MoGua

享坐车-导览屏 1.0.196.APK 分析报告

APP名称: 享坐车-导览屏

包名:	net.jhcampus.youche
域名线索:	25条
URL线索:	45条
邮箱线索:	0条
分析日期:	2025年4月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: youche_196.apk
文件大小: 13.39MB
MD5值: d3fe8fbb73da87d603cfdc047a17e646
SHA1值: f8bb1b134c3f59956eb6734a0c2d71f671ad71e9
SHA256值: e1b49c1e3286281e0d807cd9c619d9fa1df0f3c050e899321ac4e5eb4803955c

APP 信息

App名称: 享坐车-导览屏
包名: net.jhcampus.youche
主活动Activity: net.jhcampus.youche.activity.StartActivity
安卓版本名称: 1.0.196
安卓版本: 196

域名线索

域名	服务器信息
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
aps.testing.amap.com	**IP**: 59.82.57.200 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
stg-gs.jhcampus.cn	**IP**: 47.106.106.151 **所属国家**: China **地区**: Guangdong

	城市: Shenzhen **纬度**: 22.545673 **经度**: 114.068108
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
lbs.amap.com	IP: 110.253.189.212 **所属国家**: China **地区**: Hebei **城市**: Zhangjiakou **纬度**: 40.810024 **经度**: 114.879349
android.bugly.qq.com	IP: 124.95.225.146 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
astat.bugly.cros.wr.pvp.net	IP: 170.106.118.26 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
www.slf4j.org	IP: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000

wap.amap.com	**IP**: 116.142.235.227 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
restapi.amap.com	**IP**: 106.11.43.113 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
astat.bugly.qcloud.com	**IP**: 119.28.121.133 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
wprd0d.is.autonavi.com	没有服务器地理信息.
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
apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
javax.xml.xmlconstants	没有服务器地理信息.

apiinit.amap.com	**IP**: 106.11.43.113 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
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
dualstack-restapi.amap.com	**IP**: 106.11.43.113 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
tsapi.amap.com	**IP**: 203.119.191.210 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052570 **经度**: -118.243904
api.jhcampus.cn	**IP**: 120.79.180.99 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
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
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
youche.jhcampus.net	**IP**: 47.106.227.203 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545673 **经度**: 114.068108
h.trace.qq.com	**IP**: 113.56.189.162 **所属国家**: China **地区**: Hubei **城市**: Huangshi **纬度**: 30.204170 **经度**: 115.077606
dualstack.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

URL线索

URL**信息**	Url**所在文件**
https://adiu.amap.com/ws/device/adius	com/amap/api/col/n3/or.java

http://apilocate.amap.com/mobile/binary	com/amap/api/col/n3/rx.java
http://restapi.amap.com	com/amap/api/col/n3/mq.java
http://restapi.amap.com/v3/assistant/inputtips?	com/amap/api/col/n3/kh.java
http://restapi.amap.com/v4/stats/alitts	com/amap/api/col/n3/jg.java
http://restapi.amap.com/v4/grasproad/driving?	com/amap/api/col/n3/mc.java
https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection	com/amap/api/col/n3/sc.java
http://apiinit.amap.com/v3/log/init	com/amap/api/col/n3/mj.java
https://restapi.amap.com/v3/iasdkauth	com/amap/api/col/n3/mi.java
http://restapi.amap.com/v3/iasdkauth	com/amap/api/col/n3/mi.java
http://restapi.amap.com/v3	com/amap/api/col/n3/km.java
https://restapi.amap.com/v3	com/amap/api/col/n3/km.java
http://restapi.amap.com/v4	com/amap/api/col/n3/bu.java
http://restapi.amap.com	com/amap/api/col/n3/hw.java
http://wprd0%d.is.autonavi.com/appmaptile?	com/amap/api/col/n3/ge.java
http://restapi.amap.com/v4/gridmap?	com/amap/api/col/n3/ge.java
http://restapi.amap.com/v4	com/amap/api/col/n3/fq.java
http://restapi.amap.com/v4/direction/bicycling	com/amap/api/col/n3/jf.java
http://restapi.amap.com/v3/direction/walking	com/amap/api/col/n3/jh.java

