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

**优赢国际（ 3.6.0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 | 优赢国际 |
| 版本 | 3.6.0 |
| 包名 | com.flb.zj.omkxm |
| 域名线索 | 182条 |
| URL线索 | 37条 |
| APP图标 |  |
| 分析日期 | 2025年7月10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 | omkxm.apk |
| 文件大小 | 7.61MB |
| MD5值 | ea80b5e8c7eae460d50f240c3be39c1d |
| SHA1值 | 761167ec97977fb78e2648b1b9c6ee2bc703e3ab |
| SHA256值 | 3b6c2a90bbdc1e7048d199aeb8008a74c8e0f23f14e1450c0ed8146c3b643920 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 优赢国际 |
| 包名 | com.flb.zj.omkxm |
| 主活动Activity | com.fob.ds.activity.InitActivity |
| 安卓版本名称 | 3.6.0 |
| 安卓版本 | 360 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| 4ossb3.dtd5682.com | 没有服务器地理信息. |
| b5d9o2.dtd5680.com | 没有服务器地理信息. |
| bvfds47.dtd5680.com | 没有服务器地理信息. |
| vghjk72.dtd5682.com | 没有服务器地理信息. |
| oq1si5.dtd5680.com | 没有服务器地理信息. |
| m8bdog.dtd5681.com | 没有服务器地理信息. |
| tsis.jpush.cn | IP: 183.232.58.229  所属国家: China  地区: Guangdong  城市: Guangzhou |
| px-intl.ucweb.com | IP: 157.185.188.1  所属国家: United States of America  地区: California  城市: Monrovia |
| cnkake25.dtd5681.com | 没有服务器地理信息. |
| q4chyj.dtd5683.com | 没有服务器地理信息. |
| ut9iqw.dtd5682.com | 没有服务器地理信息. |
| iwg2qi.dtd5683.com | 没有服务器地理信息. |
| 12lbrt.dtd5682.com | 没有服务器地理信息. |
| claoe45.dtd5683.com | 没有服务器地理信息. |
| ss945p.dtd5683.com | 没有服务器地理信息. |
| a9jwxe.dtd5682.com | 没有服务器地理信息. |
| rh6mb3.dtd5682.com | 没有服务器地理信息. |
| 12lbrt.dtd5683.com | 没有服务器地理信息. |
| oihvg63.dtd5683.com | 没有服务器地理信息. |
| vsjsdg13.dtd5682.com | 没有服务器地理信息. |
| b5d9o2.dtd5683.com | 没有服务器地理信息. |
| n0t82m.dtd5683.com | 没有服务器地理信息. |
| ulogs.umeng.com | IP: 223.109.148.177  所属国家: China  地区: Beijing  城市: Beijing |
| 9gy29g.dtd5680.com | 没有服务器地理信息. |
| cvghuj76.dtd5681.com | 没有服务器地理信息. |
| iwg2qi.dtd5681.com | 没有服务器地理信息. |
| cvs341.dtd5680.com | 没有服务器地理信息. |
| vag0ux.dtd5683.com | 没有服务器地理信息. |
| dhms24.dtd5682.com | 没有服务器地理信息. |
| oq1si5.dtd5681.com | 没有服务器地理信息. |
| m8bdog.dtd5680.com | 没有服务器地理信息. |
| t1jyqs.dtd5682.com | 没有服务器地理信息. |
| 9gy29g.dtd5683.com | 没有服务器地理信息. |
| vsjsdg13.dtd5680.com | 没有服务器地理信息. |
| claoe45.dtd5681.com | 没有服务器地理信息. |
| 915uml.dtd5681.com | 没有服务器地理信息. |
| bckjsj31.dtd5683.com | 没有服务器地理信息. |
| vghjk72.dtd5680.com | 没有服务器地理信息. |
| bckjsj31.dtd5681.com | 没有服务器地理信息. |
| 9y6php.dtd5680.com | 没有服务器地理信息. |
| t1jyqs.dtd5680.com | 没有服务器地理信息. |
| i2u2wo.dtd5681.com | 没有服务器地理信息. |
| anfan33.dtd5680.com | 没有服务器地理信息. |
| cvs341.dtd5681.com | 没有服务器地理信息. |
| 053q4d.dtd5680.com | 没有服务器地理信息. |
| w7l6o6.dtd5680.com | 没有服务器地理信息. |
| 915uml.dtd5683.com | 没有服务器地理信息. |
| 915uml.dtd5682.com | 没有服务器地理信息. |
| cafkaa30.dtd5682.com | 没有服务器地理信息. |
| bb7o11.dtd5681.com | 没有服务器地理信息. |
| image.cnamedomain.com | 没有服务器地理信息. |
| i2u2wo.dtd5682.com | 没有服务器地理信息. |
