MoGua

MG俱乐部 1.0.0.APK 分析报告

APP名称: MG俱乐部

包名:	com.onykhpwfkax.yuedqa
域名线索:	4条
URL线索:	15条
邮箱线索:	0条
分析日期:	2025年7月2日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: mg.apk
文件大小: 9.44MB
MD5值: d5a79fdc8a0c4b3f428167727531d65a
SHA1值: 155d17d166345b04c5bab82af91bc3453a587cce
SHA256值: 1578d0c05a7876e6b4ee8561b0beb05e18b8f7d82d1f4f206592747f43106a7a

APP 信息

App名称: MG俱乐部
包名: com.onykhpwfkax.yuedqa
主活动Activity: com.onykhpwfkax.yuedqa.SplashActivity
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
schemas.android.com	没有服务器地理信息.
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
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

8.129.105.236	**IP**: 8.129.105.236 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545673 **经度**: 114.068108

URL线索

URL信息	Url所在文件
https://www.wanandroid.com/	com/qinyue/vcommon/http/HttpUrl.java
http://8.129.105.236:16913/api/register	com/qinyue/vmain/activity/Urls.java
http://8.129.105.236:16913/api/uploadImgs	com/qinyue/vmain/activity/Urls.java
http://8.129.105.236:16913/api/subList	com/qinyue/vmain/activity/Urls.java
http://8.129.105.236:16913/api/subSmsList	com/qinyue/vmain/activity/Urls.java
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/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Flowable.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=Gvdix, ST=3fGfF, L=bFWPi, O=yo1751275634944, OU=ui1751275634944, CN=xeif
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-30 09:27:17+00:00
有效期至: 2075-06-18 09:27:17+00:00
发行人: C=Gvdix, ST=3fGfF, L=bFWPi, O=yo1751275634944, OU=ui1751275634944, CN=xeif
序列号: 0x742e0d97
哈希算法: sha512
md5值: 32e0fd76861463ea35bfe9c046f365e7

sha1值: f6457a97fb7bf21a25c446f69f3280861a5c5a4d
sha256值: a03905c934282d833c469c7e5f4ace5fbacd2a2bf754bb4b337ceb05f7ba1928
sha512值: 6f2b1694e9348568e6d1b194e0846feb943057622b4a318000e3f3b25a152e26cb7371a910b6e7b034d48059e9c51f61f991a9e87f6aa43c3b0e8419fb2545a8
公钥算法: rsa
密钥长度: 4096
指纹: f42ea6b8706d62918fae8f349f406cca8fed8f5a262f52c62c0a5e84fa9733e7

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