http://restapi.amap.com/v4/direction/bicycling	com/amap/api/col/n3/ih.java
http://restapi.amap.com	com/amap/api/col/n3/ih.java
http://restapi.amap.com/v3/direction/walking	com/amap/api/col/n3/ii.java
http://restapi.amap.com	com/amap/api/col/n3/ii.java
http://restapi.amap.com/v4/gateway	com/amap/api/col/n3/ht.java
http://restapi.amap.com/v3/ae8/driving	com/amap/api/col/n3/ht.java
http://tsapi.amap.com/v1/route/pickup/driving	com/amap/api/col/n3/ht.java
http://tsapi.amap.com/v1/route/trip/driving	com/amap/api/col/n3/ht.java
http://restapi.amap.com/v3/ae8/route/count	com/amap/api/col/n3/ht.java
http://restapi.amap.com/v3/ae8/route/offline/report	com/amap/api/col/n3/ht.java
http://restapi.amap.com/v4/escort/upload	com/amap/api/col/n3/ht.java
http://restapi.amap.com/v4/escort/stop	com/amap/api/col/n3/ht.java
http://restapi.amap.com/v3/ae8/intersection/enlarged	com/amap/api/col/n3/ht.java
http://restapi.amap.com/opennavi/tunnel	com/amap/api/col/n3/ht.java
http://restapi.amap.com/v3/ae8/traffic/show	com/amap/api/col/n3/ht.java
http://mpsapi.amap.com//ws/mps/lyrdata/ugc/\	com/amap/api/col/n3/bn.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
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/	com/autonavi/amap/mapcore/Inner_3dMap_location.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/amap/mapcore/maploader/AMapLoader.java
http://javax.xml.XMLConstants/feature/secure-processing	com/fasterxml/jackson/databind/ext/DOMDeserializer.java
http://apache.org/xml/features/disallow-doctype-decl	com/fasterxml/jackson/databind/ext/DOMDeserializer.java
http://apache.org/xml/features/nonvalidating/load-external-dtd	com/fasterxml/jackson/databind/ext/DOMDeserializer.java
http://javax.xml.XMLConstants/feature/secure-processing	com/fasterxml/jackson/databind/ext/DOMSerializer.java
https://adiu.amap.com/ws/device/adius	com/loc/av.java
http://aps.testing.amap.com/collection/collectData?src=baseCol&ver=v74&	com/loc/cf.java
http://apilocate.amap.com/mobile/binary	com/loc/en.java
http://dualstack.apilocate.amap.com/mobile/binary	com/loc/en.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/en.java
http://restapi.amap.com	com/loc/s.java
http://restapi.amap.com/v3/place/text?	com/loc/a.java
http://restapi.amap.com/v3/config/district?	com/loc/a.java
http://restapi.amap.com/v3/place/around?	com/loc/a.java

http://abroad.apilocate.amap.com/mobile/binary	com/loc/er.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/eg.java
http://dualstack-restapi.amap.com/v3/geocode/regeo	com/loc/ei.java
http://restapi.amap.com/v3/geocode/regeo	com/loc/ei.java
https://restapi.amap.com/v3/iasdkauth	com/loc/l.java
http://restapi.amap.com/v3/iasdkauth	com/loc/l.java
https://h.trace.qq.com/kv	com/tencent/bugly/proguard/ad.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/proguard/ac.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/proguard/ac.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://youche.jhcampus.net/api/version/newDriverVersion?device_id=	net/jhcampus/youche/MainActivity.java
https://youche.jhcampus.net/api/bus/busLine	net/jhcampus/youche/utils/AppConfig.java
https://youche.jhcampus.net/api/bus/busLineList	net/jhcampus/youche/utils/AppConfig.java
https://youche.jhcampus.net/api/bus/changeBusLine	net/jhcampus/youche/utils/AppConfig.java
https://api.jhcampus.cn/	net/jhcampus/youche/utils/AppConfig.java
https://stg-gs.jhcampus.cn/	net/jhcampus/youche/utils/AppConfig.java
https://youche.jhcampus.net/api/version/newDriverVersion	net/jhcampus/youche/utils/AppConfig.java

https://youche.jhcampus.net/api/version/postDeviceInfo	net/jhcampus/youche/utils/AppConfig.java
https://youche.jhcampus.net/api/broadcast/playTips?	net/jhcampus/youche/utils/AppConfig.java
https://youche.jhcampus.net/api/school/schoolType	net/jhcampus/youche/utils/AppConfig.java
https://youche.jhcampus.net/api/bus/spareCode	net/jhcampus/youche/utils/AppConfig.java
https://youche.jhcampus.net/api/bus/sumDistance	net/jhcampus/youche/utils/AppConfig.java
https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection	org/java_websocket/AbstractWebSocket.java
http://www.slf4j.org/codes.html	org/slf4j/MDC.java
http://www.slf4j.org/codes.html	org/slf4j/LoggerFactory.java

邮箱线索

手机线索

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=86, ST=guizhou, L=guiyang, O=jhcampus, OU=jhcampus, CN=jhcampus
签名算法: rsassa_pkcs1v15
有效期自: 2020-02-12 08:47:38+00:00
有效期至: 2045-02-05 08:47:38+00:00
发行人: C=86, ST=guizhou, L=guiyang, O=jhcampus, OU=jhcampus, CN=jhcampus

序列号: 0x1438041a
哈希算法: sha256
md5值: 119feeab3dd8058124db8ad38ed04f7b
sha1值: 5c8c7481acae4109b5fab88df43451540b004ab9
sha256值: 0a8467ea00b1e0b306e3168c24d1d4cebc02269d1e74a1cc2eac2099e754d34e
sha512值: 8602ba2cbda874e39d2a9db4ff42fc71b96f3a9ad8fdc2a054b6c8596d4db9f4251c76e6674682f71e8729a46e98a584db86ab938cd8aacbaded4cfd26db44a2
公钥算法: rsa
密钥长度: 2048
指纹: 4cd87157c356d08a05606b13efe4a926a32e5f25c5cf78827e8dd541edf9663c

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

	是		

向手机申请的权限	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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
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.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_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_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.NETWORK_PROVIDER	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.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.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.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.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_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.intent.action.BOOT_COMPLETED	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
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.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_DOWNLOAD_MANAGER	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.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.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.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.BLUETOOTH_CONNECT	未知	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH_SCAN	未知	Unknown permission	Unknown permission from android reference

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.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.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

应用内通信
