MoGua

昆仑大模型 1.0.1.APK 分析报告

APP名称: 昆仑大模型

包名:	com.cnpc.kllm.android
域名线索:	16条
URL线索:	11条
邮箱线索:	2条
分析日期:	2025年6月17日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: kunlun-app.apk
文件大小: 45.61MB
MD5值: 6e0609bee954bf8d6414fe9f53a71a3a
SHA1值: ba96033cbee7be4f066090a912c65089a6f6669d
SHA256值: dc5ea7abf68fb28d75998fabbf5a853b38740f74f1fcac8da1cdf7bc21beeb2e

APP 信息

App名称: 昆仑大模型
包名: com.cnpc.kllm.android
主活动Activity: vue.activity.Activity_Welcom
安卓版本名称: 1.0.1
安卓版本: 102

域名线索

域名	服务器信息
ricostacruz.com	**IP**: 104.21.70.75 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
lea.verou.me	**IP**: 3.33.186.135 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199
opensource.org	**IP**: 172.67.26.198 **所属国家**: United States of America **地区**: California

	城市: San Francisco **纬度**: 37.775700 **经度**: -122.395203
npms.io	IP: 104.21.48.1 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
hertzen.com	IP: 172.67.140.170 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
newclient.map.baidu.com	IP: 111.206.209.17 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
lodash.com	IP: 52.220.155.145 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
html2canvas.hertzen.com	IP: 104.21.65.51 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

lexical.dev	**IP**: 76.76.21.22 **所属国家**: United States of America **地区**: California **城市**: Walnut **纬度**: 34.015400 **经度**: -117.858223
vuejs.org	**IP**: 3.33.186.135 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199
client.map.baidu.com	**IP**: 111.206.209.119 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
expert.kunlungpt.cn	**IP**: 36.140.170.129 **所属国家**: China **地区**: Gansu **城市**: Lanzhou **纬度**: 36.056690 **经度**: 103.792221
underscorejs.org	**IP**: 104.21.25.112 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
openjsf.org	**IP**: 76.76.21.21 **所属国家**: United States of America **地区**: California **城市**: Walnut

	纬度: 34.015400 **经度**: -117.858223
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
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

URL线索

URL信息	Url所在文件
https://expert.kunlungpt.cn	摸瓜V2引擎
https://github.com/uuidjs/uuid	摸瓜V2引擎
https://expert.kunlungpt.cn/app/subapp-carlife/detail/index?tag=hotel	摸瓜V2引擎
https://expert.kunlungpt.cn/app/subapp-carlife/detail/index	摸瓜V2引擎
https://vuejs.org/error-reference/	摸瓜V2引擎
https://github.com/Tencent/vConsole)	摸瓜V2引擎
http://opensource.org/licenses/MIT	摸瓜V2引擎

https://github.com/zloirock/core-js/blob/v3.21.1/LICENSE	摸瓜V2引擎
https://github.com/zloirock/core-js	摸瓜V2引擎
https://github.com/highlightjs/highlight.js/issues/2277	摸瓜V2引擎
https://github.com/highlightjs/highlight.js/wiki/security	摸瓜V2引擎
https://html2canvas.hertzen.com>	摸瓜V2引擎
https://hertzen.com>	摸瓜V2引擎
https://lodash.com/>	摸瓜V2引擎
https://openjsf.org/>	摸瓜V2引擎
https://lodash.com/license>	摸瓜V2引擎
http://underscorejs.org/LICENSE>	摸瓜V2引擎
https://npms.io/search?q=ponyfill.	摸瓜V2引擎
https://expert.kunlungpt.cn/api/chat/conversation/streamChat	摸瓜V2引擎
https://expert.kunlungpt.cn/api	摸瓜V2引擎
https://github.com/ecomfe/zrender/blob/master/LICENSE.txt	摸瓜V2引擎
https://expert.kunlungpt.cn/expert-chat/hotspot-detail	摸瓜V2引擎
https://expert.kunlungpt.cn/expert-chat/hotspot	摸瓜V2引擎
https://vuejs.org/error-reference/	摸瓜V2引擎
http://ricostacruz.com/nprogress	摸瓜V2引擎