| 053q4d.dtd5681.com | 没有服务器地理信息. |
| oss-cn-.aliyuncs.comor | 没有服务器地理信息. |
| w7l6o6.dtd5683.com | 没有服务器地理信息. |
| cnkake25.dtd5682.com | 没有服务器地理信息. |
| dsapi1.ds16387.com | IP: 128.242.245.253  所属国家: United States of America  地区: California  城市: Milpitas |
| 90iyue.dtd5682.com | 没有服务器地理信息. |
| bb7o11.dtd5683.com | 没有服务器地理信息. |
| cvs341.dtd5683.com | 没有服务器地理信息. |
| 172.25.12.1 | IP: 172.25.12.1  所属国家: -  地区: -  城市: - |
| bckjsj31.dtd5682.com | 没有服务器地理信息. |
| cnkake25.dtd5680.com | 没有服务器地理信息. |
| bvfds47.dtd5681.com | 没有服务器地理信息. |
| oq1si5.dtd5683.com | 没有服务器地理信息. |
| plbslog.umeng.com | IP: 36.156.202.68  所属国家: China  地区: Beijing  城市: Beijing |
| vag0ux.dtd5681.com | 没有服务器地理信息. |
| 9y6php.dtd5681.com | 没有服务器地理信息. |
| rh6mb3.dtd5681.com | 没有服务器地理信息. |
| www.huobi.vc | IP: 69.63.184.30  所属国家: Netherlands  地区: Noord-Holland  城市: Amsterdam |
| ip.taobao.com | IP: 203.119.169.6  所属国家: China  地区: Beijing  城市: Beijing |
| m8bdog.dtd5683.com | 没有服务器地理信息. |
| pslog.umeng.com | IP: 59.82.29.162  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| oss.aliyuncs.com | IP: 118.178.29.5  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| cswbaa74.dtd5680.com | 没有服务器地理信息. |
| rh6mb3.dtd5680.com | 没有服务器地理信息. |
| iwg2qi.dtd5682.com | 没有服务器地理信息. |
| errlog.umeng.com | IP: 223.109.148.180  所属国家: China  地区: Beijing  城市: Beijing |
| y0aa70.dtd5683.com | 没有服务器地理信息. |
| aaid.umeng.com | IP: 218.91.197.67  所属国家: China  地区: Jiangsu  城市: Nantong |
| cafkaa30.dtd5683.com | 没有服务器地理信息. |
| cswbaa74.dtd5682.com | 没有服务器地理信息. |
| cvs341.dtd5682.com | 没有服务器地理信息. |
| claoe45.dtd5680.com | 没有服务器地理信息. |
| goy1kc.dtd5681.com | 没有服务器地理信息. |
| oss-cn-shanghai.aliyuncs.com | IP: 106.14.228.220  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ut9iqw.dtd5683.com | 没有服务器地理信息. |
| 127.0.0.1 | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| y0aa70.dtd5680.com | 没有服务器地理信息. |
| oihvg63.dtd5680.com | 没有服务器地理信息. |
| ut9iqw.dtd5680.com | 没有服务器地理信息. |
| vag0ux.dtd5682.com | 没有服务器地理信息. |
| www.okex.com | IP: 119.28.87.227  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| bvfds47.dtd5682.com | 没有服务器地理信息. |
| 9gy29g.dtd5681.com | 没有服务器地理信息. |
| n0t82m.dtd5681.com | 没有服务器地理信息. |
| cvghuj76.dtd5682.com | 没有服务器地理信息. |
| a9jwxe.dtd5683.com | 没有服务器地理信息. |
| 053q4d.dtd5683.com | 没有服务器地理信息. |
| y0aa70.dtd5682.com | 没有服务器地理信息. |
| t1jyqs.dtd5683.com | 没有服务器地理信息. |
| b5d9o2.dtd5682.com | 没有服务器地理信息. |
| alogsus.umeng.com | IP: 223.109.148.178  所属国家: China  地区: Beijing  城市: Beijing |
| cvghuj76.dtd5683.com | 没有服务器地理信息. |
| 12lbrt.dtd5681.com | 没有服务器地理信息. |
| 053q4d.dtd5682.com | 没有服务器地理信息. |
| 4ossb3.dtd5680.com | 没有服务器地理信息. |
| bckjsj31.dtd5680.com | 没有服务器地理信息. |
| bb7o11.dtd5680.com | 没有服务器地理信息. |
| ut9iqw.dtd5681.com | 没有服务器地理信息. |
| 90iyue.dtd5681.com | 没有服务器地理信息. |
