 | 49条 |
| URL线索 | 24条 |
| APP图标 |  |
| 分析日期 | 2025年7月31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 | com.egh.flgvjsb.apk |
| 文件大小 | 6.83MB |
| MD5值 | aadf0893529fcd7bc8877a1941a42197 |
| SHA1值 | 9d9b290bf5fd6b421d0877df79bd2cffb55e0eda |
| SHA256值 | ea739a91600f0e1533ca8a6281578f05dbdb44ad9de322e2c1672cd3c2385eec |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 任性包 |
| 包名 | com.egh.flgvjsb |
| 主活动Activity | com.egh.flgvjsb.MainActivity |
| 安卓版本名称 | 1.0.1 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| developer.ean.com | IP: 23.215.212.48 所属国家: Australia 地区: Western Australia 城市: Perth  |
| app.baifubao.com | 没有服务器地理信息.  |
| alltest.baifubao.com | 没有服务器地理信息.  |
| wallet.baidu.com | 没有服务器地理信息.  |
| html.spec.whatwg.org | IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| gzns-nbg-fpu-aug-c02xi2-49.gzns.baidu.com | 没有服务器地理信息.  |
| tongji.baidu.com | IP: 111.206.208.102 所属国家: China 地区: Beijing 城市: Beijing  |
| jqueryvalidation.org | IP: 172.67.193.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| cp01-ra09-jueheng2qa063.cp01.baidu.com | 没有服务器地理信息.  |
| lark.baidu.com | IP: 110.242.68.103 所属国家: China 地区: Hebei 城市: Baoding  |
| sns.qzone.qq.com | IP: 116.130.229.200 所属国家: China 地区: Beijing 城市: Beijing  |
| cp01-front.epc.baidu.com | 没有服务器地理信息.  |
| smoke.fpd | 没有服务器地理信息.  |
| www.baifubao.com | 没有服务器地理信息.  |
| connect.qq.com | IP: 116.130.223.156 所属国家: China 地区: Beijing 城市: Beijing  |
| m.baifubao.com | 没有服务器地理信息.  |
| layer.layui.com | 没有服务器地理信息.  |
| qylark.baidu.com | 没有服务器地理信息.  |
| hmcdn.baidu.com | IP: 61.163.9.48 所属国家: China 地区: Henan 城市: Luoyang  |
| a.app.qq.com | IP: 60.28.219.32 所属国家: China 地区: Tianjin 城市: Tianjin  |
| qyfront.baidu.com | IP: 39.156.68.146 所属国家: China 地区: Beijing 城市: Beijing  |
| en.wikipedia.org | IP: 199.16.158.182 所属国家: United States of America 地区: California 城市: San Francisco  |
| mathiasbynens.be | IP: 83.137.145.144 所属国家: Netherlands 地区: Groningen 城市: Groningen  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| schemas.android.com | 没有服务器地理信息.  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| testqa.fbu | 没有服务器地理信息.  |
| front.baidu.com | 没有服务器地理信息.  |
| baifubao.baidu.com | IP: 220.181.33.113 所属国家: China 地区: Beijing 城市: Beijing  |
| jin.baidu.com | 没有服务器地理信息.  |
| cp01-yinping.epc.baidu.com | 没有服务器地理信息.  |
| smoke2.fbu | 没有服务器地理信息.  |
| fex.bdstatic.com | IP: 121.22.239.48 所属国家: China 地区: Hebei 城市: Qinhuangdao  |
| gist.github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| img.yzcdn.cn | IP: 116.136.200.241 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| icash.baidu.com | 没有服务器地理信息.  |
| h5.u51.com | IP: 125.38.11.60 所属国家: China 地区: Tianjin 城市: Tianjin  |
| tjdeho.com | 没有服务器地理信息.  |
| qyicash.baidu.com | 没有服务器地理信息.  |
| mechatim.com | IP: 39.100.35.138 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| gzns-nbg-fpu-aug-c02xi2-87.gzns.baidu.com | 没有服务器地理信息.  |
| itunes.apple.com | IP: 111.161.122.2 所属国家: China 地区: Tianjin 城市: Tianjin  |
| widget.renren.com | IP: 120.133.12.123 所属国家: China 地区: Beijing 城市: Beijing  |
| api.map.baidu.com | IP: 111.206.208.72 所属国家: China 地区: Beijing 城市: Beijing  |
| v.t.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| 119.91.247.63 | IP: 119.91.247.63 所属国家: China 地区: Beijing 城市: Beijing  |
| service.weibo.com | IP: 116.133.8.18 所属国家: China 地区: Beijing 城市: Beijing  |
| yf-fso-rdtest-00.yf01.baidu.com | 没有服务器地理信息.  |
