MoGua

同城佳丽 1.0.0.APK 分析报告

APP名称:	同城佳丽

包名:	j5fiq.qcuec.ygy3z
域名线索:	4条
URL线索:	15条
邮箱线索:	0条
分析日期:	2025年10月9日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: tcjl.APK
文件大小: 6.91MB
MD5值: 1b63639218e5d7305d98d1a1d86718fb
SHA1值: aa15e0de66753a457da4edcf768c3d2ff82f6428
SHA256值: 2301c19b0e872c8f8f1f04e5711db5147a1caefb9ca1cb3b55f2997c8de1af31

APP 信息

App名称: 同城佳丽
包名: j5fiq.qcuec.ygy3z
主活动Activity: k54mn5.gy9u81.p4r6l1.xk2w6i
安卓版本名称: 1.0.0
安卓版本: 1

域名线索

域名	服务器信息
112.74.94.182	**IP**: 112.74.94.182 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545673 **经度**: 114.068108
www.wanandroid.com	**IP**: 39.101.178.149 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
schemas.android.com	没有服务器地理信息.
	IP: 20.205.243.166

github.com	**所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	com/rxjava/rxlife/MaybeLife.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	com/rxjava/rxlife/ObservableLife.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	com/rxjava/rxlife/CompletableLife.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	com/rxjava/rxlife/SingleLife.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	com/rxjava/rxlife/FlowableLife.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/rxjava3/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Flowable.java

https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Observable.java
http://112.74.94.182:16917/api/register	k54mn5/gy9u81/bssz5s/my__q9/uiu6cu.java
http://112.74.94.182:16917/api/uploadImgs	k54mn5/gy9u81/bssz5s/my__q9/uiu6cu.java
http://112.74.94.182:16917/api/subList	k54mn5/gy9u81/bssz5s/my__q9/uiu6cu.java
http://112.74.94.182:16917/api/subSmsList	k54mn5/gy9u81/bssz5s/my__q9/uiu6cu.java
https://www.wanandroid.com/	k54mn5/gy9u81/ejao6n/ew292o/uf2cjo.java

邮箱线索

手机线索

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=admint_6bom, ST=admint_6bom, L=admint_6bom, O=admint_6bom, OU=admint_6bom, CN=admint_6bom
签名算法: rsassa_pkcs1v15
有效期自: 2024-11-26 15:40:26+00:00
有效期至: 2124-11-02 15:40:26+00:00
发行人: C=admint_6bom, ST=admint_6bom, L=admint_6bom, O=admint_6bom, OU=admint_6bom, CN=admint_6bom
序列号: 0x5d33bbf3
哈希算法: sha256
md5值: 4e0d8bb75394dc294c43fef023d3e79e
sha1值: 177b58fbd87e3b0328721ef1819e565182c58b02

sha256值: b9c0fd67f0eb456bb5dbb052bcb7f1c0f5ab7f1d3db3f09ce43452b47ea56a40
sha512值: 84b828a801bdaa30207798a7bf7cc36b7442a28226f61f4a7945f258cab76771ffff061fc8b6afc769e0d8a4721044b7af9fb46acef8e009e5cfc0867fe0a821
公钥算法: rsa
密钥长度: 1024
指纹: 284b87a3958a2aa743163e7e72c5cfb1677f33fcdc99f1856903d1588821880c

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

向手机申请的权限	是否危险	类型	详细情况
android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低

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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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_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_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.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

应用内通信