MoGua

KK牛店 29.APK 分析报告

APP名称:	KK牛店

包名:	com.pnijcvw.fxyabdp
域名线索:	6条
URL线索:	17条
邮箱线索:	0条
分析日期:	2025年1月9日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: b3abb42cc947ec61(1).apk
文件大小: 49.03MB
MD5值: b22f5405775b8645621220849464e457
SHA1值: 47d42ad31727cd35fc8690a858042cbccbce8cb3
SHA256值: 1fb22309b5c49362cc170e8cfe79a877b58f59909dce17e330be106d25f7302a

APP 信息

App名称: KK牛店
包名: com.pnijcvw.fxyabdp
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 29
安卓版本: 1

域名线索

域名	服务器信息
schemas.android.com	没有服务器地理信息.
ask.dcloud.net.cn	**IP**: 221.204.43.211 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
m3w.cn	**IP**: 119.188.150.187 **所属国家**: China **地区**: Shandong **城市**: Jinan **纬度**: 36.668331 **经度**: 116.997223

er.dcloud.io	没有服务器地理信息.
ns.adobe.com	没有服务器地理信息.
er.dcloud.net.cn	IP: 43.142.57.168 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/283	io/dcloud/feature/utsplugin/ProxyModule.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/e/b/a.java

https://ask.dcloud.net.cn/article/35877	io/dcloud/e/b/a.java
https://er.dcloud.io/rv	io/dcloud/e/c/h/c.java
https://er.dcloud.net.cn/rv	io/dcloud/e/c/h/c.java
https://ask.dcloud.net.cn/article/283	io/dcloud/g/b.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java

邮箱线索

手机线索

手机号	所在文件
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: True

找到 1 个唯一证书
主题: CN=rodepk.com, OU=dev, O=ukywl, L=SZ, ST=GD, C=CN
签名算法: rsassa_pkcs1v15
有效期自: 2025-01-08 15:00:40+00:00
有效期至: 2124-12-15 15:00:40+00:00
发行人: CN=rodepk.com, OU=dev, O=ukywl, L=SZ, ST=GD, C=CN
序列号: 0x4a36218ae9e9b5d4
哈希算法: sha384
md5值: 3a996ca9fb30e314dfcbfff9b903ddbd
sha1值: 5e61895b9833946b803cec0f3944297a7b103bbc
sha256值: 77a732a09a22f8b1589ad9fa1c895203a0816411b0bbda83a7855c9722f97617
sha512值: fcb2e431b14b4d7348b21a67d7d6af3ab779b858ebc981d9e00a7411dfa936f17ed0391422be32ad605047edc32e5fd4db142a10ff987a7a4dfaf24525a85859
公钥算法: rsa
密钥长度: 2048
指纹: bb6aa9f0167b46d954561e6f759e258f924cf200b5cc94193fd1abd0428b7cc1

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.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_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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_IMAGES	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.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
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.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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.CALL_PRIVILEGED	系统需要	直接拨打任何电话号码	允许应用程序拨打任何电话号码,包括紧急电话号码,而无需您的干预。恶意应用程序可能会向紧急服务发出不必要和非法的呼叫
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_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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器

应用内通信