| www.douban.com | IP: 81.70.124.99 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://119.91.247.63/ip.json  | com/egh/flgvjsb/MainActivity.java  |
| http://schemas.android.com/apk/res/android  | com/hjq/permissions/AndroidManifestParser.java  |
| https://baifubao.baidu.com/jump?domain=https://www.baifubao.com/&uri=  | 摸瓜V2引擎  |
| https://front.baidu.com/fms/tpl/coupon/couponChoose?type=loan&  | 摸瓜V2引擎  |
| https://front.baidu.com/fms/tpl/coupon/couponChoose?type=repay&  | 摸瓜V2引擎  |
| https://jin.baidu.com/loan/apply/quick?page=myaccount&channel=shoubaicashloan  | 摸瓜V2引擎  |
| https://wallet.baidu.com/content/mywallet/h5/sdk\_page/sdk\_quan\_manager.html  | 摸瓜V2引擎  |
| https://lark.baidu.com  | 摸瓜V2引擎  |
| https://front.baidu.com  | 摸瓜V2引擎  |
| https://icash.baidu.com/hiloan/Home  | 摸瓜V2引擎  |
| https://icash.baidu.com/cloan/Home  | 摸瓜V2引擎  |
| https://baifubao.baidu.com/jump?domain=https://alltest.baifubao.com/&uri=  | 摸瓜V2引擎  |
| https://qyfront.baidu.com/fms/tpl/coupon/couponChoose?type=loan&  | 摸瓜V2引擎  |
| https://qyfront.baidu.com/fms/tpl/coupon/couponChoose?type=repay&  | 摸瓜V2引擎  |
| https://jin.baidu.com/loan/apply/quick?page=myaccount&channel=shoubaicashloan&orp\_preview=1  | 摸瓜V2引擎  |
| https://alltest.baifubao.com/content/mywallet/h5/sdk\_page/sdk\_quan\_manager.html?type=h5qianbao&  | 摸瓜V2引擎  |
| https://qylark.baidu.com  | 摸瓜V2引擎  |
| https://qyfront.baidu.com  | 摸瓜V2引擎  |
| https://qyicash.baidu.com/hiloan/Home  | 摸瓜V2引擎  |
| https://qyicash.baidu.com/cloan/Home  | 摸瓜V2引擎  |
| http://cp01-front.epc.baidu.com:8099/fms/tpl/coupon/couponChoose?type=loan&  | 摸瓜V2引擎  |
| http://cp01-front.epc.baidu.com:8099/fms/tpl/coupon/couponChoose?type=repay&  | 摸瓜V2引擎  |
| https://m.baifubao.com/content/mywallet/h5/sdk\_page/sdk\_quan\_manager.html?type=h5qianbao&  | 摸瓜V2引擎  |
| http://yf-fso-rdtest-00.yf01.baidu.com:8082/loan/apply/quick?page=myaccount&channel=shoubaicashloan  | 摸瓜V2引擎  |
| http://gzns-nbg-fpu-aug-c02xi2-49.gzns.baidu.com:8081  | 摸瓜V2引擎  |
| http://cp01-front.epc.baidu.com:8082  | 摸瓜V2引擎  |
| https://gzns-nbg-fpu-aug-c02xi2-87.gzns.baidu.com:8877/hiloan/Home  | 摸瓜V2引擎  |
| https://gzns-nbg-fpu-aug-c02xi2-87.gzns.baidu.com:8077/cloan/Home  | 摸瓜V2引擎  |
| http://smoke2.fbu\_node.otp.baidu.com/fms/tpl/coupon/couponChoose?type=loan&  | 摸瓜V2引擎  |
| http://smoke2.fbu\_node.otp.baidu.com/fms/tpl/coupon/couponChoose?type=repay&  | 摸瓜V2引擎  |
| http://cp01-yinping.epc.baidu.com:8000/loan/apply/quick?page=myaccount&channel=shoubaicashloan  | 摸瓜V2引擎  |
| http://smoke.fpd\_lark.otp.baidu.com  | 摸瓜V2引擎  |
| http://testqa.fbu\_node.otp.baidu.com  | 摸瓜V2引擎  |
| https://cp01-ra09-jueheng2qa063.cp01.baidu.com:8604/hiloan/Home  | 摸瓜V2引擎  |
| https://cp01-ra09-jueheng2qa063.cp01.baidu.com:8606/cloan/Home  | 摸瓜V2引擎  |
| http://gzns-nbg-fpu-aug-c02xi2-87.gzns.baidu.com:8979/lark/coupon/choose?type=loan&  | 摸瓜V2引擎  |
| http://gzns-nbg-fpu-aug-c02xi2-87.gzns.baidu.com:8979/lark/coupon/choose?type=repay&  | 摸瓜V2引擎  |
| http://cp01-front.epc.baidu.com:8099  | 摸瓜V2引擎  |
| https://gzns-nbg-fpu-aug-c02xi2-87.gzns.baidu.com:8877/cloan/Home  | 摸瓜V2引擎  |
| https://qylark.baidu.com/lark/coupon/choose?type=loan&  | 摸瓜V2引擎  |
| https://qylark.baidu.com/lark/coupon/choose?type=repay&  | 摸瓜V2引擎  |
| http://cp01-ra09-jueheng2qa063.cp01.baidu.com:8140/loan/apply/quick?page=myaccount&channel=shoubaicashloan  | 摸瓜V2引擎  |
| https://app.baifubao.com/Home.html?channel=1019132i&from=xianjindai&bdwallet\_type=1&bdwallet\_url\_ios=  | 摸瓜V2引擎  |
