



# MoGua

## SGEX 1.0.0.APK 分析报告



APP名称:

SGEX

|        |                            |
|--------|----------------------------|
| 包名:    | com.sgex.sgex              |
| 域名线索:  | 35条                        |
| URL线索: | 17条                        |
| 邮箱线索:  | 2条                         |
| 分析日期:  | 2025年8月4日                  |
| 分析平台:  | <a href="#">摸瓜APK反编译平台</a> |

文件名: app-release-v1.0.01.apk  
文件大小: 160.81MB  
MD5值: 39438291be56ff0ceea052398b4b201f  
SHA1值: f07a00ee8e82fedcbf4a8a1562f228de517e0e58  
SHA256值: 85ded77c5529fb0b6914615dc18ac00b1e7e5ad260378c14d61940fd40635ff3

## i APP 信息

App名称: SGEX  
包名: com.sgex.sgex  
主活动Activity: com.sgex.sgex.MainActivity  
安卓版本名称: 1.0.0  
安卓版本: 1

## 🔍 域名线索

| 域名                    | 服务器信息                                                                                                                           |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------|
| 162.14.13.170         | IP: 162.14.13.170<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102                               |
| developer.android.com | IP: 142.250.73.110<br>所属国家: United States of America<br>地区: California<br>城市: Mountain View<br>纬度: 37.405991<br>经度: -122.078514 |
| docs.flutter.dev      | IP: 199.36.158.100<br>所属国家: United States of America<br>地区: California                                                          |

|                                                |                                                                                                                                                                        |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                | <b>城市:</b> Mountain View<br><b>纬度:</b> 37.405991<br><b>经度:</b> -122.078514                                                                                             |
| sdk-im-1252463788.cos.ap-hongkong.myqcloud.com | <b>IP:</b> 43.128.240.33<br><b>所属国家:</b> Japan<br><b>地区:</b> Tokyo<br><b>城市:</b> Tokyo<br><b>纬度:</b> 35.689499<br><b>经度:</b> 139.692322                                |
| stackoverflow.com                              | <b>IP:</b> 104.18.32.7<br><b>所属国家:</b> United States of America<br><b>地区:</b> California<br><b>城市:</b> San Francisco<br><b>纬度:</b> 37.775700<br><b>经度:</b> -122.395203 |
| 162.14.6.156                                   | <b>IP:</b> 162.14.6.156<br><b>所属国家:</b> China<br><b>地区:</b> Beijing<br><b>城市:</b> Beijing<br><b>纬度:</b> 39.907501<br><b>经度:</b> 116.397102                             |
| 162.14.19.114                                  | <b>IP:</b> 162.14.19.114<br><b>所属国家:</b> China<br><b>地区:</b> Beijing<br><b>城市:</b> Beijing<br><b>纬度:</b> 39.907501<br><b>经度:</b> 116.397102                            |
| 43.129.43.42                                   | <b>IP:</b> 43.129.43.42<br><b>所属国家:</b> Indonesia<br><b>地区:</b> Jakarta Raya<br><b>城市:</b> Jakarta<br><b>纬度:</b> -6.208678<br><b>经度:</b> 106.845490                    |
|                                                |                                                                                                                                                                        |

|                       |                                                                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------|
| dev.w3.org            | IP: 104.18.22.19<br>所属国家: United States of America<br>地区: California<br>城市: San Francisco<br>纬度: 37.775700<br>经度: -122.395203 |
| 162.14.17.129         | IP: 162.14.17.129<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102                             |
| www.unicode.org       | IP: 64.182.27.164<br>所属国家: United States of America<br>地区: Texas<br>城市: Dallas<br>纬度: 32.814899<br>经度: -96.879204             |
| 162.14.13.203         | IP: 162.14.13.203<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102                             |
| developer.mozilla.org | IP: 34.111.97.67<br>所属国家: United States of America<br>地区: Missouri<br>城市: Kansas City<br>纬度: 39.099731<br>经度: -94.578568      |
| 162.14.19.159         | IP: 162.14.19.159<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102                             |