| cswbaa74.dtd5683.com | 没有服务器地理信息. |
| ss945p.dtd5682.com | 没有服务器地理信息. |
| goy1kc.dtd5680.com | 没有服务器地理信息. |
| help.kg-88.net | 没有服务器地理信息. |
| cswbaa74.dtd5681.com | 没有服务器地理信息. |
| q4chyj.dtd5682.com | 没有服务器地理信息. |
| 4ossb3.dtd5683.com | 没有服务器地理信息. |
| bb7o11.dtd5682.com | 没有服务器地理信息. |
| hkig9whk2.dtd111.com | 没有服务器地理信息. |
| 182.92.20.189 | IP: 182.92.20.189  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ss945p.dtd5680.com | 没有服务器地理信息. |
| ss945p.dtd5681.com | 没有服务器地理信息. |
| www.jdc.com | 没有服务器地理信息. |
| dhms24.dtd5680.com | 没有服务器地理信息. |
| goy1kc.dtd5682.com | 没有服务器地理信息. |
| w7l6o6.dtd5682.com | 没有服务器地理信息. |
| i2u2wo.dtd5680.com | 没有服务器地理信息. |
| oq1si5.dtd5682.com | 没有服务器地理信息. |
| ds-app-line.obs.ap-southeast-1.myhuaweicloud.com | IP: 104.17.218.97  所属国家: United States of America  地区: California  城市: San Francisco |
| a9jwxe.dtd5681.com | 没有服务器地理信息. |
| vag0ux.dtd5680.com | 没有服务器地理信息. |
| b5d9o2.dtd5681.com | 没有服务器地理信息. |
| 12lbrt.dtd5680.com | 没有服务器地理信息. |
| developer.umeng.com | IP: 59.82.60.43  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ulogs.umengcloud.com | IP: 223.109.148.130  所属国家: China  地区: Beijing  城市: Beijing |
| 9gy29g.dtd5682.com | 没有服务器地理信息. |
| a9jwxe.dtd5680.com | 没有服务器地理信息. |
| errlogos.umeng.com | IP: 47.246.110.96  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| ouplog.umeng.com | IP: 47.246.110.93  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| goy1kc.dtd5683.com | 没有服务器地理信息. |
| oss-cn-hangzhou.aliyuncs.com | IP: 118.31.219.248  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 915uml.dtd5680.com | 没有服务器地理信息. |
| 9y6php.dtd5683.com | 没有服务器地理信息. |
| cafkaa30.dtd5681.com | 没有服务器地理信息. |
| n0t82m.dtd5682.com | 没有服务器地理信息. |
| oihvg63.dtd5681.com | 没有服务器地理信息. |
| vsjsdg13.dtd5683.com | 没有服务器地理信息. |
| 90iyue.dtd5680.com | 没有服务器地理信息. |
| vsjsdg13.dtd5681.com | 没有服务器地理信息. |
| cafkaa30.dtd5680.com | 没有服务器地理信息. |
| vghjk72.dtd5681.com | 没有服务器地理信息. |
| aqefaash2.dtd111.com | 没有服务器地理信息. |
| rh6mb3.dtd5683.com | 没有服务器地理信息. |
| 90iyue.dtd5683.com | 没有服务器地理信息. |
| bjuser.jpush.cn | IP: 122.9.15.248  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| cvghuj76.dtd5680.com | 没有服务器地理信息. |
| y0aa70.dtd5681.com | 没有服务器地理信息. |
| anfan33.dtd5683.com | 没有服务器地理信息. |
| vghjk72.dtd5683.com | 没有服务器地理信息. |
| px.ucweb.com | IP: 106.8.139.123  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| alogus.umeng.com | IP: 223.109.148.177  所属国家: China  地区: Beijing  城市: Beijing |
| claoe45.dtd5682.com | 没有服务器地理信息. |
| q4chyj.dtd5680.com | 没有服务器地理信息. |
| anfan33.dtd5681.com | 没有服务器地理信息. |
| i2u2wo.dtd5683.com | 没有服务器地理信息. |
| anfan33.dtd5682.com | 没有服务器地理信息. |
| n0t82m.dtd5680.com | 没有服务器地理信息. |
| iwg2qi.dtd5680.com | 没有服务器地理信息. |
| cnkake25.dtd5683.com | 没有服务器地理信息. |
| ds.close | 没有服务器地理信息. |
| bvfds47.dtd5683.com | 没有服务器地理信息. |
