



MoGua

佳人 3.2.6.APK 分析报告



APP名称:

佳人

包名:	jriut1108.geix.com
域名线索:	16条
URL线索:	11条
邮箱线索:	0条
分析日期:	2025年8月14日
分析平台:	摸瓜APK反编译平台

文件名: 199296008_sign.apk
文件大小: 60.0MB
MD5值: 6b5cda9385aba43e266025a51fa26833
SHA1值: 60a9673e7b65bb3123ed21df6fdab2feeb262090
SHA256值: fdec63e78b0aa6d5660cf35de3d64a7a05a1032da54d3ed67e2bd01aab06f46c

i APP 信息

App名称: 佳人
包名: jriut1108.geix.com
主活动Activity: com.yunbao.phonelive.activity.LauncherActivity
安卓版本名称: 3.2.6
安卓版本: 900036

🔍 域名线索

域名	服务器信息
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
api.jd.co.th	没有服务器地理信息.
confluence.agoralab.co	IP: 123.125.46.42 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

www.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
heracles.jd.com	IP: 116.78.120.73 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
beta-api.jd.co.th	没有服务器地理信息.
uranus.jd.com	IP: 120.52.87.249 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
api.m.jd.com	IP: 120.52.83.71 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
139.224.238.21	IP: 139.224.238.21 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
	IP: 47.98.237.147 所属国家: China

api.hcharts.cn	地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
stream-outside.jd.com	IP: 211.144.27.35 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
app.xhs.cn	没有服务器地理信息.
11.50.163.13	IP: 11.50.163.13 所属国家: United States of America 地区: Ohio 城市: Columbus 纬度: 39.966381 经度: -83.012772
www.webrtc.org	IP: 172.217.14.206 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
beta-api.m.jd.com	IP: 172.18.255.235 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
www.highcharts.com	IP: 104.18.9.9 所属国家: United States of America 地区: California 城市: San Francisco

纬度: 37.775700
经度: -122.395203

URL线索

URL信息	Url所在文件
https://api.m.jd.com/api	com/jingdong/aura/sdk/update/request/c.java
https://beta-api.m.jd.com/api	com/jingdong/aura/sdk/update/request/c.java
https://beta-api.jd.co.th/api	com/jingdong/aura/sdk/update/request/c.java
https://api.jd.co.th/api	com/jingdong/aura/sdk/update/request/c.java
http://11.50.163.13:8088/microAppPlugin	com/jingdong/aura/sdk/update/request/c.java
https://heracles.jd.com/download/policy_eids/	com/jingdong/jdma/record/JDMAEngineImpl.java
https://uranus.jd.com/log/m/v2	com/jingdong/jdma/common/utils/Constant.java
https://stream-outside.jd.com/track/verify	com/jingdong/jdma/d/g.java
https://heracles.jd.com/download/policy_eids/	com/jingdong/jdma/strategy/ConfigBean.java
https://heracles.jd.com/download/policy_eids/	com/jingdong/jdma/strategy/ConfigManager.java
https://app.xhs.cn/	yu1/a.java
https://github.com/vinc3m1	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView	摸瓜V1引擎

https://github.com/vinc3m1/RoundedImageView.git	摸瓜V1引擎
https://api.hcharts.cn/highcharts	摸瓜V2引擎
https://www.highcharts.com?credits	摸瓜V2引擎
http://agoratest	lib/armeabi-v7a/libagora-rtc-sdk.so
http://139.224.238.21:9090/udrm/udrmGetLicense	lib/armeabi-v7a/libagora-rtc-sdk.so
https://confluence.agoralab.co/pages/viewpage.action?pageId=	lib/armeabi-v7a/libagora-rtc-sdk.so
https://confluence.agoralab.co/pages/viewpage.action?pageId=1161004477	lib/armeabi-v7a/libagora-rtc-sdk.so
https://confluence.agoralab.co/pages/viewpage.action?pageId=1035862602	lib/armeabi-v7a/libagora-rtc-sdk.so
http://s	lib/armeabi-v7a/libagora-rtc-sdk.so
http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor	lib/armeabi-v7a/libagora-rtc-sdk.so

 邮箱线索

 手机线索

 签名证书

无法读取代码签名证书.

 硬编码敏感信息

可能的敏感信息
"cash_input_bank_user_name": "请输入持卡人姓名"
"emotion_status_secret": "保密"
"enter_withdraw_pwd": "请输入提现密码"
"find_pwd": "找回密码"
"find_pwd_find": "立即找回"
"find_pwd_forget": "忘记密码"
"follow_author": "关注主播"
"input_payment_password": "请输入支付密码(6位纯数字)"
"library_roundedimageview_author": "Vince Mi"
"library_roundedimageview_authorWebsite": "https://github.com/vinc3m1"
"live_input_password": "请输入房间密码"
"live_set_pwd": "请设置房间密码"
"live_type_pwd": "密码房间"
"login_auth_candle": "授权取消"
"login_auth_failure": "授权失败"
"login_auth_ing": "正在授权登录"
"login_auth_success": "登录成功"

login_auth_success : 登录成功
"login_forget_pwd" : "忘记密码"
"login_input_pwd" : "请输入密码"
"main_live_type_pwd" : "密码"
"mobile_authentication" : "手机认证"
"modify_pwd" : "重置密码"
"payment_password" : "支付密码"
"phone_auth" : "手机绑定"
"promotion_user" : "用户"
"reg_input_pwd_1" : "请填写密码"
"reg_input_pwd_2" : "请确认密码"
"reg_input_pwd_3" : "邀请码(选填)"
"withdraw_pwd_str" : "提现密码"

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

向手机申请的权限	是否危险	类型	详细情况
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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
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.NETWORK_PROVIDER	未知	Unknown permission	Unknown permission from android reference
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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.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.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.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.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
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.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加和删除帐户以及删除其密码等操作
android.permission.RECEIVE_USER_PRESENT	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.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.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.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.yunbao.common.arouter.SchemeFilterActivity	Schemes: guming://, Hosts: com.guming,