| https://app.baifubao.com/Home.html?channel=1019132i&from=hiloan&bdwallet\_type=1&bdwallet\_url\_ios=  | 摸瓜V2引擎  |
| https://www.baifubao.com/wallet-fe/0/large\_payment/0  | 摸瓜V2引擎  |
| https://itunes.apple.com/app/apple-store/id992762663&mt=8  | 摸瓜V2引擎  |
| https://fex.bdstatic.com  | 摸瓜V2引擎  |
| http://fex.bdstatic.com  | 摸瓜V2引擎  |
| http://service.weibo.com/share/share.php  | 摸瓜V2引擎  |
| http://connect.qq.com/widget/shareqq/index.html  | 摸瓜V2引擎  |
| http://sns.qzone.qq.com/cgi-bin/qzshare/cgi\_qzshare\_onekey  | 摸瓜V2引擎  |
| http://v.t.qq.com/share/share.php  | 摸瓜V2引擎  |
| http://widget.renren.com/dialog/share  | 摸瓜V2引擎  |
| http://www.douban.com/recommend/  | 摸瓜V2引擎  |
| http://api.map.baidu.com/getscript?type=quick&file=feature&ak=WVAXZ05oyNRXS5egLImmentg&t=20140109092002  | 摸瓜V2引擎  |
| http://api.map.baidu.com/getscript?type=quick&file=api&ak=WVAXZ05oyNRXS5egLImmentg&t=20140109092002  | 摸瓜V2引擎  |
| http://mechatim.com/js/unit/button.js?id=  | 摸瓜V2引擎  |
| http://a.app.qq.com/o/simple.jsp?pkgname=com.fenqi.geinihua  | 摸瓜V2引擎  |
| https://itunes.apple.com/app/id1076275012  | 摸瓜V2引擎  |
| http://h5.u51.com/99fenqi/apk/com.fenqi.geinihua\_geinihua\_signed.apk  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/validate/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/valid/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/rules/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/blank-selector/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/filled-selector/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/unchecked-selector/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/jQuery.validator.format/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/jQuery.validator.setDefaults/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/Validator.form/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/Validator.element/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/Validator.showErrors/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/Validator.resetForm/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/jQuery.validator.addMethod/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/required-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/email-method/  | 摸瓜V2引擎  |
| https://html.spec.whatwg.org/multipage/forms.html  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/url-method/  | 摸瓜V2引擎  |
| https://gist.github.com/dperini/729294  | 摸瓜V2引擎  |
| https://mathiasbynens.be/demo/url-regex  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/date-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/dateISO-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/number-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/digits-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/creditcard-method/  | 摸瓜V2引擎  |
| http://en.wikipedia.org/wiki/Luhn\_algorithm  | 摸瓜V2引擎  |
| http://developer.ean.com/general\_info/Valid\_Credit\_Card\_Types  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/minlength-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/maxlength-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/rangelength-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/min-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/max-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/range-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/equalTo-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/remote-method/  | 摸瓜V2引擎  |
