



MoGua

西乌智慧人大 1.6.25.APK 分析报告



APP名称:

西乌智慧人大

包名:	com.xiwu.renda
域名线索:	27条
URL线索:	48条
邮箱线索:	0条
分析日期:	2025年7月9日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: xwrd.apk

文件大小: 41.44MB
MD5值: ea31290296c61e1d9ab6c6e149e1534c
SHA1值: faeba5db9d85db72b654da20b51e015d152b9b16
SHA256值: 3d3f98b12e92c02e8e2ff3c8b827f0849c498a1d308898e56b8c95fc6b444399

i APP 信息

App名称: 西乌智慧人大
包名: com.xiwu.renda
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.6.25
安卓版本: 1625

🔍 域名线索

域名	服务器信息
long.open.weixin.qq.com	IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
m5.amap.com	IP: 106.11.35.98 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
restsdk.amap.com	IP: 59.82.132.217 所属国家: China 地区: Zhejiang 城市: Hangzhou

	纬度: 30.293650 经度: 120.161583
mpsapi.amap.com	IP: 59.82.112.213 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
yuntuapi.amap.com	没有服务器地理信息.
ns.adobe.com	没有服务器地理信息.
mst01.is.autonavi.com	IP: 110.253.189.211 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
dualstack-arestapi.amap.com	IP: 59.82.132.217 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
apilocate.amap.com	IP: 106.11.43.81 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
schemas.android.com	没有服务器地理信息.
	IP: 123.125.244.31 所属国家: China

ask.dcloud.net.cn	地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
m3w.cn	IP: 116.136.15.191 所属国家: China 地区: Nei Mongol 城市: Hohhot 纬度: 40.810650 经度: 111.650665
lbs.amap.com	IP: 110.253.188.148 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
er.dcloud.io	没有服务器地理信息.
lbs-3dtiles-service.amap.com	IP: 110.253.189.211 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
er.dcloud.net.cn	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
wb.amap.com	IP: 110.253.189.211 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024

	经度: 114.879349
open.weixin.qq.com	IP: 116.128.171.214 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
abroad.apilocate.amap.com	IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
wap.amap.com	IP: 116.142.235.233 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
apiinit.amap.com	IP: 59.82.132.217 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
adiu.amap.com	IP: 110.253.188.147 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
	IP: 59.82.133.102 所属国家: China

apistore.amap.com	地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
cgicol.amap.com	IP: 110.253.188.147 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
wprd0d.is.autonavi.com	没有服务器地理信息.
dualstack-a.apilocate.amap.com	IP: 59.82.31.183 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
restapi.amap.com	IP: 59.82.132.217 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583

 URL线索

URL信息	Url所在文件
https://adiu.amap.com/ws/device/adius	com/emap/api/col/p0003sl/ku.java
http://apiinit.amap.com/v3/log/init	com/emap/api/col/p0003sl/ij.java

http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&	com/amap/api/col/p0003sl/mp.java
http://restsdk.amap.com/v3	com/amap/api/col/p0003sl/fp.java
https://restsdk.amap.com/v3	com/amap/api/col/p0003sl/fp.java
http://restsdk.amap.com/v4	com/amap/api/col/p0003sl/fp.java
https://restsdk.amap.com/v4	com/amap/api/col/p0003sl/fp.java
http://restsdk.amap.com/v5	com/amap/api/col/p0003sl/fp.java
https://restsdk.amap.com/v5	com/amap/api/col/p0003sl/fp.java
http://yuntuapi.amap.com	com/amap/api/col/p0003sl/fp.java
https://yuntuapi.amap.com	com/amap/api/col/p0003sl/fp.java
http://restsdk.amap.com/rest/me/cpoint	com/amap/api/col/p0003sl/fp.java
https://restsdk.amap.com/rest/me/cpoint	com/amap/api/col/p0003sl/fp.java
http://apistore.amap.com	com/amap/api/col/p0003sl/fp.java
https://apistore.amap.com	com/amap/api/col/p0003sl/fp.java
http://m5.amap.com/ws/mapapi/shortaddress/transform	com/amap/api/col/p0003sl/fp.java
https://m5.amap.com/ws/mapapi/shortaddress/transform	com/amap/api/col/p0003sl/fp.java
https://restsdk.amap.com/v3/iasdkauth	com/amap/api/col/p0003sl/ii.java
https://dualstack-arestapi.amap.com/v3/iasdkauth	com/amap/api/col/p0003sl/ii.java
https://restsdk.amap.com/sdk/compliance/params	com/amap/api/col/p0003sl/ke.java