| w7l6o6.dtd5681.com | 没有服务器地理信息. |
| dhms24.dtd5681.com | 没有服务器地理信息. |
| m8bdog.dtd5682.com | 没有服务器地理信息. |
| q4chyj.dtd5681.com | 没有服务器地理信息. |
| t1jyqs.dtd5681.com | 没有服务器地理信息. |
| 4ossb3.dtd5681.com | 没有服务器地理信息. |
| dhms24.dtd5683.com | 没有服务器地理信息. |
| 9y6php.dtd5682.com | 没有服务器地理信息. |
| oihvg63.dtd5682.com | 没有服务器地理信息. |
| schemas.android.com | 没有服务器地理信息. |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://errlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/f/c.java |
| https://errlogos.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://errlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://pslog.umeng.com | com/umeng/commonsdk/vchannel/a.java |
| https://pslog.umeng.com/ | com/umeng/commonsdk/vchannel/a.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://plbslog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ouplog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| http://developer.umeng.com/docs/66650/cate/66650 | com/umeng/analytics/pro/j.java |
| https://aaid.umeng.com/api/updateZdata | com/umeng/umzid/ZIDManager.java |
| https://aaid.umeng.com/api/postZdata | com/umeng/umzid/ZIDManager.java |
| https://www.okex.com | com/fob/ds/activity/WebViewActivity.java |
| https://www.huobi.vc/zh-cn | com/fob/ds/activity/WebViewActivity.java |
| http://www.jdc.com/close | com/fob/ds/activity/JDCWebViewActivity.java |
| http://www.jdc.com/login | com/fob/ds/activity/JDCWebViewActivity.java |
| http://ds.close/ | com/fob/ds/activity/HongbaoWebViewActivity.java |
| http://ds.close/?login=1 | com/fob/ds/activity/HongbaoWebViewActivity.java |
| http://help.kg-88.net:81/#/home?tab=3&path= | com/fob/ds/activity/fragment/CommitMoneySecondUSDTFragment.java |
| https://errlogos.umeng.com/upload | com/uc/crashsdk/e.java |
| https://errlog.umeng.com/upload | com/uc/crashsdk/e.java |
| https://errlog.umeng.com/api/crashsdk/logcollect | com/uc/crashsdk/a/h.java |
| https://errlogos.umeng.com/api/crashsdk/logcollect | com/uc/crashsdk/a/h.java |
| https://px-intl.ucweb.com | com/uc/crashsdk/a/h.java |
| https://px.ucweb.com | com/uc/crashsdk/a/h.java |
| https://errlog.umeng.com | com/uc/crashsdk/a/d.java |
| https://errlogos.umeng.com | com/uc/crashsdk/a/d.java |
| https://ip. | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://image.cnamedomain.com'! | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://oss.aliyuncs.com | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://127.0.0.1 | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://image.cnamedomain.com'! | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://oss-cn-hangzhou.aliyuncs.com | com/alibaba/sdk/android/oss/common/OSSConstants.java |
| https://tsis.jpush.cn | cn/jiguang/c/a.java |
| http://182.92.20.189:9099/ | cn/jiguang/a/a/c/i.java |