http://ncostacruz.com/nprogress	摸瓜V2引擎
https://expert.kunlungpt.cn/api	摸瓜V2引擎
https://expert.kunlungpt.cn/expert-chat/hotspot	摸瓜V2引擎
https://expert.kunlungpt.cn/expert-chat/hotspot-detail	摸瓜V2引擎
https://lexical.dev/docs/error?$	摸瓜V2引擎
https://opensource.org/licenses/MIT>	摸瓜V2引擎
https://lea.verou.me>	摸瓜V2引擎
https://$	摸瓜V2引擎
https://newclient.map.baidu.com/client/	lib/armeabi-v7a/libaime.so
https://client.map.baidu.com/	lib/armeabi-v7a/libaime.so

邮箱线索

邮箱地址	所在文件
您可以通过邮箱kunlungpx@petrochina.com 请通过邮箱kunlungpx@petrochina.com 您可通过邮箱kunlungpx@petrochina.com 官方邮箱为kunlungpx@petrochina.com kunlungpx@petrochina.com 联系邮箱kunlungpx@petrochina.com 可以随时联系邮箱kunlungpx@petrochina.com	摸瓜V2引擎
ftp@example.com	lib/armeabi-v7a/libcurl.so

手机线索

手机号	所在文件
17657828125	摸瓜V2引擎
19760984375	摸瓜V2引擎
17192984375	摸瓜V2引擎
18006671875	摸瓜V2引擎
17448515625	摸瓜V2引擎
17516515625	摸瓜V2引擎

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=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=kllm, CN=kllm
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-16 02:27:25+00:00
有效期至: 2052-09-01 02:27:25+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=kllm, CN=kllm
序列号: 0xe4c098f6f52a79af
哈希算法: sha256
md5值: 38dcbd54fe16160599d95f6dbae7db75
sha1值: d11e2b4b7291c35e4be03116effec7f839b7978b

sha256值: 79a326156d83a8457eea182d39f3ef77c68cdc7e87cf5a18169911e2eacd714b
sha512值: aade9fac50ba3fd6a27acb9d7d18abae5fa4c3bfa8e9749cec4e014ac3a803e08d7add9200c865e2756b624b759a2f9fe2ae05be9058e5c652c5a1cbdaf5e448
公钥算法: rsa
密钥长度: 2048
指纹: b7af245f7a14d82f1d65598dfa7104a3082bd95306d5161a69dab60ac1728065

硬编码敏感信息

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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.USE_FINGERPRINT	正常	allow use of指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
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.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.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
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.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_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.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.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
android.permission.SMS	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
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_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
com.android.launcher.permission.READ_SETTINGS	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.ACCES_MOCK_LOCATION	未知	Unknown permission	Unknown permission from android reference
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_GPS	未知	Unknown permission	Unknown permission from android reference
	危	检索正在运行的应用	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

android.permission.GET_TASKS	险	程序	恶意应用程序发现有关其他应用程序的私人信息
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
andrnetwork_security_configoid.permission.MODIFY_AUDIO_SETTINGS	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
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.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小
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_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
org.simalliance.openmobileapi.SMARTCARD	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.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
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。

android.permission.RECEIVE_USER_PRESENT	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.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
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.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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.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.ACCESS_MEDIA_LOCATION	危险	访问的任何地理位置	允许应用程序访问的任何地理位置持久保存在用户的共享集合
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	未知	Unknown permission	Unknown permission from android reference
cn.com.cnpc.ulink.permission.private_communicate	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NOTIFICATION_POLICY	正常		希望访问通知策略的应用程序的标记权限。
com.cnpc.kllm.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
vue.activity.Activity_Welcom	Schemes: jumpjiangxiapp://, Hosts: jump,
com.tencent.tauth.AuthActivity	Schemes: tencent1108003460://,

---