http://restsdk.amap.com/sdk/compliance/params	com/amap/api/col/p0003sl/ke.java
http://restsdk.amap.com	com/amap/api/col/p0003sl/is.java
http://restsdk.amap.com/v3/place/text?	com/amap/api/col/p0003sl/a.java
http://restsdk.amap.com/v3/place/around?	com/amap/api/col/p0003sl/a.java
http://restsdk.amap.com/v3/config/district?	com/amap/api/col/p0003sl/a.java
https://restapi.amap.com/rest/aaid/get	com/amap/api/col/p0003sl/jc.java
http://restapi.amap.com/rest/aaid/get	com/amap/api/col/p0003sl/jc.java
http://restsdk.amap.com/v4/graspoad/driving?	com/amap/api/col/p0003sl/ic.java
http://restsdk.amap.com/v4/gridmap?	com/amap/api/col/p0003sl/dg.java
http://wprd0%d.is.autonavi.com/appmaptile?	com/amap/api/col/p0003sl/df.java
http://restsdk.amap.com/v4/gridmap?	com/amap/api/col/p0003sl/df.java
http://restsdk.amap.com/v4	com/amap/api/col/p0003sl/t.java
http://restsdk.amap.com/v4	com/amap/api/col/p0003sl/cs.java
http://restsdk.amap.com	com/amap/api/col/p0003sl/w.java
http://wb.amap.com/? r=%f,%f,%s,%f,%f,%s,%d,%d,%d,%s,%s,%s&sourceapplication=openapi/0	com/amap/api/col/p0003sl/hw.java
http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0	com/amap/api/col/p0003sl/hw.java
http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0	com/amap/api/col/p0003sl/hw.java

http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0	com/amap/api/col/p0003sl/hw.java
http://mpsapi.amap.com/ws/mps/lyrdata/ugc/\	com/amap/api/col/p0003sl/m.java
https://restapi.amap.com/rest/lbs/geohub/3d/tiles?z=%d&x=%d&y=%d&id=	com/amap/api/col/p0003sl/l.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/	com/amap/api/location/AMapLocation.java
http://wap.amap.com/	com/amap/api/maps/AMapUtils.java
https://lbs-3dtiles-service.amap.com/basemap/tiles/staging? compose=building@1669011850923&compose=tree@1668678765481&z=%d&x=%d&y=%d	com/amap/api/maps/model/AMap3dmodeltile/AMap3DModelTileProvider.java
http://apilocate.amap.com/mobile/binary	com/autonavi/aps/AMapapi/Utils/b.java
http://dualstack-a.apilocate.amap.com/mobile/binary	com/autonavi/aps/AMapapi/Utils/b.java
http://abroad.apilocate.amap.com/mobile/binary	com/autonavi/aps/AMapapi/Utils/b.java
http://abroad.apilocate.amap.com/mobile/binary	com/autonavi/aps/AMapapi/Utils/h.java
http://abroad.apilocate.amap.com/mobile/binary	com/autonavi/aps/AMapapi/trans/a.java
http://dualstack-arestapi.amap.com/v3/geocode/regeo	com/autonavi/aps/AMapapi/trans/c.java
http://restsdk.amap.com/v3/geocode/regeo	com/autonavi/aps/AMapapi/trans/c.java
http://restsdk.amap.com/rest/lbs/dem/data?z=%d&x=%d&y=%d&type=2	com/autonavi/base/ae/gmap/TerrainOverlayProvider.java
http://mst01.is.autonavi.com/appmaptile? z=%d&x=%d&y=%d&lang=zh_cn&size=1&scale=1&style=6	com/autonavi/base/ae/gmap/TerrainOverlayProvider.java
http://mpsapi.amap.com/	com/autonavi/base/ae/gmap/GLMapEngine.java
http://m5.amap.com/	com/autonavi/base/ae/gmap/GLMapEngine.java

http://m5.amap.com/	com/autonavi/base/emap/mapcore/maploader/AMapLoader.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.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/283	io/dcloud/feature/utsplugin/ProxyModule.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/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
http://lbs.amap.com/api/android-sdk/guide/error/	io/dcloud/js/map/emap/adapter/AMapLink.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/p/r.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/p/r.java
https://ask.dcloud.net.cn/article/283	io/dcloud/p/h1.java
https://er.dcloud.io/rv	io/dcloud/p/d0.java
https://er.dcloud.net.cn/rv	io/dcloud/p/d0.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: False
找到 1 个唯一证书
主题: C=中国, ST=山东, L=济南, O=山东文津信息科技有限公司, OU=山东文津信息科技有限公司, CN=山东文津信息科技有限公司
签名算法: rsassa_pkcs1v15
有效期自: 2020-12-05 02:19:43+00:00
有效期至: 2120-11-11 02:19:43+00:00
发行人: C=中国, ST=山东, L=济南, O=山东文津信息科技有限公司, OU=山东文津信息科技有限公司, CN=山东文津信息科技有限公司
序列号: 0x737f5da9
哈希算法: sha256
md5值: ff738966a1315f1117eac9ae7f60ac18
sha1值: 9ac76627903b3efd55aa29455958f32771408f87

sha256值: abd6d8c0d42af6db367e4ed59682c92a96f9273b60d9ea8aebfc8a8bd4f4febe

sha512值: 4b192e698a178e5a8ce7d1405828ec9f998d2519e39b42d62270827ccd69c0b1c23b55b194845a13b2bceab985e4eb54d4363f96b0dfc9941c456e671bea1bdc

公钥算法: rsa

密钥长度: 2048

指纹: 1b7a01360d3565a4a17ff2594d0c152613bc0625f85739fc7dc596bec22bc6

 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.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
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
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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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

com.xiwu.renda.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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.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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
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.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.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
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.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.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

应用内通信