| http://bjuser.jpush.cn/v1/appawake/status | cn/jiguang/d/i/c.java |
| http://schemas.android.com/apk/res/android | c/b/f/a/e/g.java |
| http://cvghuj76.dtd5680.com:80/ | d/d/a/b/b.java |
| http://cvghuj76.dtd5681.com:80/ | d/d/a/b/b.java |
| http://cvghuj76.dtd5682.com:80/ | d/d/a/b/b.java |
| https://cvghuj76.dtd5683.com:443/ | d/d/a/b/b.java |
| http://claoe45.dtd5680.com:80/ | d/d/a/b/b.java |
| http://claoe45.dtd5681.com:80/ | d/d/a/b/b.java |
| http://claoe45.dtd5682.com:80/ | d/d/a/b/b.java |
| https://claoe45.dtd5683.com:443/ | d/d/a/b/b.java |
| http://m8bdog.dtd5680.com:80/ | d/d/a/b/b.java |
| http://m8bdog.dtd5681.com:80/ | d/d/a/b/b.java |
| http://m8bdog.dtd5682.com:80/ | d/d/a/b/b.java |
| https://m8bdog.dtd5683.com:443/ | d/d/a/b/b.java |
| http://9gy29g.dtd5680.com:80/ | d/d/a/b/b.java |
| http://9gy29g.dtd5681.com:80/ | d/d/a/b/b.java |
| http://9gy29g.dtd5682.com:80/ | d/d/a/b/b.java |
| https://9gy29g.dtd5683.com:443/ | d/d/a/b/b.java |
| http://915uml.dtd5680.com:80/ | d/d/a/b/b.java |
| http://915uml.dtd5681.com:80/ | d/d/a/b/b.java |
| http://915uml.dtd5682.com:80/ | d/d/a/b/b.java |
| https://915uml.dtd5683.com:443/ | d/d/a/b/b.java |
| http://vsjsdg13.dtd5680.com:80/ | d/d/a/b/b.java |
| http://vsjsdg13.dtd5681.com:80/ | d/d/a/b/b.java |
| http://vsjsdg13.dtd5682.com:80/ | d/d/a/b/b.java |
| https://vsjsdg13.dtd5683.com:443/ | d/d/a/b/b.java |
| http://b5d9o2.dtd5680.com:80/ | d/d/a/b/b.java |
| http://b5d9o2.dtd5681.com:80/ | d/d/a/b/b.java |
| http://b5d9o2.dtd5682.com:80/ | d/d/a/b/b.java |
| https://b5d9o2.dtd5683.com:443/ | d/d/a/b/b.java |
| http://vag0ux.dtd5680.com:80/ | d/d/a/b/b.java |
| http://vag0ux.dtd5681.com:80/ | d/d/a/b/b.java |
| http://vag0ux.dtd5682.com:80/ | d/d/a/b/b.java |
| https://vag0ux.dtd5683.com:443/ | d/d/a/b/b.java |
| http://053q4d.dtd5680.com:80/ | d/d/a/b/b.java |
| http://053q4d.dtd5681.com:80/ | d/d/a/b/b.java |
| http://053q4d.dtd5682.com:80/ | d/d/a/b/b.java |
| https://053q4d.dtd5683.com:443/ | d/d/a/b/b.java |
| http://n0t82m.dtd5680.com:80/ | d/d/a/b/b.java |
| http://n0t82m.dtd5681.com:80/ | d/d/a/b/b.java |
| http://n0t82m.dtd5682.com:80/ | d/d/a/b/b.java |
| https://n0t82m.dtd5683.com:443/ | d/d/a/b/b.java |
| http://ut9iqw.dtd5680.com:80/ | d/d/a/b/b.java |
| http://ut9iqw.dtd5681.com:80/ | d/d/a/b/b.java |
| http://ut9iqw.dtd5682.com:80/ | d/d/a/b/b.java |
| https://ut9iqw.dtd5683.com:443/ | d/d/a/b/b.java |
| http://cswbaa74.dtd5680.com:80/ | d/d/a/b/b.java |
| http://cswbaa74.dtd5681.com:80/ | d/d/a/b/b.java |
| http://cswbaa74.dtd5682.com:80/ | d/d/a/b/b.java |
| https://cswbaa74.dtd5683.com:443/ | d/d/a/b/b.java |
| http://oihvg63.dtd5680.com:80/ | d/d/a/b/b.java |
| http://oihvg63.dtd5681.com:80/ | d/d/a/b/b.java |
| http://oihvg63.dtd5682.com:80/ | d/d/a/b/b.java |
