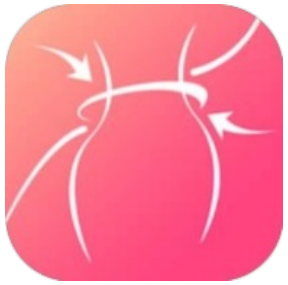
# MoGua

# 晚夕 1.0.APK 分析报告



| | |
|---|---|
| APP名称: | 晚夕 |

| | |
|---|---|
| 包名: | jvvwt.jkrbs.qjvrm.eockzh |
| 域名线索: | 7条 |
| URL线索: | 7条 |
| 邮箱线索: | 0条 |
| 分析日期: | 2025年7月17日 |
| 分析平台: | 摸瓜APK反编译平台 |

## 文件信息

**文件名**: D6A0A0488DC81A92D32D7DC4E4B3D1A6 (1).APK
**文件大小**: 16.26MB
**MD5值**: d6a0a0488dc81a92d32d7dc4e4b3d1a6
**SHA1值**: 8dab7085bf72b347fed70981991710fee7decd33
**SHA256值**: 2d74136f1390bbd37b1e4898af15796f3e8cc1cdb9a06e247399812f03f0fff2

# APP 信息

**App名称**: 晚夕
**包名**: jvvwt.jkrbs.qjvrm.eockzh
**主活动Activity**: jvvwt.jkrbs.qjvrm.eockzh.ui.home.MainActivity
**安卓版本名称**: 1.0
**安卓版本**: 1

# 域名线索

| 域名 | 服务器信息 |
| --- | --- |
| schemas.android.com | 没有服务器地理信息. |
| 118.195.132.210 | **IP**: 118.195.132.210<br>**所属国家**: China<br>**地区**: Guangxi Zhuangzu<br>**城市**: Liuzhou<br>**纬度**: 24.312729<br>**经度**: 109.389046 |
| s.sharetrace.com | **IP**: 39.98.67.122<br>**所属国家**: China<br>**地区**: Zhejiang<br>**城市**: Hangzhou<br>**纬度**: 30.293650<br>**经度**: 120.161583 |

| | |
|---|---|
| 2022.ip138.com | **IP**: 110.81.155.138<br>**所属国家**: China<br>**地区**: Fujian<br>**城市**: Quanzhou<br>**纬度**: 24.913891<br>**经度**: 118.585831 |
| pv.sohu.com | **IP**: 123.125.244.81<br>**所属国家**: China<br>**地区**: Beijing<br>**城市**: Beijing<br>**纬度**: 39.907501<br>**经度**: 116.397102 |
| api.sharetrace.com | **IP**: 39.98.67.122<br>**所属国家**: China<br>**地区**: Zhejiang<br>**城市**: Hangzhou<br>**纬度**: 30.293650<br>**经度**: 120.161583 |
| wanxi417.evgoq.cn | **IP**: 154.38.69.10<br>**所属国家**: Hong Kong<br>**地区**: Hong Kong<br>**城市**: Hong Kong<br>**纬度**: 22.285521<br>**经度**: 114.157692 |

## URL线索

| URL信息 | Url所在文件 |
|---|---|
| https://api.sharetrace.com | cn/net/shoot/sharetracesdk/c/d.java |
| http://schemas.android.com/apk/res/android | com/hjq/permissions/AndroidManifestParser.java |

| | |
|---|---|
| http://pv.sohu.com/cityjson | jvvwt/jkrbs/qjvrm/eockzh/utils/LDNetUtil.java |
| http://pv.sohu.com/cityjson?ie=utf-8 | jvvwt/jkrbs/qjvrm/eockzh/utils/LDNetUtil.java |
| https://2022.ip138.com/ | jvvwt/jkrbs/qjvrm/eockzh/utils/LDNetUtil.java |
| https://wanxi417.evgoq.cn/ | jvvwt/jkrbs/qjvrm/eockzh/base/MyApp.java |
| http://118.195.132.210:3559 | jvvwt/jkrbs/qjvrm/eockzh/http/Content.java |

# 邮箱线索

# 手机线索

| 手机号 | 所在文件 |
|---|---|
| 15555215554 | jvvwt/jkrbs/qjvrm/eockzh/utils/EmulatorCheck.java |

# 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=beijing, ST=beijing, L=beijing, O=lv1745160120436, OU=en1745160120436, CN=ltyn
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-20 14:42:02+00:00
有效期至: 2075-04-08 14:42:02+00:00
发行人: C=beijing, ST=beijing, L=beijing, O=lv1745160120436, OU=en1745160120436, CN=ltyn
序列号: 0x5f9517cb

哈希算法: sha512
md5值: 3b5553e2bfc95cfc71666a8d04e26e23
sha1值: c90e35ece62fabb86263498d2faa44e8b1a075c5
sha256值: 87bfd184eedc75f6aeb5391d68e5054e56ae7f4f4387f5e4313f18ae7182dd2b
sha512值: cf0b35f13e949c9f3104191855934d67a0fe8410a4a6a7f6fbc6d0241e180500fdeeaa18d527be642a5969e261699f049015b04ca6cc4ecb58a660adf67836c0
公钥算法: rsa
密钥长度: 4096
指纹: 34bac8d63bc5e14ca7b9d74797316cb3ff3088f3a284c32878002dde159bff6d

# 硬编码敏感信息

# 加壳分析

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 | |

# 第三方插件

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 | | |

# 此APP的危险动作

| | 是否 | | |
| --- | --- | --- | --- |

| 向手机申请的权限 | 危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| com.google.android.gms.permission.AD_ID | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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_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.READ_SMS | 危险 | 阅读短信或彩信 | 允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息 |
| android.permission.READ_CALENDAR | 危险 | 读取日历事件 | 允许应用程序读取您手机上存储的所有日历事件。恶意应用程序可以借此将您的日历事件发送给其他人 |
| android.permission.READ_CALL_LOG | 危险 |  | 允许应用程序读取用户的通话日志 |
| | | 读取联系人数 | 允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应 |

| | | | |
|---|---|---|---|
| android.permission.READ_CONTACTS | 危险 | 读取联系人数据 | 允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人 |
| 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.READ_MEDIA_IMAGES | 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.READ_MEDIA_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| jvvwt.jkrbs.qjvrm.eockzh.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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。 |

# 应用内通信