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

**JLWCS（ 1.1.7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 | JLWCS |
| 版本 | 1.1.7 |
| 包名 | com.lq.nblg |
| 域名线索 | 23条 |
| URL线索 | 29条 |
| APP图标 |  |
| 分析日期 | 2025年10月2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 | hsjl-117-1.apk |
| 文件大小 | 59.54MB |
| MD5值 | dab2a611254670a606f6b10828a69fac |
| SHA1值 | b7005645e8edaf67a1c5f844511459e12ff7c484 |
| SHA256值 | 55ef503bf53e58c956d809fc75286bba9d38dd80d80f2019350b4c444c297ee2 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | JLWCS |
| 包名 | com.lq.nblg |
| 主活动Activity | com.unity3d.player.UnityPlayerActivity |
| 安卓版本名称 | 1.1.7 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| openmobile.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| appsupport.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| cgi.connect.qq.com | IP: 60.28.215.27 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  |
| pingma.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| android.bugly.qq.com | IP: 124.95.225.169 所属国家: China 地区: Liaoning 城市: Shenyang  |
| app.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| huatuocode.huatuo.qq.com | 没有服务器地理信息.  |
| up.sdk.mob.com | IP: 180.188.26.28 所属国家: China 地区: Zhejiang 城市: Taizhou  |
| mta.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| p.share.mob.com | 没有服务器地理信息.  |
| long.open.weixin.qq.com | IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai  |
| fusion.qq.com | IP: 116.130.228.157 所属国家: China 地区: Beijing 城市: Beijing  |
| api.utag.mob.com | 没有服务器地理信息.  |
| api.u.mob.com | 没有服务器地理信息.  |
| mta.oa.com | IP: 141.144.196.217 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam  |
| www.mob.com | IP: 180.188.26.28 所属国家: China 地区: Zhejiang 城市: Taizhou  |
| api.weixin.qq.com | IP: 116.128.170.42 所属国家: China 地区: Shanghai 城市: Shanghai  |
| rqd.uu.qq.com | IP: 60.28.219.32 所属国家: China 地区: Tianjin 城市: Tianjin  |
| open.weixin.qq.com | IP: 140.207.176.25 所属国家: China 地区: Shanghai 城市: Shanghai  |
| cgi.qplus.com | 没有服务器地理信息.  |
| qzs.qq.com | IP: 123.6.25.75 所属国家: China 地区: Henan 城市: Zhengzhou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://qzs.qq.com/open/mobile/login/qzsjump.html?sdkv=3.3.0.lite&display=mobile  | cn/sharesdk/tencent/qq/a.java  |
| http://app.qq.com/detail/com.tencent.mobileqq?autodownload=1&norecommend=1&rootvia=opensdk  | cn/sharesdk/tencent/qq/a.java  |
| https://graph.qq.com/oauth2.0/m\_authorize?response\_type=token&client\_id=  | cn/sharesdk/tencent/qq/c.java  |
| https://graph.qq.com/user/get\_simple\_userinfo  | cn/sharesdk/tencent/qq/c.java  |
| https://graph.qq.com  | cn/sharesdk/tencent/qq/c.java  |
| https://graph.qq.com/oauth2.0/m\_authorize?response\_type=token&client\_id=  | cn/sharesdk/tencent/qzone/b.java  |
| https://graph.qq.com/user/get\_simple\_userinfo  | cn/sharesdk/tencent/qzone/b.java  |
| https://graph.qq.com/photo/upload\_pic  | cn/sharesdk/tencent/qzone/b.java  |
| https://graph.qq.com  | cn/sharesdk/tencent/qzone/b.java  |
| http://p.share.mob.com/tags/getTagList  | cn/sharesdk/framework/authorize/f.java  |
| https://)  | cn/sharesdk/framework/b/a.java  |
| https://api.weixin.qq.com/sns/oauth2/access\_token  | cn/sharesdk/wechat/utils/g.java  |
| https://api.weixin.qq.com/sns/oauth2/refresh\_token  | cn/sharesdk/wechat/utils/g.java  |
| https://api.weixin.qq.com/sns/userinfo  | cn/sharesdk/wechat/utils/g.java  |
| http://api.u.mob.com  | com/mob/MobUser.java  |
| http://www.mob.com/about/policy\  | com/mob/commons/dialog/d.java  |
| http://www.mob.com/about/policy</a>  | com/mob/commons/dialog/d.java  |
| http://api.utag.mob.com/conf  | com/mob/commons/utag/TagRequester.java  |
| http://api.utag.mob.com/bdata  | com/mob/commons/utag/UserTager.java  |
| http://up.sdk.mob.com  | com/mob/commons/filesys/FileUploader.java  |
| http://rqd.uu.qq.com/rqd/sync  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| http://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.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  |
| https://graph.qq.com/cgi-bin/qunopensdk/unbind  | com/tencent/open/SocialOperation.java  |
| https://graph.qq.com/cgi-bin/qunopensdk/check\_group  | com/tencent/open/SocialOperation.java  |
| http://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf  | com/tencent/open/utils/f.java  |
| http://cgi.qplus.com/report/report  | com/tencent/open/utils/k.java  |
| https://huatuocode.huatuo.qq.com  | com/tencent/open/b/d.java  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/f.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/d.java  |