| https://oihvg63.dtd5683.com:443/ | d/d/a/b/b.java |
| http://bckjsj31.dtd5680.com:80/ | d/d/a/b/b.java |
| http://bckjsj31.dtd5681.com:80/ | d/d/a/b/b.java |
| http://bckjsj31.dtd5682.com:80/ | d/d/a/b/b.java |
| https://bckjsj31.dtd5683.com:443/ | d/d/a/b/b.java |
| http://t1jyqs.dtd5680.com:80/ | d/d/a/b/b.java |
| http://t1jyqs.dtd5681.com:80/ | d/d/a/b/b.java |
| http://t1jyqs.dtd5682.com:80/ | d/d/a/b/b.java |
| https://t1jyqs.dtd5683.com:443/ | d/d/a/b/b.java |
| http://y0aa70.dtd5680.com:80/ | d/d/a/b/b.java |
| http://y0aa70.dtd5681.com:80/ | d/d/a/b/b.java |
| http://y0aa70.dtd5682.com:80/ | d/d/a/b/b.java |
| https://y0aa70.dtd5683.com:443/ | d/d/a/b/b.java |
| http://4ossb3.dtd5680.com:80/ | d/d/a/b/b.java |
| http://4ossb3.dtd5681.com:80/ | d/d/a/b/b.java |
| http://4ossb3.dtd5682.com:80/ | d/d/a/b/b.java |
| https://4ossb3.dtd5683.com:443/ | d/d/a/b/b.java |
| http://90iyue.dtd5680.com:80/ | d/d/a/b/b.java |
| http://90iyue.dtd5681.com:80/ | d/d/a/b/b.java |
| http://90iyue.dtd5682.com:80/ | d/d/a/b/b.java |
| https://90iyue.dtd5683.com:443/ | d/d/a/b/b.java |
| http://oq1si5.dtd5680.com:80/ | d/d/a/b/b.java |
| http://oq1si5.dtd5681.com:80/ | d/d/a/b/b.java |
| http://oq1si5.dtd5682.com:80/ | d/d/a/b/b.java |
| https://oq1si5.dtd5683.com:443/ | d/d/a/b/b.java |
| http://9y6php.dtd5680.com:80/ | d/d/a/b/b.java |
| http://9y6php.dtd5681.com:80/ | d/d/a/b/b.java |
| http://9y6php.dtd5682.com:80/ | d/d/a/b/b.java |
| https://9y6php.dtd5683.com:443/ | d/d/a/b/b.java |
| http://cvs341.dtd5680.com:80/ | d/d/a/b/b.java |
| http://cvs341.dtd5681.com:80/ | d/d/a/b/b.java |
| http://cvs341.dtd5682.com:80/ | d/d/a/b/b.java |
| https://cvs341.dtd5683.com:443/ | d/d/a/b/b.java |
| http://cafkaa30.dtd5680.com:80/ | d/d/a/b/b.java |
| http://cafkaa30.dtd5681.com:80/ | d/d/a/b/b.java |
| http://cafkaa30.dtd5682.com:80/ | d/d/a/b/b.java |
| https://cafkaa30.dtd5683.com:443/ | d/d/a/b/b.java |
| http://anfan33.dtd5680.com:80/ | d/d/a/b/b.java |
| http://anfan33.dtd5681.com:80/ | d/d/a/b/b.java |
| http://anfan33.dtd5682.com:80/ | d/d/a/b/b.java |
| https://anfan33.dtd5683.com:443/ | d/d/a/b/b.java |
| http://vghjk72.dtd5680.com:80/ | d/d/a/b/b.java |
| http://vghjk72.dtd5681.com:80/ | d/d/a/b/b.java |
| http://vghjk72.dtd5682.com:80/ | d/d/a/b/b.java |
| https://vghjk72.dtd5683.com:443/ | d/d/a/b/b.java |
| http://iwg2qi.dtd5680.com:80/ | d/d/a/b/b.java |
| http://iwg2qi.dtd5681.com:80/ | d/d/a/b/b.java |
| http://iwg2qi.dtd5682.com:80/ | d/d/a/b/b.java |
| https://iwg2qi.dtd5683.com:443/ | d/d/a/b/b.java |
| http://12lbrt.dtd5680.com:80/ | d/d/a/b/b.java |
| http://12lbrt.dtd5681.com:80/ | d/d/a/b/b.java |
| http://12lbrt.dtd5682.com:80/ | d/d/a/b/b.java |
| https://12lbrt.dtd5683.com:443/ | d/d/a/b/b.java |
