MoGua

PG电子 3.2.1.APK 分析报告

APP名称:	PG电子

包名:	com.saas.h5android.n1155.d20241031
域名线索:	34条
URL线索:	19条
邮箱线索:	0条
分析日期:	2024年11月7日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 1155PG电子.apk
文件大小: 9.49MB
MD5值: 739adb2ef9cf7f25859dd6c8e36cf9ae
SHA1值: c23cb14a6364f28a0dbfdcce9c83aedccabd6bb7
SHA256值: 49dc5556488ce85c51216a28629a825317818ece6392556198463c1fdb93827c

APP 信息

App名称: PG电子
包名: com.saas.h5android.n1155.d20241031
主活动Activity: com.example.saasapp.MainActivity
安卓版本名称: 3.2.1
安卓版本: 1

域名线索

域名	服务器信息
yshj.7hg16.com	**IP**: 104.21.67.159 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
gitee.com	**IP**: 180.76.198.77 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
aaid.umeng.com	**IP**: 223.109.148.171 **所属国家**: China **地区**: Jiangsu

	城市: Nanjing **纬度**: 32.061668 **经度**: 118.777992
h5api.stumfvj.com	**IP**: 154.31.227.12 **所属国家**: Germany **地区**: Hessen **城市**: Frankfurt am Main **纬度**: 50.110882 **经度**: 8.681996
errnewlog.umeng.com	**IP**: 223.109.148.129 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
alogus.umeng.com	**IP**: 223.109.148.176 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
en.wikipedia.org	**IP**: 103.102.166.224 **所属国家**: United States of America **地区**: Indiana **城市**: Francisco **纬度**: 38.333290 **经度**: -87.447083
ouplog.umeng.com	**IP**: 47.246.110.93 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281

errlog.umeng.com	**IP**: 223.109.148.142 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
h5api5.ljtmk.com	**IP**: 116.130.221.21 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
errlogos.umeng.com	**IP**: 47.246.110.96 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
developer.umeng.com	**IP**: 59.82.29.162 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
ulogs.umeng.com	**IP**: 223.109.148.178 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
h5api.sremnoa.com	**IP**: 154.31.227.126 **所属国家**: Germany **地区**: Hessen **城市**: Frankfurt am Main

	纬度: 50.110882 **经度**: 8.681996
plbslog.umeng.com	**IP**: 36.156.202.73 **所属国家**: China **地区**: Jiangsu **城市**: Yangzhou **纬度**: 32.397221 **经度**: 119.435600
h5static.smyuez.com	**IP**: 154.31.227.12 **所属国家**: Germany **地区**: Hessen **城市**: Frankfurt am Main **纬度**: 50.110882 **经度**: 8.681996
h5static.spemzl.com	**IP**: 154.39.103.5 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
h5api.shgtyoo.com	**IP**: 154.31.227.126 **所属国家**: Germany **地区**: Hessen **城市**: Frankfurt am Main **纬度**: 50.110882 **经度**: 8.681996
h5static.sfoyxw.com	**IP**: 154.39.103.6 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
	IP: 154.39.103.6 **所属国家**: Hong Kong

h5static.ahduanyun.com	**地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
alogsus.umeng.com	**IP**: 223.109.148.177 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
h5api4.ljtmk.com	**IP**: 61.48.83.199 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
errnewlogos.umeng.com	**IP**: 47.246.110.96 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
h5api1.ljtmk.com	**IP**: 154.39.103.21 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
h5static.sptjzt.com	**IP**: 154.31.227.12 **所属国家**: Germany **地区**: Hessen **城市**: Frankfurt am Main **纬度**: 50.110882 **经度**: 8.681996

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
ucc.umeng.com	**IP**: 203.119.169.43 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
api.82761486.com	**IP**: 18.166.142.85 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
h5api.stlsyud.com	**IP**: 154.39.103.21 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
pslog.umeng.com	**IP**: 59.82.29.249 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
ulogs.umengcloud.com	**IP**: 223.109.148.178 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing

	纬度: 32.061668 **经度**: 118.777992
h5static3.ahduanyun.com	**IP**: 61.48.83.219 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
manual.sensorsdata.cn	**IP**: 125.39.47.215 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
h5api.89822821.com	**IP**: 154.31.227.126 **所属国家**: Germany **地区**: Hessen **城市**: Frankfurt am Main **纬度**: 50.110882 **经度**: 8.681996