| https://github.com/think2011/localResizeIMG/issues/7  | 摸瓜V2引擎  |
| http://layer.layui.com/mobile  | 摸瓜V2引擎  |
| http://service.weibo.com/share/share.php  | 摸瓜V2引擎  |
| http://connect.qq.com/widget/shareqq/index.html  | 摸瓜V2引擎  |
| http://sns.qzone.qq.com/cgi-bin/qzshare/cgi\_qzshare\_onekey  | 摸瓜V2引擎  |
| http://v.t.qq.com/share/share.php  | 摸瓜V2引擎  |
| http://widget.renren.com/dialog/share  | 摸瓜V2引擎  |
| http://www.douban.com/recommend/  | 摸瓜V2引擎  |
| http://api.map.baidu.com/getscript?type=quick&file=feature&ak=WVAXZ05oyNRXS5egLImmentg&t=20140109092002  | 摸瓜V2引擎  |
| http://api.map.baidu.com/getscript?type=quick&file=api&ak=WVAXZ05oyNRXS5egLImmentg&t=20140109092002  | 摸瓜V2引擎  |
| http://mechatim.com/js/unit/button.js?id=  | 摸瓜V2引擎  |
| https://github.com/aui/artTemplate  | 摸瓜V2引擎  |
| https://github.com/aui/artTemplate  | 摸瓜V2引擎  |
| https://github.com/aui/artTemplate/issues/41  | 摸瓜V2引擎  |
| https://tjdeho.com  | 摸瓜V2引擎  |
| https://tjdeho.com/  | 摸瓜V2引擎  |
| http://a  | 摸瓜V2引擎  |
| http://a/c%20d?a\x3d1\x26c\x3d3  | 摸瓜V2引擎  |
| https://a@b  | 摸瓜V2引擎  |
| http://\u0442\u0435\u0441\u0442  | 摸瓜V2引擎  |
| http://x  | 摸瓜V2引擎  |
| https://img.yzcdn.cn/vant/empty-image-  | 摸瓜V2引擎  |
| http://a  | 摸瓜V2引擎  |
| http://a/c%20d?a\x3d1\x26c\x3d3  | 摸瓜V2引擎  |
| https://a@b  | 摸瓜V2引擎  |
| http://\u0442\u0435\u0441\u0442  | 摸瓜V2引擎  |
| http://x  | 摸瓜V2引擎  |
| https://img.yzcdn.cn/vant/empty-image-  | 摸瓜V2引擎  |
| http://tongji.baidu.com/hm-web/welcome/ico  | 摸瓜V2引擎  |
| https://hmcdn.baidu.com/static/tongji/plugins/  | 摸瓜V2引擎  |
| https://baifubao.baidu.com/jump?domain=https://www.baifubao.com/&uri=  | 摸瓜V2引擎  |
| https://front.baidu.com/fms/tpl/coupon/couponChoose?type=loan&  | 摸瓜V2引擎  |
| https://front.baidu.com/fms/tpl/coupon/couponChoose?type=repay&  | 摸瓜V2引擎  |
| https://jin.baidu.com/loan/apply/quick?page=myaccount&channel=shoubaicashloan  | 摸瓜V2引擎  |
| https://wallet.baidu.com/content/mywallet/h5/sdk\_page/sdk\_quan\_manager.html  | 摸瓜V2引擎  |
| https://lark.baidu.com  | 摸瓜V2引擎  |
| https://front.baidu.com  | 摸瓜V2引擎  |
| https://icash.baidu.com/hiloan/Home  | 摸瓜V2引擎  |
| https://icash.baidu.com/cloan/Home  | 摸瓜V2引擎  |
| https://baifubao.baidu.com/jump?domain=https://alltest.baifubao.com/&uri=  | 摸瓜V2引擎  |
| https://qyfront.baidu.com/fms/tpl/coupon/couponChoose?type=loan&  | 摸瓜V2引擎  |
| https://qyfront.baidu.com/fms/tpl/coupon/couponChoose?type=repay&  | 摸瓜V2引擎  |
| https://jin.baidu.com/loan/apply/quick?page=myaccount&channel=shoubaicashloan&orp\_preview=1  | 摸瓜V2引擎  |
| https://alltest.baifubao.com/content/mywallet/h5/sdk\_page/sdk\_quan\_manager.html?type=h5qianbao&  | 摸瓜V2引擎  |
| https://qylark.baidu.com  | 摸瓜V2引擎  |
| https://qyfront.baidu.com  | 摸瓜V2引擎  |
| https://qyicash.baidu.com/hiloan/Home  | 摸瓜V2引擎  |
| https://qyicash.baidu.com/cloan/Home  | 摸瓜V2引擎  |
| http://cp01-front.epc.baidu.com:8099/fms/tpl/coupon/couponChoose?type=loan&  | 摸瓜V2引擎  |
| http://cp01-front.epc.baidu.com:8099/fms/tpl/coupon/couponChoose?type=repay&  | 摸瓜V2引擎  |
| https://m.baifubao.com/content/mywallet/h5/sdk\_page/sdk\_quan\_manager.html?type=h5qianbao&  | 摸瓜V2引擎  |
| http://yf-fso-rdtest-00.yf01.baidu.com:8082/loan/apply/quick?page=myaccount&channel=shoubaicashloan  | 摸瓜V2引擎  |
| http://gzns-nbg-fpu-aug-c02xi2-49.gzns.baidu.com:8081  | 摸瓜V2引擎  |
| http://cp01-front.epc.baidu.com:8082  | 摸瓜V2引擎  |
