MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

车场管理 2.19.0.APK

APP名称:	车场管理
包名:	com.parkingwang.iopcommon
域名线索:	26条
URL线索:	35条
邮箱线索:	7条
分析日期:	2022年2月2日 19:28

文件信息

文件名: ccgl.apk
文件大小: 4.65MB
MD5值: 80985498994b9bf8b4060dc24cea79a1
SHA1值: 2bc018cb03472e1a5e70f767f1fa5b35ed25ea55
SHA256值: 78ec6fbacb1fa38357387daca3f63d0ee27548a6e018434d29545b8159f29def

APP 信息

App名称: 车场管理
包名: com.parkingwang.iopcommon
主活动**Activity:** com.parkingwang.iop.SplashActivity
安卓版本名称: 2.19.0
安卓版本: 21900

域名线索

域名	是否危险域名	服务器信息
cfg.imtt.qq.com	good	**IP:** 121.51.158.70 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map

域名	是否危险域名	服务器信息
mta.oa.com	good	**IP:** 193.123.33.15 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.374031 经度: 4.889690 查看地图: Google Map
www.qq.com	good	**IP:** 175.27.8.138 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
adash.man.aliyuncs.com	good	**IP:** 59.82.40.77 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
mdc.html5.qq.com	good	**IP:** 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map

域名	是否危险域名	服务器信息
www.baidu.com	good	**IP:** 110.242.68.4 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280 查看地图: Google Map
open.weixin.qq.com	good	**IP:** 175.24.209.30 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
xmlpull.org	good	**IP:** 74.50.61.58 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204 查看地图: Google Map
182.254.116.117	good	**IP:** 182.254.116.117 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map

域名	是否危险域名	服务器信息
wup.imtt.qq.com	good	**IP:** 182.254.56.113 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
pms.mb.qq.com	good	**IP:** 121.51.158.70 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
pingma.qq.com	good	**IP:** 119.45.78.184 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
rqd.uu.qq.com	good	**IP:** 182.254.88.185 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map

域名	是否危险域名	服务器信息
mqqad.html5.qq.com	good	**IP:** 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
www.parkingwang.com	good	**IP:** 59.38.126.81 所属国家: China 地区: Guangdong 城市: Foshan 纬度: 23.026770 经度: 113.131477 查看地图: Google Map
github.com	good	**IP:** 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903 查看地图: Google Map
schemas.android.com	good	没有服务器地理信息.
debugtbs.qq.com	good	**IP:** 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map

域名	是否危险域名	服务器信息
long.open.weixin.qq.com	good	**IP:** 109.244.216.15 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
log.tbs.qq.com	good	**IP:** 109.244.244.32 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
android.bugly.qq.com	good	**IP:** 109.244.244.35 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
www.slf4j.org	good	**IP:** 83.173.251.158 所属国家: Switzerland 地区: Zurich 城市: Zurich 纬度: 47.366669 经度: 8.550000 查看地图: Google Map

域名	是否危险域名	服务器信息
api.parkingwang.com	good	**IP:** 120.26.39.165 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
mta.qq.com	good	**IP:** 111.161.14.94 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map
debugx5.qq.com	good	**IP:** 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
soft.tbs.imtt.qq.com	good	**IP:** 121.51.175.105 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map

URL线索

URL信息	Url所在文件
http://adash.man.aliyuncs.com:80/man/api?ak=23356390&s=	com/a/a/a/a/a.java
http://pingma.qq.com:80/mstat/report	com/tencent/stat/StatConfig.java
http://mta.qq.com/	com/tencent/stat/StatServiceImpl.java
http://mta.oa.com/	com/tencent/stat/StatServiceImpl.java
http://mta.qq.com/mta/api/ctr_feedback/add_feedback	com/tencent/stat/c.java
http://mta.qq.com/mta/api/ctr_feedback/get_feedback	com/tencent/stat/c.java
http://mta.qq.com/mta/api/ctr_feedback/reply_feedback	com/tencent/stat/c.java
http://mta.qq.com/mta/api/ctr_feedback	com/tencent/stat/common/StatConstants.java
http://pingma.qq.com:80/mstat/report	com/tencent/stat/common/StatConstants.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/beta/upgrade/BetaUploadStrategy.java
http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://pingma.qq.com:80/mstat/report	com/tencent/android/tpush/stat/c.java
http://182.254.116.117/d?dn=99e2d153e4d0527186ebed5ac5608367&id=6&ttl=1	com/tencent/android/tpush/service/b/b.java

URL信息	Url所在文件
www.qq.com	com/tencent/android/tpush/service/e/a.java
http://www.baidu.com	com/tencent/android/tpush/service/channel/i.java
http://www.qq.com	com/tencent/android/tpush/service/channel/i.java
www.qq.com	com/tencent/smtt/sdk/e.java
http://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/e.java
http://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugtbs.qq.com?10000	com/tencent/smtt/sdk/WebView.java
http://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/a/d.java
http://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/k.java
http://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/y.java
http://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/y.java
http://wup.imtt.qq.com:8080	com/tencent/smtt/utils/y.java
http://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/y.java
http://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/y.java

URL信息	Url所在文件
http://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/y.java
http://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/y.java
http://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/y.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/f.java
http://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/d.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/StatConfig.java
http://mta.qq.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://mta.oa.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/common/StatConstants.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/b/a/e.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/b/a/a.java
http://iop_api.srv2.parkingwang.com	com/parkingwang/iop/IopApplication.java
https://github.com/google/gson	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/parkingwang/hey-permission	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/parkingwang/okhttp3-loginterceptor	com/parkingwang/iop/profile/about/OpenSourceListActivity.java