| http://dhms24.dtd5680.com:80/ | d/d/a/b/b.java |
| http://dhms24.dtd5681.com:80/ | d/d/a/b/b.java |
| http://dhms24.dtd5682.com:80/ | d/d/a/b/b.java |
| https://dhms24.dtd5683.com:443/ | d/d/a/b/b.java |
| http://q4chyj.dtd5680.com:80/ | d/d/a/b/b.java |
| http://q4chyj.dtd5681.com:80/ | d/d/a/b/b.java |
| http://q4chyj.dtd5682.com:80/ | d/d/a/b/b.java |
| https://q4chyj.dtd5683.com:443/ | d/d/a/b/b.java |
| http://goy1kc.dtd5680.com:80/ | d/d/a/b/b.java |
| http://goy1kc.dtd5681.com:80/ | d/d/a/b/b.java |
| http://goy1kc.dtd5682.com:80/ | d/d/a/b/b.java |
| https://goy1kc.dtd5683.com:443/ | d/d/a/b/b.java |
| http://bb7o11.dtd5680.com:80/ | d/d/a/b/b.java |
| http://bb7o11.dtd5681.com:80/ | d/d/a/b/b.java |
| http://bb7o11.dtd5682.com:80/ | d/d/a/b/b.java |
| https://bb7o11.dtd5683.com:443/ | d/d/a/b/b.java |
| http://bvfds47.dtd5680.com:80/ | d/d/a/b/b.java |
| http://bvfds47.dtd5681.com:80/ | d/d/a/b/b.java |
| http://bvfds47.dtd5682.com:80/ | d/d/a/b/b.java |
| https://bvfds47.dtd5683.com:443/ | d/d/a/b/b.java |
| http://172.25.12.1:8500/ | d/d/a/b/b.java |
| http://a9jwxe.dtd5680.com:80/ | d/d/a/b/b.java |
| http://a9jwxe.dtd5681.com:80/ | d/d/a/b/b.java |
| http://a9jwxe.dtd5682.com:80/ | d/d/a/b/b.java |
| https://a9jwxe.dtd5683.com:443/ | d/d/a/b/b.java |
| http://w7l6o6.dtd5680.com:80/ | d/d/a/b/b.java |
| http://w7l6o6.dtd5681.com:80/ | d/d/a/b/b.java |
| http://w7l6o6.dtd5682.com:80/ | d/d/a/b/b.java |
| https://w7l6o6.dtd5683.com:443/ | d/d/a/b/b.java |
| http://i2u2wo.dtd5680.com:80/ | d/d/a/b/b.java |
| http://i2u2wo.dtd5681.com:80/ | d/d/a/b/b.java |
| http://i2u2wo.dtd5682.com:80/ | d/d/a/b/b.java |
| https://i2u2wo.dtd5683.com:443/ | d/d/a/b/b.java |
| http://ss945p.dtd5680.com:80/ | d/d/a/b/b.java |
| http://ss945p.dtd5681.com:80/ | d/d/a/b/b.java |
| http://ss945p.dtd5682.com:80/ | d/d/a/b/b.java |
| https://ss945p.dtd5683.com:443/ | d/d/a/b/b.java |
| http://rh6mb3.dtd5680.com:80/ | d/d/a/b/b.java |
| http://rh6mb3.dtd5681.com:80/ | d/d/a/b/b.java |
| http://rh6mb3.dtd5682.com:80/ | d/d/a/b/b.java |
| https://rh6mb3.dtd5683.com:443/ | d/d/a/b/b.java |
| http://cnkake25.dtd5680.com:80/ | d/d/a/b/b.java |
| http://cnkake25.dtd5681.com:80/ | d/d/a/b/b.java |
| http://cnkake25.dtd5682.com:80/ | d/d/a/b/b.java |
| https://cnkake25.dtd5683.com:443/ | d/d/a/b/b.java |
| http://oss-cn-shanghai.aliyuncs.com | d/d/a/h/a.java |
| http://dsapi1.ds16387.com:8500/ | d/d/a/e/d.java |
| https://hkig9whk2.dtd111.com:1443/ | d/d/a/e/d.java |
| https://aqefaash2.dtd111.com:1443/ | d/d/a/e/d.java |
| https://ds-app-line.obs.ap-southeast-1.myhuaweicloud.com/line\_ | d/d/a/e/d.java |
| http://ip.taobao.com/service/getIpInfo.php?ip=myip | d/d/a/j/k.java |
| https://errlog.umeng.com/api/crashsdk/logcollect | lib/armeabi-v7a/libcrashsdk.so |
