MoGua

小红书 7.53.0.APK 分析报告

APP名称: 小红书

包名:	com.xingin.xhs
域名线索:	11条
URL线索:	2条
邮箱线索:	2条
分析日期:	2024年9月10日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 2_af0c61849f6cf19ff7fd52af192ef598.apk
文件大小: 109.8MB
MD5值: 6e30041897c16e17864c12c9d9e5904b
SHA1值: 7f75715857a4024fe2341529b25b58476a56f53c
SHA256值: e3fa23c7a7a6ae8b0bba00090c158b92b3d65fc7011702eca624f28c8f33fdab

APP 信息

App名称: 小红书
包名: com.xingin.xhs
主活动Activity: com.xingin.xhs.index.v2.IndexActivityV2
安卓版本名称: 7.53.0
安卓版本: 7530239

域名线索

域名	服务器信息
play.google.com	**IP**: 142.251.43.14 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
upload.ffmpeg.org	**IP**: 213.36.253.119 **所属国家**: France **地区**: Ile-de-France **城市**: Paris **纬度**: 48.853409 **经度**: 2.348800
store-at-dre.hispace.dbankcloud.com	**IP**: 80.158.5.6 **所属国家**: Germany **地区**: Schleswig-Holstein

	城市: Kiel **纬度**: 54.321331 **经度**: 10.134890
e.189.cn	IP: 42.123.76.65 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
wap.cmpassport.com	IP: 120.197.235.27 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
sns-video-hw.xhscdn.com	IP: 123.151.96.28 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142220 **经度**: 117.176666
www.sharesdk.cn	IP: 115.227.41.64 **所属国家**: China **地区**: Zhejiang **城市**: Taizhou **纬度**: 28.666668 **经度**: 121.349998
store.hispace.hicloud.com	IP: 49.4.44.164 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232

www.xiaohongshu.com	**IP**: 212.64.115.101 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
opencloud.wostore.cn	**IP**: 116.128.209.136 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.222219 **经度**: 121.458061
appgallery.cloud.huawei.com	**IP**: 117.78.15.51 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000

URL线索

URL**信息**	Url**所在文件**
https://www.xiaohongshu.com/crown/community/advanced_agreement?fullscreen=true	Android String Resource
http://sns-video-hw.xhscdn.com/351ad9a64564b75ec82eb668fd7344832208c188.mp4?v=2	Android String Resource
https://play.google.com/store	Android String Resource
https://appgallery.cloud.huawei.com/app/	Android String Resource
https://play.google.com/store/apps/details?id=	Android String Resource

https://appgallery.cloud.huawei.com	Android String Resource
https://wap.cmpassport.com/resources/html/contract.html	Android String Resource
https://e.189.cn/sdk/agreement/detail.do?hidetop=true	Android String Resource
https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true	Android String Resource
http://www.xiaohongshu.com/crown/community/terms	Android String Resource
http://www.xiaohongshu.com/crown/community/privacy	Android String Resource
https://www.xiaohongshu.com/privacy/teenager	Android String Resource
www.xiaohongshu.com/content_dispute	Android String Resource
http://www.xiaohongshu.com/mobile/terms	Android String Resource
http://www.xiaohongshu.com/mobile/privacy	Android String Resource
http://www.sharesdk.cn	Android String Resource
https://store-at-dre.hispace.dbankcloud.com/hwmarket/api/	Android String Resource
https://store.hispace.hicloud.com/hwmarket/api/	Android String Resource
ftp://upload.ffmpeg.org/incoming/	lib/armeabi-v7a/libswdecoder.so

邮箱线索

邮箱地址	所在文件

qinquan@xiaohongshu.com	Android String Resource
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libswdecoder.so