|                                     |                                                                                                                          |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
|                                     | 经度: 116.397102                                                                                                           |
| 162.14.10.42                        | IP: 162.14.10.42<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102                         |
| 162.14.11.59                        | IP: 162.14.11.59<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102                         |
| www.example.com                     | IP: 23.220.70.110<br>所属国家: Japan<br>地区: Tokyo<br>城市: Tokyo<br>纬度: 35.689499<br>经度: 139.692322                            |
| sdk-im-1252463788.file.myqcloud.com | IP: 116.196.150.251<br>所属国家: China<br>地区: Zhejiang<br>城市: Jinhua<br>纬度: 30.013470<br>经度: 120.288658                      |
| paulbakaus.com                      | IP: 167.172.18.193<br>所属国家: United States of America<br>地区: New Jersey<br>城市: Clifton<br>纬度: 40.858585<br>经度: -74.163605 |
|                                     | IP: 216.239.32.21<br>所属国家: United States of America                                                                      |

|                 |                                                                                                                                                 |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| dartbug.com     | <div>地区: California<br/>城市: Mountain View<br/>纬度: 37.405991<br/>经度: -122.078514</div>                                                           |
| 43.129.34.169   | <div>IP: 43.129.34.169<br/>所属国家: Indonesia<br/>地区: Jakarta Raya<br/>城市: Jakarta<br/>纬度: -6.208678<br/>经度: 106.845490</div>                      |
| github.com      | <div>IP: 20.205.243.166<br/>所属国家: Singapore<br/>地区: Singapore<br/>城市: Singapore<br/>纬度: 1.289987<br/>经度: 103.850281</div>                       |
| 162.14.3.250    | <div>IP: 162.14.3.250<br/>所属国家: China<br/>地区: Beijing<br/>城市: Beijing<br/>纬度: 39.907501<br/>经度: 116.397102</div>                                |
| api.flutter.dev | <div>IP: 199.36.158.100<br/>所属国家: United States of America<br/>地区: California<br/>城市: Mountain View<br/>纬度: 37.405991<br/>经度: -122.078514</div> |
| 162.14.13.181   | <div>IP: 162.14.13.181<br/>所属国家: China<br/>地区: Beijing<br/>城市: Beijing<br/>纬度: 39.907501<br/>经度: 116.397102</div>                               |
|                 |                                                                                                                                                 |

|                                               |                                                                                                                               |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| www.w3.org                                    | IP: 104.18.22.19<br>所属国家: United States of America<br>地区: California<br>城市: San Francisco<br>纬度: 37.775700<br>经度: -122.395203 |
| 162.14.20.148                                 | IP: 162.14.20.148<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102                             |
| journeyapps.com                               | IP: 18.65.25.108<br>所属国家: United States of America<br>地区: California<br>城市: Los Angeles<br>纬度: 34.052570<br>经度: -118.243904   |
| 162.14.13.104                                 | IP: 162.14.13.104<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102                             |
| im.sdk.qcloud.com                             | IP: 116.196.151.115<br>所属国家: China<br>地区: Zhejiang<br>城市: Jinhua<br>纬度: 30.013470<br>经度: 120.288658                           |
| sdk-im-1252463788.cos.accelerate.myqcloud.com | IP: 127.0.0.1<br>所属国家: -<br>地区: -<br>城市: -<br>纬度: 0.000000                                                                    |

|              |                                                                                                                                |
|--------------|--------------------------------------------------------------------------------------------------------------------------------|
|              | 经度: 0.000000                                                                                                                   |
| 162.14.3.17  | IP: 162.14.3.17<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102                                |
| www.gnu.org  | IP: 209.51.188.116<br>所属国家: United States of America<br>地区: Massachusetts<br>城市: Somerville<br>纬度: 42.387600<br>经度: -71.099503 |
| 162.14.19.46 | IP: 162.14.19.46<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102                               |
| mozilla.org  | IP: 35.190.14.201<br>所属国家: United States of America<br>地区: Missouri<br>城市: Kansas City<br>纬度: 39.099731<br>经度: -94.578568      |

