



# MoGua

## 草榴社區 1.1.0.APK 分析報告



APP名称:

草榴社區

|        |                            |
|--------|----------------------------|
| 包名:    | uk.bygyx.fuwmsa            |
| 域名线索:  | 24条                        |
| URL线索: | 20条                        |
| 邮箱线索:  | 4条                         |
| 分析日期:  | 2025年8月5日                  |
| 分析平台:  | <a href="#">摸瓜APK反编译平台</a> |

文件名: hjgj\_1.1.0\_240624\_2.apk  
文件大小: 30.93MB  
MD5值: 6608a5d9f158718ebb335f705110c228  
SHA1值: 2839a8a801a60070955fb7341916eedc26d81f18  
SHA256值: ea5f17cd22dc8fbecdf0e9d55e061456812a94e38ab790ea2e352109b11b9bac

# i APP 信息

App名称: 草榴社區  
包名: uk.bygyx.fuwmsa  
主活动Activity: com.tbone.hjgj.MainActivity  
安卓版本名称: 1.1.0  
安卓版本: 2

## 🔍 域名线索

| 域名              | 服务器信息                                                                                                                          |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------|
| exoplayer.dev   | IP: 185.199.108.153<br>所属国家: United States of America<br>地区: Pennsylvania<br>城市: California<br>纬度: 40.065647<br>经度: -79.891724 |
| staff.tea123.me | IP: 104.21.71.17<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  |
| www.w3.org      | IP: 104.18.23.19<br>所属国家: United States of America<br>地区: California                                                           |

|                       |                                                                                                                                                                           |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <b>城市:</b> San Francisco<br><b>纬度:</b> 37.775700<br><b>经度:</b> -122.395203                                                                                                |
| flutter.dev           | <b>IP:</b> 199.36.158.100<br><b>所属国家:</b> United States of America<br><b>地区:</b> California<br><b>城市:</b> Mountain View<br><b>纬度:</b> 37.405991<br><b>经度:</b> -122.078514 |
| schemas.microsoft.com | <b>IP:</b> 13.107.253.39<br><b>所属国家:</b> Germany<br><b>地区:</b> Hessen<br><b>城市:</b> Frankfurt am Main<br><b>纬度:</b> 50.110882<br><b>经度:</b> 8.681996                      |
| github.com            | <b>IP:</b> 20.205.243.166<br><b>所属国家:</b> Singapore<br><b>地区:</b> Singapore<br><b>城市:</b> Singapore<br><b>纬度:</b> 1.289987<br><b>经度:</b> 103.850281                       |
| developer.android.com | <b>IP:</b> 142.251.42.238<br><b>所属国家:</b> United States of America<br><b>地区:</b> California<br><b>城市:</b> Mountain View<br><b>纬度:</b> 37.405991<br><b>经度:</b> -122.078514 |
| data.flurry.com       | <b>IP:</b> 98.136.147.18<br><b>所属国家:</b> United States of America<br><b>地区:</b> New York<br><b>城市:</b> New York City<br><b>纬度:</b> 40.731323<br><b>经度:</b> -73.990089     |
|                       |                                                                                                                                                                           |

|                             |                                                                                                                                |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| developer.apple.com         | IP: 17.253.87.204<br>所属国家: Hong Kong<br>地区: Hong Kong<br>城市: Hong Kong<br>纬度: 22.285521<br>经度: 114.157692                      |
| 127.0.0.1                   | IP: 127.0.0.1<br>所属国家: -<br>地区: -<br>城市: -<br>纬度: 0.000000<br>经度: 0.000000                                                     |
| bp.haijiinternational.com   | IP: 172.67.148.33<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 |
| bp.haijiaointernational.net | IP: 104.21.8.63<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   |
| ns.adobe.com                | 没有服务器地理信息.                                                                                                                     |
| www.jsdelivr.com            | IP: 104.21.23.24<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  |
|                             | IP: 114.250.66.34<br>所属国家: China                                                                                               |

|                           |                                                                                                                                                                          |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| www.google.cn             | <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                                                                                |
| gitee.com                 | <b>IP:</b> 180.76.198.77<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                              |
| www.ibm.com               | <b>IP:</b> 23.13.189.250<br><b>所属国家:</b> Hong Kong<br><b>地区:</b> Hong Kong<br><b>城市:</b> Hong Kong<br><b>纬度:</b> 22.285521<br><b>经度:</b> 114.157692                      |
| raw.githubusercontent.com | <b>IP:</b> 0.0.0.0<br><b>所属国家:</b> -<br><b>地区:</b> -<br><b>城市:</b> -<br><b>纬度:</b> 0.000000<br><b>经度:</b> 0.000000                                                       |
| new.cnzuqiu.mobi          | <b>IP:</b> 103.224.212.214<br><b>所属国家:</b> Australia<br><b>地区:</b> Victoria<br><b>城市:</b> Beaumaris<br><b>纬度:</b> -37.982201<br><b>经度:</b> 145.038940                    |
| aomedia.org               | <b>IP:</b> 185.199.111.153<br><b>所属国家:</b> United States of America<br><b>地区:</b> Pennsylvania<br><b>城市:</b> California<br><b>纬度:</b> 40.065647<br><b>经度:</b> -79.891724 |

|                       |                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------|
| wvseee.jsbacjr.com    | IP: 104.21.31.88<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   |
| proton.flurry.com     | 没有服务器地理信息.                                                                                                                      |
| 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        |
| api.flutter.dev       | 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 |

