Evaluation Warning: The document was created with Spire.Doc for Python.

**PortalDev（ 2.0.6.r86.8ed0978版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | PortalDev |
| 版本 | 2.0.6.r86.8ed0978 |
| 包名 | moe.fuqiuluo.portaldev |
| 域名线索 | 22条 |
| URL线索 | 34条 |
| APP图标 |  |
| 分析日期 | 2025年6月8日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | base.apk |
| 文件大小 | 43.25MB |
| MD5值 | b5f9d21c0d2ea5d64201211309e79623 |
| SHA1值 | 7f747cf518bbad92d57f6156ce4900039c870d73 |
| SHA256值 | 12fed4c1cfacd7eccb9c8a15d8d37a212a9ab2621e74f7fa4088df1b56cafdb4 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | PortalDev |
| 包名 | moe.fuqiuluo.portaldev |
| 主活动Activity | moe.fuqiuluo.portaldev.MainActivity |
| 安卓版本名称 | 2.0.6.r86.8ed0978 |
| 安卓版本 | 1745784436 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| apilocate.amap.com | IP: 59.82.31.183 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| docs.swmansion.com | IP: 104.21.27.136 所属国家: United States of America 地区: California 城市: San Francisco  |
| cgicol.amap.com | IP: 110.253.189.212 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| abroad.apilocate.amap.com | IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai  |
| restsdk.amap.com | IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| restapi.amap.com | IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| wap.amap.com | IP: 116.136.186.234 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| adiu.amap.com | IP: 110.253.189.211 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| lbs.amap.com | IP: 110.253.189.211 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| dualstack-arestapi.amap.com | IP: 59.82.132.217 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| lbs-3dtiles-service.amap.com | IP: 110.253.188.147 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| mpsapi.amap.com | IP: 203.119.169.143 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| m5.amap.com | IP: 106.11.43.74 所属国家: China 地区: Beijing 城市: Beijing  |
| wb.amap.com | IP: 110.253.189.212 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| 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  |
| apistore.amap.com | IP: 203.119.238.84 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| yuntuapi.amap.com | 没有服务器地理信息.  |
| render.amap.com | IP: 203.119.204.137 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| apiinit.amap.com | IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mst01.is.autonavi.com | IP: 110.253.188.147 所属国家: China 地区: Hebei 城市: Zhangjiakou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://adiu.amap.com/ws/device/adius  | com/amap/api/col/p0003sl/kq.java  |
| http://apiinit.amap.com/v3/log/init  | com/amap/api/col/p0003sl/il.java  |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&  | com/amap/api/col/p0003sl/mk.java  |
| http://restsdk.amap.com/v3  | com/amap/api/col/p0003sl/fr.java  |
| https://restsdk.amap.com/v3  | com/amap/api/col/p0003sl/fr.java  |
| http://restsdk.amap.com/v4  | com/amap/api/col/p0003sl/fr.java  |
| https://restsdk.amap.com/v4  | com/amap/api/col/p0003sl/fr.java  |
| http://restsdk.amap.com/v5  | com/amap/api/col/p0003sl/fr.java  |
| https://restsdk.amap.com/v5  | com/amap/api/col/p0003sl/fr.java  |
| http://yuntuapi.amap.com  | com/amap/api/col/p0003sl/fr.java  |
| https://yuntuapi.amap.com  | com/amap/api/col/p0003sl/fr.java  |
| http://restsdk.amap.com/rest/me/cpoint  | com/amap/api/col/p0003sl/fr.java  |
| https://restsdk.amap.com/rest/me/cpoint  | com/amap/api/col/p0003sl/fr.java  |
| http://apistore.amap.com  | com/amap/api/col/p0003sl/fr.java  |
| https://apistore.amap.com  | com/amap/api/col/p0003sl/fr.java  |
| http://m5.amap.com/ws/mapapi/shortaddress/transform  | com/amap/api/col/p0003sl/fr.java  |
| https://m5.amap.com/ws/mapapi/shortaddress/transform  | com/amap/api/col/p0003sl/fr.java  |
| https://restsdk.amap.com/v3/iasdkauth  | com/amap/api/col/p0003sl/ik.java  |
| https://dualstack-arestapi.amap.com/v3/iasdkauth  | com/amap/api/col/p0003sl/ik.java  |
| https://restsdk.amap.com/sdk/compliance/params  | com/amap/api/col/p0003sl/ka.java  |
| http://restsdk.amap.com/sdk/compliance/params  | com/amap/api/col/p0003sl/ka.java  |
| http://restsdk.amap.com  | com/amap/api/col/p0003sl/iu.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  |
