MoGua

抖音免费版 1.0.5.APK 分析报告

APP名称:	抖音免费版

包名:	com.frlHr.erqVa
域名线索:	8条
URL线索:	7条
邮箱线索:	1条
分析日期:	2025年6月21日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 抖音免费版.apk
文件大小: 25.31MB
MD5值: f08cf537896c40d311647b62f837930f
SHA1值: d387fe7cd31b105f897531b33743c4a2df40b8b0
SHA256值: fb2fd08eb41b5b87c29caa863ccbc56e6bf0a27c2ae4033937fdfd32e2a98f37

APP 信息

App名称: 抖音免费版
包名: com.frlHr.erqVa
主活动Activity: com.frlHr.erqVa.MainActivity
安卓版本名称: 1.0.5
安卓版本: 1

域名线索

域名	服务器信息
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
www.jsdelivr.com	**IP**: 172.67.208.113 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
journeyapps.com	**IP**: 18.65.168.85 **所属国家**: Japan **地区**: Tokyo

	城市: Tokyo **纬度**: 35.689499 **经度**: 139.692322
www.w3.org	**IP**: 104.18.22.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
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
dartbug.com	**IP**: 216.239.32.21 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
picsum.photos	**IP**: 104.26.4.30 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
api.flutter.dev	**IP**: 199.36.158.100 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514

URL线索

URL信息	Url所在文件
https://journeyapps.com/	摸瓜V1引擎
https://github.com/journeyapps/zxing-android-embedded	摸瓜V1引擎
https://picsum.photos/200/200?random=1	摸瓜V2引擎
https://picsum.photos/167/300	摸瓜V2引擎
https://picsum.photos/200/200?random=2	摸瓜V2引擎
https://picsum.photos/200/200?random=3	摸瓜V2引擎
https://picsum.photos/200/200?random=4	摸瓜V2引擎
https://picsum.photos/200/200?random=5	摸瓜V2引擎
https://picsum.photos/200/200?random=6	摸瓜V2引擎
https://picsum.photos/200/200?random=7	摸瓜V2引擎
https://picsum.photos/200/200?random=8	摸瓜V2引擎
https://picsum.photos/200/200?random=9	摸瓜V2引擎
https://picsum.photos/200/200?random=10	摸瓜V2引擎
https://picsum.photos/200/200?random=11	摸瓜V2引擎
https://www.jsdelivr.com/using-sri-with-dynamic-files	摸瓜V2引擎

https://github.com/apvarun/toastify-js	摸瓜V2引擎
https://github.com/richtr/NoSleep.js/issues/15	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)	摸瓜V2引擎
https://github.com/nodeca/pica	摸瓜V2引擎
https://github.com/flutter/flutter/issues.	lib/arm64-v8a/libflutter.so
https://dartbug.com/52121.	lib/arm64-v8a/libflutter.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/arm64-v8a/libapp.so

邮箱线索

邮箱地址	所在文件
appro@openssl.org	lib/arm64-v8a/libflutter.so

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='中国', ST='北京', L='北京', O='北京', OU='北京', CN='中国'
签名算法: rsassa_pkcs1v15
有效期自: 2025-02-13 04:17:11+00:00
有效期至: 2035-02-11 04:17:11+00:00
发行人: C='中国', ST='北京', L='北京', O='北京', OU='北京', CN='中国'
序列号: 0xa112d485c36401ff
哈希算法: sha256
md5值: d3973942a738264195622c1f720ba3df
sha1值: 1fb614d41a10f3d44dcadb367d6e143280579387
sha256值: 36c9ee12307bd792d8b6315b86b093d5f92031876f25b5ed976c384a78361767
sha512值: dd558a40df9d6a0bf85a74bd99551379f32596ee55542f51ce7d081aea4d9473caa55bab73ac52ecdfb4c747344cf0b13b71b91dd075e6e69adf39dfd959a261
公钥算法: rsa
密钥长度: 2048
指纹: 05fe2406fb609620139dcce094b26cbf5c0264e055344100f44897c70bea3b51

硬编码敏感信息

可能的敏感信息
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

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.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.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_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference

android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
com.frlHr.erqVa.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
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.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.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

应用内通信