 URL线索

| URL信息                              | Url所在文件       |
|------------------------------------|---------------|
| http://ns.adobe.com/xap/1.0/\u0000 | e/d/a/a.java  |
| https://data.flurry.com/pcr.do     | f/e/b/a0.java |
| https://data.flurry.com/aap.do     | f/e/b/k0.java |
| http://data.flurry.com/aap.do      | f/e/b/k0.java |
|                                    |               |

|                                                                                                                                                                     |                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| <a href="https://proton.flurry.com/sdk/v1/config">https://proton.flurry.com/sdk/v1/config</a>                                                                       | f/e/b/s.java                      |
| <a href="https://exoplayer.dev/issues/player-accessed-on-wrong-thread">https://exoplayer.dev/issues/player-accessed-on-wrong-thread</a>                             | f/f/a/a/e2.java                   |
| <a href="http://www.w3.org/ns/ttml">http://www.w3.org/ns/ttml</a>                                                                                                   | f/f/a/a/c4/v/c.java               |
| <a href="https://exoplayer.dev/issues/cleartext-not-permitted">https://exoplayer.dev/issues/cleartext-not-permitted</a>                                             | f/f/a/a/e4/d0.java                |
| <a href="http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense">http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense</a>                   | f/f/a/a/w3/l0.java                |
| <a href="https://x&lt;/LA_URL&gt;">https://x&lt;/LA_URL&gt;</a>                                                                                                     | f/f/a/a/w3/k0.java                |
| <a href="https://x">https://x</a>                                                                                                                                   | f/f/a/a/w3/k0.java                |
| <a href="http://ns.adobe.com/xap/1.0/">http://ns.adobe.com/xap/1.0/</a>                                                                                             | f/f/a/a/x3/m0/a.java              |
| <a href="https://aomedia.org/emsg/ID3">https://aomedia.org/emsg/ID3</a>                                                                                             | f/f/a/a/z3/j/a.java               |
| <a href="https://developer.apple.com/streaming/emsg-id3">https://developer.apple.com/streaming/emsg-id3</a>                                                         | f/f/a/a/z3/j/a.java               |
| <a href="https://developer.android.com/guide/topics/permissions/overview">https://developer.android.com/guide/topics/permissions/overview</a>                       | io/flutter/plugin/platform/e.java |
| <a href="https://github.com/flutter/flutter/issues/2897).It">https://github.com/flutter/flutter/issues/2897).It</a>                                                 | io/flutter/plugin/platform/l.java |
| <a href="https://developer.android.com/reference/javax/net/ssl/SSLSocket">https://developer.android.com/reference/javax/net/ssl/SSLSocket</a>                       | io/flutter/plugins/d/t.java       |
| <a href="https://github.com/richtr/NoSleep.js/issues/15">https://github.com/richtr/NoSleep.js/issues/15</a>                                                         | Mogua Engine V2                   |
| <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> | Mogua Engine V2                   |
| <a href="https://www.jsdelivr.com/using-sri-with-dynamic-files">https://www.jsdelivr.com/using-sri-with-dynamic-files</a>                                           | Mogua Engine V2                   |
| <a href="https://github.com/apvarun/toastify-js">https://github.com/apvarun/toastify-js</a>                                                                         | Mogua Engine V2                   |
| <a href="https://www.google.cn/intl/zh-CN/chrome">https://www.google.cn/intl/zh-CN/chrome</a>                                                                       | Mogua Engine V2                   |