| https://gzns-nbg-fpu-aug-c02xi2-87.gzns.baidu.com:8877/hiloan/Home  | 摸瓜V2引擎  |
| https://gzns-nbg-fpu-aug-c02xi2-87.gzns.baidu.com:8077/cloan/Home  | 摸瓜V2引擎  |
| http://smoke2.fbu\_node.otp.baidu.com/fms/tpl/coupon/couponChoose?type=loan&  | 摸瓜V2引擎  |
| http://smoke2.fbu\_node.otp.baidu.com/fms/tpl/coupon/couponChoose?type=repay&  | 摸瓜V2引擎  |
| http://cp01-yinping.epc.baidu.com:8000/loan/apply/quick?page=myaccount&channel=shoubaicashloan  | 摸瓜V2引擎  |
| http://smoke.fpd\_lark.otp.baidu.com  | 摸瓜V2引擎  |
| http://testqa.fbu\_node.otp.baidu.com  | 摸瓜V2引擎  |
| https://cp01-ra09-jueheng2qa063.cp01.baidu.com:8604/hiloan/Home  | 摸瓜V2引擎  |
| https://cp01-ra09-jueheng2qa063.cp01.baidu.com:8606/cloan/Home  | 摸瓜V2引擎  |
| http://gzns-nbg-fpu-aug-c02xi2-87.gzns.baidu.com:8979/lark/coupon/choose?type=loan&  | 摸瓜V2引擎  |
| http://gzns-nbg-fpu-aug-c02xi2-87.gzns.baidu.com:8979/lark/coupon/choose?type=repay&  | 摸瓜V2引擎  |
| http://cp01-front.epc.baidu.com:8099  | 摸瓜V2引擎  |
| https://gzns-nbg-fpu-aug-c02xi2-87.gzns.baidu.com:8877/cloan/Home  | 摸瓜V2引擎  |
| https://qylark.baidu.com/lark/coupon/choose?type=loan&  | 摸瓜V2引擎  |
| https://qylark.baidu.com/lark/coupon/choose?type=repay&  | 摸瓜V2引擎  |
| http://cp01-ra09-jueheng2qa063.cp01.baidu.com:8140/loan/apply/quick?page=myaccount&channel=shoubaicashloan  | 摸瓜V2引擎  |
| https://app.baifubao.com/Home.html?channel=1019132i&from=xianjindai&bdwallet\_type=1&bdwallet\_url\_ios=  | 摸瓜V2引擎  |
| https://app.baifubao.com/Home.html?channel=1019132i&from=hiloan&bdwallet\_type=1&bdwallet\_url\_ios=  | 摸瓜V2引擎  |
| https://www.baifubao.com/wallet-fe/0/large\_payment/0  | 摸瓜V2引擎  |
| https://itunes.apple.com/app/apple-store/id992762663&mt=8  | 摸瓜V2引擎  |
| https://fex.bdstatic.com  | 摸瓜V2引擎  |
| http://fex.bdstatic.com  | 摸瓜V2引擎  |
| http://service.weibo.com/share/share.php  | 摸瓜V2引擎  |
| http://connect.qq.com/widget/shareqq/index.html  | 摸瓜V2引擎  |
| http://sns.qzone.qq.com/cgi-bin/qzshare/cgi\_qzshare\_onekey  | 摸瓜V2引擎  |
| http://v.t.qq.com/share/share.php  | 摸瓜V2引擎  |
| http://widget.renren.com/dialog/share  | 摸瓜V2引擎  |
| http://www.douban.com/recommend/  | 摸瓜V2引擎  |
| http://api.map.baidu.com/getscript?type=quick&file=feature&ak=WVAXZ05oyNRXS5egLImmentg&t=20140109092002  | 摸瓜V2引擎  |
| http://api.map.baidu.com/getscript?type=quick&file=api&ak=WVAXZ05oyNRXS5egLImmentg&t=20140109092002  | 摸瓜V2引擎  |
| http://mechatim.com/js/unit/button.js?id=  | 摸瓜V2引擎  |
| http://a.app.qq.com/o/simple.jsp?pkgname=com.fenqi.geinihua  | 摸瓜V2引擎  |
| https://itunes.apple.com/app/id1076275012  | 摸瓜V2引擎  |
| http://h5.u51.com/99fenqi/apk/com.fenqi.geinihua\_geinihua\_signed.apk  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/validate/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/valid/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/rules/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/blank-selector/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/filled-selector/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/unchecked-selector/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/jQuery.validator.format/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/jQuery.validator.setDefaults/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/Validator.form/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/Validator.element/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/Validator.showErrors/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/Validator.resetForm/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/jQuery.validator.addMethod/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/required-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/email-method/  | 摸瓜V2引擎  |
