MoGua

Pornhub中文版 2.5.1.APK 分析报告

APP名称:	Pornhub中文版

包名:	vip.zhkih.glsyvq
域名线索:	13条
URL线索:	18条
邮箱线索:	1条
分析日期:	2025年6月15日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: pzhan_2.5.1_250610_7.apk

文件大小: 19.51MB
MD5值: 7b6d791e8b0fd3a8b5639dd2cdb278e8
SHA1值: 0da65839841747ba434d39d0cca7c6fa16bed0db
SHA256值: acec687c03284b2af97cb78ebdc485f00cdae9499d1d320af65fcab2e156f00b

APP 信息

App名称: Pornhub中文版
包名: vip.zhkih.glsyvq
主活动Activity:
安卓版本名称: 2.5.1
安卓版本: 251

域名线索

域名	服务器信息
schemas.microsoft.com	**IP**: 13.107.246.74 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
exoplayer.dev	**IP**: 185.199.110.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
www.w3.org	**IP**: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco

	纬度: 37.775700 **经度**: -122.395203
ns.adobe.com	没有服务器地理信息.
api.login.yahoo.com	IP: 74.6.160.138 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.731323 **经度**: -73.990089
dashif.org	IP: 185.199.110.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
lwor9w7x.oowxazq.xyz	IP: 154.207.77.38 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
schemas.android.com	没有服务器地理信息.
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
cfg.flurry.com	IP: 69.147.80.12 **所属国家**: United States of America **地区**: New York **城市**: New York City

	纬度: 40.731323 **经度**: -73.990089
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
data.flurry.com	没有服务器地理信息.
www.example.com	IP: 23.220.70.166 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322

URL线索

URL**信息**	Url**所在文件**
https://github.com/danikula/AndroidVideoCache/issues/88.	c/d/a/i.java
https://github.com/danikula/AndroidVideoCache/issues/43.	c/d/a/i.java
https://github.com/danikula/AndroidVideoCache/issues.	c/d/a/i.java
http://%s:%d/%s	c/d/a/k.java
https://github.com/danikula/AndroidVideoCache/issues/134.	c/d/a/k.java
http://%s:%d/%s	c/d/a/g.java

https://exoplayer.dev/issues/player-accessed-on-wrong-thread	c/g/a/a/i2.java
http://dashif.org/guidelines/trickmode	c/g/a/a/z2/u0/f.java
http://dashif.org/guidelines/last-segment-number	c/g/a/a/z2/u0/m/d.java
http://dashif.org/guidelines/trickmode	c/g/a/a/z2/u0/m/d.java
https://x</LA_URL>	c/g/a/a/s2/i0.java
https://x	c/g/a/a/s2/i0.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	c/g/a/a/s2/j0.java
http://ns.adobe.com/xap/1.0/	c/g/a/a/u2/h0/a.java
https://lwor9w7x.oowxazq.xyz/api.php,https://cbvhd7w.oowxazq.xyz/api.php	c/o/a/n/e1.java
http://127.0.0.1:%d%s	c/l/a/i/a.java
http://www.example.com	com/flurry/sdk/ed.java
https://cfg.flurry.com/sdk/v1/config	com/flurry/sdk/cl.java
https://cfg.flurry.com/sdk/v1/config	com/flurry/sdk/by.java
https://data.flurry.com/v1/flr.do	com/flurry/sdk/br.java
https://api.login.yahoo.com/oauth2/device_session	com/flurry/sdk/ef.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/PermissionUtils.java
https://github.com/vinc3m1	摸瓜V1引擎

https://github.com/vinc3m1/RoundedImageView	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView.git	摸瓜V1引擎

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	c/d/a/i.java

手机线索

手机号	所在文件
17512775099	c/g/b/c/a.java
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=Singapore, ST=Singapore, L=Singapore, O=., OU=., CN=.
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-10 23:38:02+00:00
有效期至: 2026-06-10 23:38:02+00:00

发行人: C=Singapore, ST=Singapore, L=Singapore, O=., OU=., CN=.
序列号: 0x18904164
哈希算法: sha256
md5值: 96f7030ab926b77dbeffa549e14bdffd
sha1值: 2b902dfe09453d2643c4e8b6c52b3046dfe82cf3
sha256值: a7a8ffca1d64530e5bea2e11d2d09dae1a577ec3ae264e4b444f0c8aa4efe5a5
sha512值: 132edbc170448c40685469125237e5150c7a6d8c38a22a89d587ce3e5b9032e8087e79c006f32a764fb488faf817e1eacf14951d0e95608f77427ffbfc1d8eba
公钥算法: rsa
密钥长度: 2048
指纹: d3e67c4b3f672e089588ee0645b56c0aad98adf0a47985fbc6fcb7ecaf760914

硬编码敏感信息

可能的敏感信息
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"str_auth_apply" : "原创博主申请"
"str_input_account_user_name" : "请输入持卡人姓名"
"str_mod_pwd" : "修改密码"
"str_mod_pwd_success" : "密码修改成功"
"str_official_auth" : "官方认证"
"str_up_auth" : "博主"

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.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.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.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_CLIPBOARD_IN_BACKGROUND	未知	Unknown permission	Unknown permission from android reference
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.WRITE_CLIPBOARD	未知	Unknown permission	Unknown permission from android reference
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
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.WRITE_MEDIA_STORAGE	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。
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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
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.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

应用内通信