 URL线索

| URL信息                                                                                                                                     | Url所在文件                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| <a href="https://github.com/Baseflow/flutter-permission-handler/issues">https://github.com/Baseflow/flutter-permission-handler/issues</a> | com/baseflow/permissionhandler/PermissionManager.java |

|                                                                                                                                                                             |                                                                                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| <a href="http://www.example.com">http://www.example.com</a>                                                                                                                 | com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/CustomTabsHelper.java |
| <a href="https://im.sdk.qcloud.com/download/plus/8.6.7019/">https://im.sdk.qcloud.com/download/plus/8.6.7019/</a>                                                           | com/tencent/imSDK/manager/LibraryDownloader.java                                  |
| <a href="https://sdk-im-1252463788.cos.accelerate.myqcloud.com/download/plus/8.6.7019/">https://sdk-im-1252463788.cos.accelerate.myqcloud.com/download/plus/8.6.7019/</a>   | com/tencent/imSDK/manager/LibraryDownloader.java                                  |
| <a href="https://sdk-im-1252463788.file.myqcloud.com/download/plus/8.6.7019/">https://sdk-im-1252463788.file.myqcloud.com/download/plus/8.6.7019/</a>                       | com/tencent/imSDK/manager/LibraryDownloader.java                                  |
| <a href="https://sdk-im-1252463788.cos.ap-hongkong.myqcloud.com/download/plus/8.6.7019/">https://sdk-im-1252463788.cos.ap-hongkong.myqcloud.com/download/plus/8.6.7019/</a> | com/tencent/imSDK/manager/LibraryDownloader.java                                  |
| <a href="https://docs.flutter.dev/deployment/android">https://docs.flutter.dev/deployment/android</a>                                                                       | io/flutter/embedding/engine/loader/FlutterLoader.java                             |
| <a href="https://developer.android.com/guide/topics/permissions/overview">https://developer.android.com/guide/topics/permissions/overview</a>                               | io/flutter/plugin/platform/PlatformPlugin.java                                    |
| <a href="https://journeyapps.com/">https://journeyapps.com/</a>                                                                                                             | 摸瓜V1引擎                                                                            |
| <a href="https://github.com/journeyapps/zxing-android-embedded">https://github.com/journeyapps/zxing-android-embedded</a>                                                   | 摸瓜V1引擎                                                                            |
| <a href="https://www.gnu.org/licenses/">https://www.gnu.org/licenses/</a> .                                                                                                 | 摸瓜V2引擎                                                                            |
| <a href="https://www.gnu.org/licenses/">https://www.gnu.org/licenses/</a> .                                                                                                 | 摸瓜V2引擎                                                                            |
| <a href="http://paulbakaus.com/tutorials/html5/web-audio-on-ios/">http://paulbakaus.com/tutorials/html5/web-audio-on-ios/</a>                                               | 摸瓜V2引擎                                                                            |
| <a href="http://stackoverflow.com/questions/24119684">http://stackoverflow.com/questions/24119684</a>                                                                       | 摸瓜V2引擎                                                                            |
| <a href="https://mozilla.org/MPL/2.0/">https://mozilla.org/MPL/2.0/</a> .                                                                                                   | 摸瓜V2引擎                                                                            |
| <a href="https://mozilla.org/MPL/2.0/">https://mozilla.org/MPL/2.0/</a> .                                                                                                   | 摸瓜V2引擎                                                                            |
| <a href="https://mozilla.org/MPL/2.0/">https://mozilla.org/MPL/2.0/</a> .                                                                                                   | 摸瓜V2引擎                                                                            |
| <a href="https://www.gnu.org/licenses/">https://www.gnu.org/licenses/</a> .                                                                                                 | 摸瓜V2引擎                                                                            |