| https://errlogos.umeng.com/api/crashsdk/logcollect | lib/armeabi-v7a/libcrashsdk.so |
| https://errlog.umeng.com | lib/armeabi-v7a/libcrashsdk.so |
| https://errlogos.umeng.com | lib/armeabi-v7a/libcrashsdk.so |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13800000000 | com/fob/ds/activity/CompleteUserDetailActivity.java |
| 13800000000 | com/fob/ds/activity/LinkBankActivity.java |

## **5. 签名证书**

**APK is signed v1 signature: True v2 signature: False v3 signature: False Found 1 unique certificates Subject: C=asd, ST=asd, L=asd, O=sadsad, OU=dasd, CN=dasdasd Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2022-02-18 03:19:59+00:00 Valid To: 2047-02-12 03:19:59+00:00 Issuer: C=asd, ST=asd, L=asd, O=sadsad, OU=dasd, CN=dasdasd Serial Number: 0x63844a4a Hash Algorithm: sha256 md5: 37d660ca9b110953e5764c397f9b5043 sha1: 072daebe58372b53c25e3e3d3d3c58d328546299 sha256: e4ade38f647a233527f3c3a4a39b889fcb538d8e5157579b424e9c5c7d5fbe8b sha512: 890c1d5a1ecb7c767139bb30c3ef593ae69b134a72941303e9fed2cfd1625b7a32227d0cd19f67215ca77c6281322a181438e3bf9c36338db9d4fe2cb44e0892**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "find\_password" : "找回密码" |
| "gesture\_password" : "手势密码" |
| "ifv\_gesture\_password" : "" |
| "mod\_password" : "修改密码" |
| "original\_password" : "原有密码" |
| "pay\_user\_name" : "入款姓名:" |
| "reg\_password" : "密码:" |
| "reg\_user\_name" : "用户名:" |
| "sure\_password" : "确认密码" |

## **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.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\_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.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 |
| com.flb.zj.omkxm.permission.JPUSH\_MESSAGE | 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 |
| 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.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| android.permission.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.ACCESS\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| 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.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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 |
| 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.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_PHONE\_STATE | 危险 | 读取电话状态和身份 | 允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等 |
| android.permission.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.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| android.permission.ACCESS\_FINE\_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| 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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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 |

## **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。**