MoGua

若惜追剧 1.3.2.APK 分析报告

APP名称:	若惜追剧

包名:	cn.fangchan.fanzan.ruoxizj
域名线索:	8条
URL线索:	4条
邮箱线索:	0条
分析日期:	2025年7月4日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 若惜追剧1.3.2.apk
文件大小: 76.39MB
MD5值: 04b7457e4ac83db6afa4be3381a9da6f
SHA1值: 9b1165a583e04d5bfa14fa953cd39ebef5a42de8
SHA256值: eb12b5dda56f60130566adfc5e7f34eba30050ff74f61ba0c15912de23bdab46

APP 信息

App名称: 若惜追剧
包名: cn.fangchan.fanzan.ruoxizj
主活动Activity: cn.fangchan.fanzan.ruoxizj.MainActivity
安卓版本名称: 1.3.2
安卓版本: 29

域名线索

域名	服务器信息
grs.dbankcloud.cn	**IP**: 49.4.40.185 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
journeyapps.com	**IP**: 18.155.68.4 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
www.jsdelivr.com	**IP**: 104.21.23.24 **所属国家**: United States of America **地区**: California

	城市: San Francisco **纬度**: 37.775700 **经度**: -122.395203
developer.mozilla.org	**IP**: 34.111.97.67 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
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
grs.dbankcloud.eu	没有服务器地理信息.
grs.dbankcloud.com	**IP**: 113.201.107.54 **所属国家**: China **地区**: Shaanxi **城市**: Baoji **纬度**: 34.353611 **经度**: 107.375275
grs.dbankcloud.asia	**IP**: 49.4.40.185 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572

URL线索

URL信息	Url所在文件
https://journeyapps.com/	Mogua Engine V1
https://github.com/journeyapps/zxing-android-embedded	Mogua Engine V1
https://grs.dbankcloud.com	Mogua Engine V2
https://grs.dbankcloud.cn	Mogua Engine V2
https://grs.dbankcloud.eu	Mogua Engine V2
https://grs.dbankcloud.asia	Mogua Engine V2
https://www.jsdelivr.com/using-sri-with-dynamic-files	Mogua Engine V2
https://github.com/apvarun/toastify-js	Mogua Engine V2
https://github.com/richtr/NoSleep.js/issues/15	Mogua Engine V2
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)	Mogua Engine V2

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=cn, ST=zj, L=hz, O=sjm, OU=sjm, CN=sjm
签名算法: rsassa_pkcs1v15
有效期自: 2022-07-11 06:41:41+00:00
有效期至: 2122-06-17 06:41:41+00:00
发行人: C=cn, ST=zj, L=hz, O=sjm, OU=sjm, CN=sjm
序列号: 0x3cad6f27
哈希算法: sha256
md5值: 84498af2969a3f28fa38c9a04ffa0626
sha1值: 8d916f8db81b15b95053d524f8e03be9a5d34477
sha256值: 6257a544a6fe91de9f29c4609a0783a2c6f4c08b7b712c79bbdfd79ab1006916
sha512值: a6da76ce84dca2c1a38fa4afe5b23b04c717f64751b54ad8e403b24ac58f6783e00300105cba30dee391048ceb34c48ebc66ea8f831fe8b65221a981c4c089b6
公钥算法: rsa
密钥长度: 2048
指纹: 671369764ebc117c0789449ee545b37b637cb4f672aa949dd10d3aba27637347

🔑 硬编码敏感信息

可能的敏感信息
"anythink_myoffer_feedback_violation_of_laws" : "Illegal"
"dyStrategy.privateAddress" : "privateAddress"
"ksad_ad_default_author" : "@可爱的广告君创造的原声"
"ksad_ad_default_username" : "@可爱的广告君"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"anythink_myoffer_feedback_violation_of_laws" : "违规违法"

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.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.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.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.GET_SIGNATURES	未知	Unknown permission	Unknown permission from android reference
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.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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.USE_FULL_SCREEN_INTENT	正常		针对想要使用通知全屏意图的 Build.VERSION_CODES.Q 的应用程序是必需的
android.permission.SCHEDULE_EXACT_ALARM	正		允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作

	常		
android.permission.POST_NOTIFICATIONS	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
cn.fangchan.fanzan.ruoxizj.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_DELETE_PACKAGES	正常		允许应用程序请求删除包
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
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.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.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.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.ACCESS_FINE_LOCATION	危	精细定位	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

	险	（GPS）	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.SET_WALLPAPER	正常	设置壁纸	允许应用程序设置系统壁纸
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
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
cn.fangchan.fanzan.ruoxizj.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
cn.fangchan.fanzan.ruoxizj.MainActivity	Schemes: rxzj://, Hosts: app,
com.qubianym.activityComm.SchemeActivity	

	Schemes: cn.fangchan.fanzan.ruoxizj.qubianym.novel://,