|                                                                                                                                                                                     |                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| <a href="http://www.w3.org/XML/1998/namespace">http://www.w3.org/XML/1998/namespace</a>                                                                                             | lib/armeabi-v7a/libflutter.so |
| <a href="http://www.w3.org/2000/xmlns/">http://www.w3.org/2000/xmlns/</a>                                                                                                           | lib/armeabi-v7a/libflutter.so |
| <a href="https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).">https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).</a>                                                                       | lib/armeabi-v7a/libflutter.so |
| <a href="https://github.com/flutter/flutter/issues.">https://github.com/flutter/flutter/issues.</a>                                                                                 | lib/armeabi-v7a/libflutter.so |
| <a href="https://bp.haijiaointernational.net/api.php">https://bp.haijiaointernational.net/api.php</a>                                                                               | lib/armeabi-v7a/libapp.so     |
| <a href="http://127.0.0.1:">http://127.0.0.1:</a>                                                                                                                                   | lib/armeabi-v7a/libapp.so     |
| <a href="https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html">https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html</a>                                   | lib/armeabi-v7a/libapp.so     |
| <a href="https://wvsee.jsbacjr.com/fds.txt">https://wvsee.jsbacjr.com/fds.txt</a>                                                                                                   | lib/armeabi-v7a/libapp.so     |
| <a href="https://staff.tea123.me/e.jpg">https://staff.tea123.me/e.jpg</a>                                                                                                           | lib/armeabi-v7a/libapp.so     |
| <a href="http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd">http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd</a>                                                 | lib/armeabi-v7a/libapp.so     |
| <a href="http://www.w3.org/2000/svg">http://www.w3.org/2000/svg</a>                                                                                                                 | lib/armeabi-v7a/libapp.so     |
| <a href="https://raw.githubusercontent.com/little-5/backup/master/haijiao-international.txt">https://raw.githubusercontent.com/little-5/backup/master/haijiao-international.txt</a> | lib/armeabi-v7a/libapp.so     |
| <a href="http://www.w3.org/1998/Math/MathML">http://www.w3.org/1998/Math/MathML</a>                                                                                                 | lib/armeabi-v7a/libapp.so     |
| <a href="http://www.w3.org/2000/xmlns/">http://www.w3.org/2000/xmlns/</a>                                                                                                           | lib/armeabi-v7a/libapp.so     |
| <a href="https://new.cnzuqiu.mobi">https://new.cnzuqiu.mobi</a>                                                                                                                     | lib/armeabi-v7a/libapp.so     |
| <a href="https://api.flutter.dev/flutter/material/Scaffold/of.html">https://api.flutter.dev/flutter/material/Scaffold/of.html</a>                                                   | lib/armeabi-v7a/libapp.so     |
| <a href="https://gitee.com/fdsaw/ffewelmcxww/raw/master/hj.txt">https://gitee.com/fdsaw/ffewelmcxww/raw/master/hj.txt</a>                                                           | lib/armeabi-v7a/libapp.so     |
|                                                                                                                                                                                     |                               |

|                                                                                                                                                                          |                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| <a href="https://bp.haijiinternational.com/api.php">https://bp.haijiinternational.com/api.php</a>                                                                        | lib/armeabi-v7a/libapp.so   |
| <a href="https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android">https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.</a> | lib/armeabi-v7a/libapp.so   |
| <a href="https://github.com/flutter/flutter/issues/new">https://github.com/flutter/flutter/issues/new.</a>                                                               | lib/armeabi-v7a/libapp.so   |
| <a href="http://www.w3.org/XML/1998/namespace">http://www.w3.org/XML/1998/namespace</a>                                                                                  | lib/arm64-v8a/libflutter.so |
| <a href="http://www.w3.org/2000/xmlns/">http://www.w3.org/2000/xmlns/</a>                                                                                                | lib/arm64-v8a/libflutter.so |
| <a href="https://www.w3.org/Style/CSS/Test/Fonts/Ahem/">https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).</a>                                                              | lib/arm64-v8a/libflutter.so |
| <a href="https://github.com/flutter/flutter/issues">https://github.com/flutter/flutter/issues.</a>                                                                       | lib/arm64-v8a/libflutter.so |

 邮箱线索

| 邮箱地址                                                                                                                                                                                                                                                          | 所在文件                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| ffmpeg-devel@ffmpeg.org                                                                                                                                                                                                                                       | lib/armeabi-v7a/libijkplayer.so |
| _double@0150898.fromintege<br>_growablelist@0150898._literal<br>_casterror@0150898._create<br>g_immutablelist@0150898._rjb<br>_growablelist@0150898._withdata<br>n_typeerror@0150898._create<br>eo_bytebuffer@7027147._new<br>_assertionerror@0150898._create | lib/armeabi-v7a/libapp.so       |
| 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           |
|-------------|----------------|
| 17512775099 | f/f/b/c/a.java |

## ☀ 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: CN=Android Debug, O=Android, C=US

签名算法: rsassa\_pkcs1v15

有效期自: 2022-11-03 10:16:02+00:00

有效期至: 2052-10-26 10:16:02+00:00

发行人: CN=Android Debug, O=Android, C=US

序列号: 0x1

哈希算法: sha1

md5值: 7d8a2c0d2493e5d6d85c3865d0918482

sha1值: 7682ef35f017d1b3d352557971c295a6885fae4c

sha256值: 7b86e6199d7c910d075153a0fe61cf241a4b390dd5f4dd0a74381dab7cf42b6f

sha512值: 5d1a8d09f651ee318f3411e559df66a5439dfea5538839f3bc527c6fa3a0671d1326e28949e56f2766e9f716b69ff5ecb1298370c4bb59b7701a43ef4744178b

公钥算法: rsa

密钥长度: 2048

指纹: a715c81d7c87ff29afca669875aed119aeed1a6f489b5d567f6e4c3922f04e1f

## 🔑 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

| 向手机申请的权限                                    | 是否危险 | 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.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.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.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.VIBRATE                       | 正常 | 可控震源               | 允许应用程序控制振动器                                                   |
| 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.DOWNLOAD_WITHOUT_NOTIFICATION | 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.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.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