| https://html.spec.whatwg.org/multipage/forms.html  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/url-method/  | 摸瓜V2引擎  |
| https://gist.github.com/dperini/729294  | 摸瓜V2引擎  |
| https://mathiasbynens.be/demo/url-regex  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/date-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/dateISO-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/number-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/digits-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/creditcard-method/  | 摸瓜V2引擎  |
| http://en.wikipedia.org/wiki/Luhn\_algorithm  | 摸瓜V2引擎  |
| http://developer.ean.com/general\_info/Valid\_Credit\_Card\_Types  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/minlength-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/maxlength-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/rangelength-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/min-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/max-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/range-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/equalTo-method/  | 摸瓜V2引擎  |
| http://jqueryvalidation.org/remote-method/  | 摸瓜V2引擎  |
| https://github.com/think2011/localResizeIMG/issues/7  | 摸瓜V2引擎  |
| http://layer.layui.com/mobile  | 摸瓜V2引擎  |
| http://service.weibo.com/share/share.php  | 摸瓜V2引擎  |
| http://connect.qq.com/widget/shareqq/index.html  | 摸瓜V2引擎  |
| http://sns.qzone.qq.com/cgi-bin/qzshare/cgi\_qzshare\_onekey  | 摸瓜V2引擎  |
| http://v.t.qq.com/share/share.php  | 摸瓜V2引擎  |
| http://widget.renren.com/dialog/share  | 摸瓜V2引擎  |
| http://www.douban.com/recommend/  | 摸瓜V2引擎  |
| http://api.map.baidu.com/getscript?type=quick&file=feature&ak=WVAXZ05oyNRXS5egLImmentg&t=20140109092002  | 摸瓜V2引擎  |
| http://api.map.baidu.com/getscript?type=quick&file=api&ak=WVAXZ05oyNRXS5egLImmentg&t=20140109092002  | 摸瓜V2引擎  |
| http://mechatim.com/js/unit/button.js?id=  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13261686610  | 摸瓜V2引擎  |

## **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=Fsya8, ST=TJASe, L=kiD7r, O=wq1751541867328, OU=ni1751541867328, CN=yzqe 签名算法: rsassa\_pkcs1v15 有效期自: 2025-07-03 11:24:32+00:00 有效期至: 2075-06-21 11:24:32+00:00 发行人: C=Fsya8, ST=TJASe, L=kiD7r, O=wq1751541867328, OU=ni1751541867328, CN=yzqe 序列号: 0x43e83b30 哈希算法: sha512 md5值: 1212850f9d2e7d936d69d30f34de0d6c sha1值: b1e50ea42a8f9afed98e4e051fcd4ce34e13b815 sha256值: 0dfa9a6c4207ae6193c1ba82aa5ca4cd93aa3deda4850d7cb0e8caf97115bef1 sha512值: 4d01adfb8441e1d9c7e3fa5c797c4860bebaff0dc7e2df820df12eb1819a04d5051dfeef85efb01a516cd092b7001e160d37e5bfb8db4f6f3fc24be5f72212cc 公钥算法: rsa 密钥长度: 4096 指纹: a345b3171cdcdf93d167a8f964e4c31c07072714bab9536df0d3cbc139857be5**

## **6. 硬编码敏感信息**

## **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.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.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.WRITE\_MEDIA\_STORAGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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\_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 |

## **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。**