手机线索

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=86, ST=shanghai, L=shanghai, O=xingin, OU=xingin, CN=xiaohongshu
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-07-16 08:32:34+00:00
Valid To: 2039-07-10 08:32:34+00:00
Issuer: C=86, ST=shanghai, L=shanghai, O=xingin, OU=xingin, CN=xiaohongshu
Serial Number: 0x53c638a2
Hash Algorithm: sha1
md5: 6cfca61d9d1eca56844806706ba18cf7
sha1: 4ae949b443ed2e33b71f024af9ef24ff14f2e4d0
sha256: f375f0f6af7c94c364b35cd6f6a66d64aefae66e32f935b48773c0faad04c121
sha512: eeadeb0436099c9fa25e9c21b546a7a94d3261f91ecddf75a0b3f8b8688d51fd13bdcb918cf72f1d2900ed3ce73884471bce5668307532f52359e5ea4a729633
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: ec7382d5768d97b472ac44689b5abcaf4f5a122e0144f3a1b70ec1066d30a09b

硬编码敏感信息

可能的敏感信息
"api" : "价格优惠"

"aws" : "微博"

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_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.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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定
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.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。
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.READ_SETTINGS	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.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_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.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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
com.xingin.xhs.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.xingin.xhs.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.xingin.xhs.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference

com.xingin.xhs.permission.JPUSH_MESSAGE	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。
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章
com.huawei.android.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章
android.permission.EXPAND_STATUS_BAR	正常	展开/折叠状态栏	允许应用程序展开或折叠状态栏
getui.permission.GetuiService.com.xingin.xhs	未知	Unknown permission	Unknown permission from android reference
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。

android.permission.WRITE_CALENDAR	危险	添加或修改日历事件并向客人发送电子邮件	允许应用程序添加或更改日历上的事件,这可能会向客人发送电子邮件。恶意应用程序可以使用它来删除或修改您的日历活动或向客人发送电子邮件
android.permission.SCHEDULE_EXACT_ALARM	正常		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
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_CALENDAR	危险	读取日历事件	允许应用程序读取您手机上存储的所有日历事件。恶意应用程序可以借此将您的日历事件发送给其他人
com.huawei.meetime.CAAS_SHARE_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
android.permission.SET_WALLPAPER	正常	设置壁纸	允许应用程序设置系统壁纸
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
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

com.xingin.xhs.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.xingin.xhs.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.permission.PUSH	未知	Unknown permission	Unknown permission from android reference
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.android.vending.CHECK_LICENSE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.xingin.xhs.routers.RouterPageActivity	Schemes: xhsdiscover://, http://, https://, qnpr8hbhw393f9://, Hosts: login_page, welcome_page, store, messages, interaction_notification, profile, webview, extweb, rn, swan, miniapp, wechat_miniprogram, home, discovery, 1, item, multi_note, video_feed, note_mix, guang, topic, homefeed, comments, portrait_feed, post, post_video_album, post_video, post_note, notes_draft_box, post_new_note, recommend, me, user, message, red_house, face_photo, ar_skin_detection, search, page, instore_search, poi, spv, spu, spv_skeleton, spl, spv_draft, *.xiaohongshu.com, choose_share_user, splashshow, advert, pm, list, scenario, account, pois, general_setting, dark_mode_setting, notification_setting, report, system_settings, callback, resource_cache_manage, board, live_audience, hey, hey_post, hey_edit, hey_home_feed, Mime Types: image/*, video/*, Paths: /follow, /explore, /localfeed, /note, /store, /user, /contacts, /weibo, /profile, /my, /center, /collections, /comments, /followers, /notifications, /room, /room_list, /room_feed, /room_inner_feed, /schedule_room, /recommend, /result, /goods_category, /native_template_landingpage, /chat, /strangers, /groupchat, /login, /bind, /bind/phone,

	Path Patterns: /.*, /item/.*, /category, /user/.*, /.*/collects, /me/collects, /.*/followers, /me/followers, .*, /goods/.*, /list/.*, /report/.*, /board/.*,
com.xingin.xhs.push.VIVOPushEmptyActivity	Schemes: xhsdiscover://, Hosts: push, Paths: /vivopush,
com.xingin.hey.heyshoot.HeyEditActivity	Schemes: @string/c93://, Hosts: @string/c72,
com.tencent.tauth.AuthActivity	Schemes: tencent100507190://,
com.alibaba.baichuan.android.trade.ui.AlibcBackActivity	Schemes: alisdk://,

---