| http://restsdk.amap.com/v4/grasproad/driving?  | com/amap/api/col/p0003sl/ie.java  |
| http://restsdk.amap.com/v4/gridmap?  | com/amap/api/col/p0003sl/dh.java  |
| http://restsdk.amap.com/v4  | com/amap/api/col/p0003sl/u.java  |
| http://wprd0%d.is.autonavi.com/appmaptile?  | com/amap/api/col/p0003sl/dg.java  |
| http://restsdk.amap.com/v4/gridmap?  | com/amap/api/col/p0003sl/dg.java  |
| http://restsdk.amap.com/v4  | com/amap/api/col/p0003sl/ct.java  |
| http://restsdk.amap.com  | com/amap/api/col/p0003sl/x.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/hy.java  |
| http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0  | com/amap/api/col/p0003sl/hy.java  |
| http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0  | com/amap/api/col/p0003sl/hy.java  |
| http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0  | com/amap/api/col/p0003sl/hy.java  |
| http://restsdk.amap.com  | com/amap/api/col/p0003sl/s.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://mpsapi.amap.com/ws/mps/lyrdata/ugc/\  | com/amap/api/col/p0003sl/m.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://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/  | com/amap/api/location/AMapLocation.java  |
| http://apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/c.java  |
| http://dualstack-a.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/c.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/c.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/i.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://render.amap.com/  | com/autonavi/base/ae/gmap/GLMapEngine.java  |
| http://mpsapi.amap.com/  | com/autonavi/base/amap/mapcore/maploader/AMapLoader.java  |
| http://m5.amap.com  | com/autonavi/base/amap/mapcore/maploader/AMapLoader.java  |
| http://render.amap.com/  | com/autonavi/base/amap/mapcore/maploader/AMapLoader.java  |
| http://restsdk.amap.com/  | com/autonavi/base/amap/mapcore/maploader/AMapLoader.java  |
| https://github.com/software-mansion/react-native-screens/issues/17  | com/swmansion/rnscreens/ScreenFragment.java  |
| https://github.com/software-mansion/react-native-screens/issues  | com/swmansion/rnscreens/InsetsObserverProxy.java  |
| https://github.com/software-mansion/react-native-screens/issues/17  | com/swmansion/rnscreens/ScreenModalFragment.java  |
| https://github.com/software-mansion/react-native-screens/issues/17  | com/swmansion/rnscreens/ScreenStackFragment.java  |
| https://github.com/software-mansion/react-native-screens/issues  | com/swmansion/rnscreens/utils/ScreenDummyLayoutHelper.java  |
| https://docs.swmansion.com/react-native-gesture-handler/docs/guides/migrating-off-rnghenabledroot  | com/swmansion/gesturehandler/react/RNGestureHandlerEnabledRootView.java  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15222222222  | com/amap/api/col/p0003sl/ik.java  |

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: CN=FQL, OU=PD, O=PortalDev, L=Shanghai, ST=Shanghai, C=CN 签名算法: rsassa\_pkcs1v15 有效期自: 2025-03-09 15:00:05+00:00 有效期至: 2050-03-03 15:00:05+00:00 发行人: CN=FQL, OU=PD, O=PortalDev, L=Shanghai, ST=Shanghai, C=CN 序列号: 0x1 哈希算法: sha256 md5值: 188eac2a63e1b115d87cc7a6745ca254 sha1值: 16a347a95d1f97e0622413944802bfd566cdcc63 sha256值: c553e1a89a6b2564f25ef6c8d5d9322758a4b44033f1e130acfe73efce4201c2 sha512值: fe5935c0f5010335ec90a78d11d9627249a272158b76c0e4a015b75d597fa5ebb64215d6e2b242e99934a14bb7de96ebd054bd4ff78353906236f3fdabe5b6d8 公钥算法: rsa 密钥长度: 2048 指纹: 44174e3b4d3e4160a86a98089a88d0751d7be9a0260142b628cd34d8b8208115**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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.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.FOREGROUND\_SERVICE\_LOCATION | 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.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\_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.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\_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.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.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.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.SYSTEM\_OVERLAY\_WINDOW | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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。 |
| moe.fuqiuluo.portaldev.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**