URL信息	Url所在文件
https://github.com/parkingwang/sms-captcha	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/square/retrofit	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/ReactiveX/RxAndroid	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/msdx/IconButton	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/msdx/androidsnippet	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/msdx/android-lite-orm	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/msdx/badge-drawable	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/msdx/group-recycler-adapter	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/msdx/hi-loadmore	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/msdx/themeskinning	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/PhilJay/MPAndroidChart	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/cloudhi/AnyUnit	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/kyleduo/SwitchButton	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/timehop/sticky-headers-recyclerview	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/msdx/status-bar-compat	com/parkingwang/iop/profile/about/OpenSourceListActivity.java

URL信息	Url所在文件
https://github.com/msdx/drawablewidget	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/hdodenhof/CircleImageView	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/bumptech/glide	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/ImKarl/CharacterPickerView	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/msdx/hi-chart	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/jhy/jsoup	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/lankton/android-flowlayout	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/yoojia/NextInputs-Android	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/liaohuqiu/android-Ultra-Pull-To-Refresh	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/greenrobot/EventBus	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/Tishka17/gson-flatten	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
https://github.com/square/leakcanary	com/parkingwang/iop/profile/about/OpenSourceListActivity.java
http://www.parkingwang.com	com/parkingwang/iop/profile/about/AboutAppActivity.java
http://api.parkingwang.com/app/iop/register.html	com/parkingwang/iop/profile/about/AboutAppActivity.java
http://www.slf4j.org/codes.html#no_static_mdc_binder	org/slf4j/MDC.java

URL信息	Url所在文件
http://www.slf4j.org/codes.html#null_MDCA	org/slf4j/MDC.java
http://www.slf4j.org/codes.html	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#loggerNameMismatch	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#multiple_bindings	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#StaticLoggerBinder	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#null_LF	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#replay	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#substituteLogger	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#unsuccessfulInit	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#version_mismatch	org/slf4j/LoggerFactory.java
http://schemas.android.com/android/skin	solid/ren/skinlibrary/b/a.java
www.parkingwang.com	Android String Resource

邮箱线索

邮箱地址	所在文件
ctwap@mycdma.cn	com/tencent/mid/a/b.java
this@dailystatactivity.layoutinfl	com/parkingwang/iop/stat/daily/DailyStatActivity.java
this@flowstatactivity.layoutinfl	com/parkingwang/iop/stat/flow/FlowStatActivity.java
this@incomestatactivity.layoutinfl	com/parkingwang/iop/stat/income/IncomeStatActivity.java
this@newmodeauthfragment.childfragm	com/parkingwang/iop/manager/auth/add/f.java
this@oldmodeauthfragment.childfragm	com/parkingwang/iop/manager/auth/add/i.java
this@parksummaryfragment.layoutinfl	com/parkingwang/iop/summary/a/d.java

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.GET_TASKS	危险	检索正在运行的应用程序	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

向手机申请的权限	是否危险	类型	详细情况
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.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.BATTERY_STATS	合法	修改电池统计信息	允许修改收集的电池统计信息。不供普通应用程序使用
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.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.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.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.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

向手机申请的权限	是否危险	类型	详细情况
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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_FIND_LOCATION	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.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_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.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

向手机申请的权限	是否危险	类型	详细情况
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.RECEIVE_USER_PRESENT	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_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.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.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息
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.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。

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CN, L=Shenzhen, O=parkingwang.com
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-03-16 08:38:13+00:00
Valid To: 3015-07-18 08:38:13+00:00
Issuer: C=CN, L=Shenzhen, O=parkingwang.com
Serial Number: 0x7f8a2a52
Hash Algorithm: sha256
md5: 97134ef3f5817108281e910ee20e049b
sha1: 884abe2290ee7c04de752f9811d5042159ce4205
sha256: c4055b78329d84ba998bd46073cd68c0f1a46ed5cc8bc9942f923d3a2d5ddaef
sha512: 85bc3ac03245b954ca4ba292a8ae4ff698ef822fbed6ca9618f7a9221a65ce4826eeae84f560f7d6ac53242005a8e4f95975b107db9bc9fc8f7614b12d028372
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 705f60926003bd6ad02493c963068fc641fbeaa859dafab8df87b0ee117a6bbc

Exodus威胁情报

名称	分类	URL链接
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116

硬编码敏感信息

可能的敏感信息
"add_auth" : "新增授权"
"add_info_username" : "车主姓名"
"authorization_bottom_info" : "批量增加授权,请登录网页端"
"authorization_detail" : "更多详情信息，请登录网页端"
"cat_username" : "车主姓名"
"colon_auth_card_type" : "授权卡类型:"
"colon_fleet_user" : "操作用户:"
"forget_password" : "忘记密码?"
"format_auth_d_day" : "授权了%d天"
"input_password" : "请输入6~16位数密码"
"park_auth" : "车位授权"
"tip_nesting_park_auth" : "此车场为嵌套车场 APP 暂不支持充值、编辑操作 请在网页端进行相关操作"
"tip_reset_password" : "重置密码后请重新登录"
"tips_long_authorize_info" : "长效授权信息"
"tips_token_invalid" : "登录信息已失效"

可能的敏感信息
"user_name" : "您的用户名为：%s"

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>assets/skin/orange.skin!classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>assets/skin/shangri-la.skin!classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
subscriber ID check
possible ro.secure check
emulator file check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>lib/armeabi/libsophix.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>模糊器</td><td>Alipay</td></tr>
</table>
</td></tr>
</table>