| https://graph.qq.com/oauth2.0/me  | com/tencent/connect/UnionInfo.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://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://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://mta.qq.com/  | com/tencent/wxop/stat/StatServiceImpl.java  |
| http://mta.oa.com/  | com/tencent/wxop/stat/StatServiceImpl.java  |
| http://pingma.qq.com:80/mstat/report  | com/tencent/wxop/stat/common/StatConstants.java  |
| http://www.mob.com/about/policy>http://www.mob.com/about/policy</a>  | 摸瓜V1引擎  |
| http://www.mob.com  | 摸瓜V1引擎  |
| http://www.mob.com/about/policy>http://www.mob.com/about/policy</a>.If  | 摸瓜V1引擎  |
| https://github.com/rust-lang/rust/issues/39364assertion  | lib/arm64-v8a/discord\_game\_sdk.so  |
| https://github.com/rust-lang/rust/issues/39364  | lib/arm64-v8a/discord\_game\_sdk.so  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 19222222222  | com/mob/commons/a/h.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=CN, ST=ZJ, L=HZ, O=BLKK, OU=BLKK, CN=Simon 签名算法: rsassa\_pkcs1v15 有效期自: 2022-04-25 03:50:33+00:00 有效期至: 2077-01-26 03:50:33+00:00 发行人: C=CN, ST=ZJ, L=HZ, O=BLKK, OU=BLKK, CN=Simon 序列号: 0x5a35cffd 哈希算法: sha256 md5值: 33b7664b6c80176842c4b66dd7fbf0a3 sha1值: 7552bf20e001f452abcd25129b78758786d9888e sha256值: adf7a0c19f6c9d2b53fc4003873261689fe706bc189c8bcd1c5e6d78c3587f54 sha512值: b61dac2bd46f9f887b4e5f2a543645fd3b5598811d087e8682101852b453ea8558ea56974c05191a50b341c844290e811d735c190f52395451c6328aaa1e5b98 公钥算法: rsa 密钥长度: 2048 指纹: 0ea4b471e8ea1add01e89c9dc34fefba079ba74262194143ffdc2a28c7b34be6**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "PASSWORD" : "Password"  |
| "USERNAME" : "Username"  |
| "mobcommon\_authorize\_dialog\_accept" : "接受"  |
| "mobcommon\_authorize\_dialog\_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见<a href=http://www.mob.com/about/policy>http://www.mob.com/about/policy</a>。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"  |
| "mobcommon\_authorize\_dialog\_reject" : "拒绝"  |
| "mobcommon\_authorize\_dialog\_title" : "服务授权"  |
| "mobdemo\_authorize\_dialog\_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见<a href=http://www.mob.com/about/policy>http://www.mob.com/about/policy</a>。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"  |
| "mobdemo\_authorize\_dialog\_title" : "服务授权"  |
| "ssdk\_cmcc\_auth" : "手机认证服务由中国移动提供"  |
| "ssdk\_cmcc\_login\_one\_key" : "本机号码一键登录"  |
| "ssdk\_instapaper\_pwd" : "密码"  |
| "ssdk\_weibo\_oauth\_regiseter" : "应用授权"  |
| "PASSWORD" : "암호"  |
| "USERNAME" : "사용자 이름"  |
| "mobdemo\_authorize\_dialog\_content" : "In order to provide you with Mobservice related products and services, please check our privacy policy in detail, see details<a href=http://www.mob.com/about/policy>http://www.mob.com/about/policy</a>.If you agree with our privacy policy, please click accept. If you disagree with our privacy policy, please click reject."  |
| "mobdemo\_authorize\_dialog\_title" : "service authority"  |
| "ssdk\_cmcc\_auth" : "Provided by China Mobile"  |
| "ssdk\_cmcc\_login\_one\_key" : "PhoneNum Login"  |
| "ssdk\_instapaper\_pwd" : "Password"  |
| "ssdk\_weibo\_oauth\_regiseter" : "Authorization"  |
| "PASSWORD" : "Adgangskode"  |
| "USERNAME" : "Brugernavn"  |
| "PASSWORD" : "パスワード"  |
| "USERNAME" : "ユーザー名"  |
| "PASSWORD" : "Passwort"  |
| "USERNAME" : "Nutzername"  |
| "PASSWORD" : "密码"  |
| "USERNAME" : "用户名"  |
| "PASSWORD" : "Mật khẩu"  |
| "USERNAME" : "Tên đăng nhập"  |
| "PASSWORD" : "Wachtwoord"  |
| "USERNAME" : "Gebruikersnaam"  |
| "PASSWORD" : "Mot de passe"  |
| "USERNAME" : "Nom d'utilisateur"  |
| "PASSWORD" : "Contraseña"  |
| "USERNAME" : "Nombre de usuario"  |
| "PASSWORD" : "Parola d'ordine"  |
| "USERNAME" : "Nome utente"  |
| "PASSWORD" : "Senha"  |
| "USERNAME" : "Nome de usuário"  |
| "PASSWORD" : "пароль"  |
| "USERNAME" : "имя пользователя"  |
| "PASSWORD" : "Lösenord"  |
| "USERNAME" : "Användarnamn"  |
| "PASSWORD" : "密碼"  |
| "USERNAME" : "用戶名"  |

## **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.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.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\_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.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.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。 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.unity3d.player.UnityPlayerActivity | **Schemes**: hsjl://, **Hosts:** com.lq.nblg,  |
| cn.sharesdk.tencent.qq.ReceiveActivity | **Schemes**: tencent101570008://,  |

**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。**