|                                                                                                                                                                     |                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| <a href="https://github.com/richtr/NoSleep.js/issues/15">https://github.com/richtr/NoSleep.js/issues/15</a>                                                         | 摸瓜V2引擎                    |
| <a href="https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released">https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released</a> | 摸瓜V2引擎                    |
| <a href="https://43.129.34.169/v4/ConfigGetSvc/GetOpenSSOIPList">https://43.129.34.169/v4/ConfigGetSvc/GetOpenSSOIPList</a>                                         | lib/arm64-v8a/libImSDK.so |
| <a href="https://162.14.19.159/v4/ConfigGetSvc/GetOpenSSOIPList">https://162.14.19.159/v4/ConfigGetSvc/GetOpenSSOIPList</a>                                         | lib/arm64-v8a/libImSDK.so |
| <a href="http://162.14.11.59/v4/ConfigGetSvc/GetOpenSSOIPList">http://162.14.11.59/v4/ConfigGetSvc/GetOpenSSOIPList</a>                                             | lib/arm64-v8a/libImSDK.so |
| <a href="http://162.14.17.129/v4/ConfigGetSvc/GetOpenSSOIPList">http://162.14.17.129/v4/ConfigGetSvc/GetOpenSSOIPList</a>                                           | lib/arm64-v8a/libImSDK.so |
| <a href="http://162.14.20.148/v4/ConfigGetSvc/GetOpenSSOIPList">http://162.14.20.148/v4/ConfigGetSvc/GetOpenSSOIPList</a>                                           | lib/arm64-v8a/libImSDK.so |
| <a href="https://162.14.3.17/v4/ConfigGetSvc/GetOpenSSOIPList">https://162.14.3.17/v4/ConfigGetSvc/GetOpenSSOIPList</a>                                             | lib/arm64-v8a/libImSDK.so |
| <a href="http://162.14.6.156/v4/ConfigGetSvc/GetOpenSSOIPList">http://162.14.6.156/v4/ConfigGetSvc/GetOpenSSOIPList</a>                                             | lib/arm64-v8a/libImSDK.so |
| <a href="https://162.14.19.46/v4/ConfigGetSvc/GetOpenSSOIPList">https://162.14.19.46/v4/ConfigGetSvc/GetOpenSSOIPList</a>                                           | lib/arm64-v8a/libImSDK.so |
| <a href="https://162.14.13.104/v4/ConfigGetSvc/GetOpenSSOIPList">https://162.14.13.104/v4/ConfigGetSvc/GetOpenSSOIPList</a>                                         | lib/arm64-v8a/libImSDK.so |
| <a href="http://43.129.43.42/v4/ConfigGetSvc/GetOpenSSOIPList">http://43.129.43.42/v4/ConfigGetSvc/GetOpenSSOIPList</a>                                             | lib/arm64-v8a/libImSDK.so |
| <a href="https://162.14.10.42/v4/ConfigGetSvc/GetOpenSSOIPList">https://162.14.10.42/v4/ConfigGetSvc/GetOpenSSOIPList</a>                                           | lib/arm64-v8a/libImSDK.so |
| <a href="http://162.14.13.181/v4/ConfigGetSvc/GetOpenSSOIPList">http://162.14.13.181/v4/ConfigGetSvc/GetOpenSSOIPList</a>                                           | lib/arm64-v8a/libImSDK.so |
| <a href="https://162.14.13.170/v4/ConfigGetSvc/GetOpenSSOIPList">https://162.14.13.170/v4/ConfigGetSvc/GetOpenSSOIPList</a>                                         | lib/arm64-v8a/libImSDK.so |
| <a href="http://162.14.3.250/v4/ConfigGetSvc/GetOpenSSOIPList">http://162.14.3.250/v4/ConfigGetSvc/GetOpenSSOIPList</a>                                             | lib/arm64-v8a/libImSDK.so |
| <a href="https://43.129.34.169/netcheck">https://43.129.34.169/netcheck</a>                                                                                         | lib/arm64-v8a/libImSDK.so |
|                                                                                                                                                                     |                           |

