MoGua

撸管社 2.4.8.1.APK 分析报告

APP名称: 撸管社

包名:	newabv.luguanshe.singiwkk.zkzhyw
域名线索:	23条
URL线索:	35条
邮箱线索:	2条
分析日期:	2025年4月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: renamed_lgshhtry.apk
文件大小: 9.22MB
MD5值: ade98e0e3e4ad8e513d9bfab4d2e29f4
SHA1值: 10cc66ec329119560e0ea79249110b2bfce1cc3d
SHA256值: 8dc950befa99417e60b07f5c66305bbcd382d13c50dd78e6249f6fdbde2041aa

APP 信息

App名称: 撸管社
包名: newabv.luguanshe.singiwkk.zkzhyw
主活动Activity: com.hqzx.hqzxdetail.activity.SplashActivity
安卓版本名称: 2.4.8.1
安卓版本: 9

域名线索

域名	服务器信息
crapi.fhhxu.cn	**IP**: 137.220.252.6 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
xml.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
debugx5.qq.com	**IP**: 60.29.240.122 **所属国家**: China **地区**: Tianjin

	城市: Tianjin **纬度**: 39.142181 **经度**: 117.176102
aaid.umeng.com	**IP**: 223.109.148.139 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
127.0.0.1	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
ulogs.umengcloud.com	**IP**: 223.109.148.141 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
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
alogsus.umeng.com	**IP**: 223.109.148.130 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992

yingshi.shop	**IP**: 45.85.77.129 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
aria.laoyuyu.me	没有服务器地理信息.
ouplog.umeng.com	**IP**: 47.246.110.93 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
schemas.android.com	没有服务器地理信息.
pslog.umeng.com	**IP**: 59.82.60.44 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
mdc.html5.qq.com	**IP**: 116.130.223.178 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
debugtbs.qq.com	**IP**: 60.29.240.122 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102

alogus.umeng.com	**IP**: 223.109.148.141 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
cfg.imtt.qq.com	**IP**: 60.29.240.17 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
plbslog.umeng.com	**IP**: 36.156.202.73 **所属国家**: China **地区**: Jiangsu **城市**: Yangzhou **纬度**: 32.397221 **经度**: 119.435600
developer.umeng.com	**IP**: 59.82.31.154 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
tbs.imtt.qq.com	**IP**: 119.188.149.164 **所属国家**: China **地区**: Shandong **城市**: Jinan **纬度**: 36.668331 **经度**: 116.997223
ulogs.umeng.com	**IP**: 223.109.148.141 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing

	纬度: 32.061668 **经度**: 118.777992
log.tbs.qq.com	**IP**: 124.95.224.248 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
pms.mb.qq.com	**IP**: 60.28.172.238 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102

URL线索

URL信息	Url所在文件
https://aria.laoyuyu.me/aria_doc/create/any_java.html	com/arialyy/aria/core/Aria.java
https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/download/DownloadReceiver.java
https://github.com/AriaLyy/Aria/issues/597	com/arialyy/aria/core/download/m3u8/M3U8Option.java
https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/upload/UploadReceiver.java
http://xml.apache.org/xslt	com/apkfuns/logutils/Logger.java
https://github.com/danikula/AndroidVideoCache/issues/88.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues/43.	com/danikula/videocache/HttpUrlSource.java

https://github.com/danikula/AndroidVideoCache/issues.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues/134.	com/danikula/videocache/Pinger.java
http://%s:%d/%s	com/danikula/videocache/Pinger.java
http://%s:%d/%s	com/danikula/videocache/HttpProxyCacheServer.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/PermissionUtils.java
https://yingshi.shop/	com/hqzx/hqzxdetail/http/Config.java
http://127.0.0.1:8080	com/hqzx/hqzxdetail/activity/FullVideoActivity.java
https://crapi.fhhxu.cn	com/hqzx/hqzxdetail/app/App.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SegmentTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SlidingTabLayout.java
https://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugtbs.qq.com?10000\	com/tencent/smtt/sdk/WebView.java
https://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/k.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/stat/MttLoader.java

https://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/o.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/o.java
https://tbs.imtt.qq.com/plugin/DebugPlugin_v2.tbs	com/tencent/smtt/utils/d.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/j.java
https://ulogs.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://developer.umeng.com/docs/119267/detail/182050	com/umeng/commonsdk/debug/UMLogCommon.java
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.java

https://aaid.umeng.com/api/updateZdata	com/umeng/umzid/ZIDManager.java
https://aaid.umeng.com/api/postZdata	com/umeng/umzid/ZIDManager.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	com/danikula/videocache/HttpUrlSource.java
x5tbs@tencent.com	com/tencent/smtt/sdk/X5Downloader.java

手机线索

签名证书

APK已签名
v1 签名: False
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=Jiangsu, ST=IeReechoht, L=AiQuo, O=Uphohwa, OU=nohCohwe, CN=shohxeRi
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-07 09:04:31+00:00
有效期至: 2125-03-14 09:04:31+00:00
发行人: C=Jiangsu, ST=IeReechoht, L=AiQuo, O=Uphohwa, OU=nohCohwe, CN=shohxeRi
序列号: 0x18bbded7
哈希算法: sha512
md5值: 0df3e4f7508be0c923d7ee4f8338c48d
sha1值: 9a3b48f30ff1a84a6bb3d4f8fe584fb75dbfef68
sha256值: 763292ab526880d14e90e3a6b42333120b209a00d9248ae66b880791c23f7fc2
sha512值: 96a7dddb7be8941dbd641d7e68e72e5529fa0ab33349d15a303a2fe65afdad80197761e6667248fd172ce2dd92ac888269fe51e856e5be8f6e5e43de6b5863df
公钥算法: rsa
密钥长度: 2048
指纹: 021d0f1dd85b9e63ed6b0393c5ab08062ae520ec5712211ced7cc1310ef75dab

硬编码敏感信息

可能的敏感信息
"seach_key" : "搜索 影片、动漫、电视剧"

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.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.READ_PRIVILEGED_PHONE_STATE	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.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.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。

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.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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.hqzx.hqzxdetail.activity.SplashActivity	Schemes: aab1yl://,