URL线索

URL**信息**	Url**所在文件**
https://errnewlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/f/c.java
https://errnewlogos.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/controller/ControllerCenter.java
https://errnewlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/controller/ControllerCenter.java
	com/example/saasapp/Constants.java

https://gitee.com/happysunday887/CocosScrollview/raw/main/saash5/m/version.json	
https://github.com/webapp8088/CocosScrollview/raw/main/saash5/m/version.json	com/example/saasapp/Constants.java
https://yshj.7hg16.com/	com/example/saasapp/Constants.java
https://h5static.ahduanyun.com/	com/example/saasapp/Constants.java
https://h5static3.ahduanyun.com/	com/example/saasapp/Constants.java
https://h5static.sptjzt.com/	com/example/saasapp/Constants.java
https://h5static.smyuez.com/	com/example/saasapp/Constants.java
https://h5static.spemzl.com/	com/example/saasapp/Constants.java
https://h5static.sfoyxw.com/	com/example/saasapp/Constants.java
https://h5api1.ljtmk.com/	com/example/saasapp/Constants.java
https://h5api4.ljtmk.com/	com/example/saasapp/Constants.java
https://h5api.shgtyoo.com/	com/example/saasapp/Constants.java
https://h5api.89822821.com/	com/example/saasapp/Constants.java
https://h5api.stumfvj.com/	com/example/saasapp/Constants.java
https://h5api.stlsyud.com/	com/example/saasapp/Constants.java
https://h5api.sremnoa.com/	com/example/saasapp/Constants.java
https://h5api5.ljtmk.com/	com/example/saasapp/Constants.java
https://api.82761486.com:8443/sa?project=production	com/example/saasapp/App.java

https://github.com/yyued/SVGAPlayer-Android	com/opensource/svgaplayer/SVGAParser.java
https://en.wikipedia.org/wiki/Hostname	com/sensorsdata/analytics/android/sdk/SensorsDataAPI.java
https://manual.sensorsdata.cn/sa/latest/flutter-22257963.html\	com/sensorsdata/analytics/android/sdk/visual/utils/AlertMessageUtils.java
https://manual.sensorsdata.cn/sa/latest/tech_sdk_client_web_use-7545346.html\	com/sensorsdata/analytics/android/sdk/visual/utils/AlertMessageUtils.java
https://errlogos.umeng.com	com/uc/crashsdk/a/d.java
https://errlog.umeng.com	com/uc/crashsdk/a/d.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/j.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://developer.umeng.com/docs/119267/detail/182050	com/umeng/commonsdk/debug/UMLogCommon.java
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java

https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.java
https://aaid.umeng.com/api/updateZdata	com/umeng/umzid/ZIDManager.java
https://aaid.umeng.com/api/postZdata	com/umeng/umzid/ZIDManager.java
https://errnewlog.umeng.com	com/umeng/umcrash/UMCrashContent.java
https://errnewlogos.umeng.com	com/umeng/umcrash/UMCrashContent.java
https://errnewlogos.umeng.com/upload	com/umeng/umcrash/UMCrash.java
https://errnewlogos.umeng.com	com/umeng/umcrash/UMCrash.java
https://errnewlog.umeng.com/upload	com/umeng/umcrash/UMCrash.java
https://errnewlog.umeng.com	com/umeng/umcrash/UMCrash.java
https://pslog.umeng.com/ablog	com/umeng/cconfig/UMRemoteConfig.java
https://ucc.umeng.com/v1/fetch	com/umeng/cconfig/UMRemoteConfig.java
https://ucc.umeng.com/v1/fetch	com/umeng/cconfig/c/b.java
https://pslog.umeng.com/ablog	com/umeng/cconfig/c/b.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=cc, ST=cc, L=cc, O=cc, OU=cc, CN=cc
签名算法: rsassa_pkcs1v15
有效期自: 2021-05-03 11:25:49+00:00
有效期至: 2121-04-09 11:25:49+00:00
发行人: C=cc, ST=cc, L=cc, O=cc, OU=cc, CN=cc
序列号: 0x3430c357
哈希算法: sha256
md5值: 4ec2f6c532cd7f26b07e4bd28aa506f4
sha1值: b3afedb87f379d4fe719642aaf4e980bb958119f
sha256值: 98eb6a727730549f2b8291a2bcbc32338e66bb547c31e63b194931fed2e7e8a9
sha512值: ba8d0b498d80588fcea4d23b12336d13d4362a04de6a9c458dd564de9bca4e4664b55130a38c0a6d94e6793d722387b954dd3b4fa736421aead61f6f72de97fe
公钥算法: rsa
密钥长度: 2048
指纹: 89a020b42c40d7f5cc6523b3af5579437486659bd35c2780529a250cb5083213

硬编码敏感信息

可能的敏感信息
"umeng_appkey" : "64be6a10bd4b621232dc6326"

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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_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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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_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.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.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.BROADCAST_PACKAGE_ADDED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_CHANGED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_INSTALL	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_REPLACED	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

应用内通信