|                                                                           |                             |
|---------------------------------------------------------------------------|-----------------------------|
| https://162.14.19.159/netcheck                                            | lib/arm64-v8a/libImSDK.so   |
| https://162.14.3.17/netcheck                                              | lib/arm64-v8a/libImSDK.so   |
| https://162.14.19.46/netcheck                                             | lib/arm64-v8a/libImSDK.so   |
| https://162.14.13.104/netcheck                                            | lib/arm64-v8a/libImSDK.so   |
| https://162.14.13.203/netcheck                                            | lib/arm64-v8a/libImSDK.so   |
| https://162.14.10.42/netcheck                                             | lib/arm64-v8a/libImSDK.so   |
| http://162.14.19.114/                                                     | lib/arm64-v8a/libImSDK.so   |
| https://api.flutter.dev/flutter/material/Scaffold/of.html                 | lib/arm64-v8a/libapp.so     |
| http://www.unicode.org/copyright.html                                     | lib/arm64-v8a/libflutter.so |
| https://docs.flutter.dev/release/breaking-changes/android-surface-plugins | lib/arm64-v8a/libflutter.so |
| https://github.com/flutter/flutter/issues.                                | lib/arm64-v8a/libflutter.so |
| https://dartbug.com/52121.                                                | lib/arm64-v8a/libflutter.so |

 邮箱线索

| 邮箱地址              | 所在文件                          |
|-------------------|-------------------------------|
| appro@openssl.org | lib/arm64-v8a/libflutter.so   |
| appro@openssl.org | lib/arm64-v8a/libijkffmpeg.so |

# ☰ 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: False  
v2 签名: True  
v3 签名: False  
找到 1 个唯一证书  
主题: CN=FENGXIA LU, OU=Seagull Technology Group Ltd, O=SGEX, L=Springs, ST=Colorado, C=80907sgex  
签名算法: rsassa\_pkcs1v15  
有效期自: 2025-07-10 12:25:05+00:00  
有效期至: 2050-07-04 12:25:05+00:00  
发行人: CN=FENGXIA LU, OU=Seagull Technology Group Ltd, O=SGEX, L=Springs, ST=Colorado, C=80907sgex  
序列号: 0x1  
哈希算法: sha256  
md5值: f4cb9db01efbb695e6ef068289e04539  
sha1值: 2d907270d06491bb4326d5bed4dda7a910ac6716  
sha256值: f5c05477368e4a899e259857d286341e1e53fe85330d7df05b36fa93c32bf475  
sha512值: 4f26dd552d0611949d0e3bcf23c49d9df5353efcb7d6893abf6248278fdb8ea66bfb6208dccdbd48473c4b3d25034fbb7513fa1a3bb3e5f5b40a8510afbd0719  
公钥算法: rsa  
密钥长度: 2048  
指纹: 0b9fa0fb44effff382e6441fe7d8c22ec0eb902069dc7b8134196bc3c4287920

# 🔑 硬编码敏感信息

| 可能的敏感信息 |
|---------|
| .....   |

|                                                                           |
|---------------------------------------------------------------------------|
| "library_zxingandroidembedded_author" : "JourneyApps"                     |
| "library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/" |

## 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.READ_PHONE_STATE | 危险   | 读取电话状态<br>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.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.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.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.RECORD_AUDIO             | 危险 | 录音                 | 允许应用程序访问音频记录路径                                            |
| 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_AUDIO         | 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                         |
| 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_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.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.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.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                    |
| Manifest.permission.CAPTURE_AUDIO_OUTPUT               | 未知 | Unknown permission | Unknown permission from android reference |
| com.sgex.sgex.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |



应用内通信

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