



# MoGua

## 小蝴蝶的花园 1.0.1.APK 分析报告



APP名称:

小蝴蝶的花园

包名: com.example.fwwzpxhng

域名线索: 7条

URL线索: 6条

邮箱线索: 5条

分析日期: 2024年11月7日

分析平台: [摸瓜APK反编译平台](#)

文件名: 小蝴蝶的花园 (2).Apk

文件大小: 47.61MB

MD5值: 555d5ffcc8073a5b43af7434bcf8e6ca

SHA1值: 669738be2e3e8f7eb30f3c433430b6c7ee01eaa6

SHA256值: c3101e2228d089ed0094ecb5342ad92f3118e334411e40ccf8bd6b4ed124636d

## i APP 信息

App名称: 小蝴蝶的花园

包名: com.example.fwwzpxhng

主活动Activity: com.example.fwwzpxhng.MainActivity

安卓版本名称: 1.0.1

安卓版本: 1

## 🔍 域名线索

域名	服务器信息
www.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
plus.google.com	IP: 199.59.149.208 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
api.flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California

	<b>城市:</b> Mountain View <b>纬度:</b> 37.405991 <b>经度:</b> -122.078514
paktor1103.s3.ap-northeast-1.amazonaws.com	<b>IP:</b> 52.219.162.250 <b>所属国家:</b> Japan <b>地区:</b> Tokyo <b>城市:</b> Tokyo <b>纬度:</b> 35.689499 <b>经度:</b> 139.692322
flutter.dev	<b>IP:</b> 199.36.158.100 <b>所属国家:</b> United States of America <b>地区:</b> California <b>城市:</b> Mountain View <b>纬度:</b> 37.405991 <b>经度:</b> -122.078514
developer.android.com	<b>IP:</b> 142.250.217.110 <b>所属国家:</b> United States of America <b>地区:</b> California <b>城市:</b> Mountain View <b>纬度:</b> 37.405991 <b>经度:</b> -122.078514
github.com	<b>IP:</b> 20.205.243.166 <b>所属国家:</b> Singapore <b>地区:</b> Singapore <b>城市:</b> Singapore <b>纬度:</b> 1.289987 <b>经度:</b> 103.850281

## URL线索

URL信息	Url所在文件
-------	---------

<a href="https://plus.google.com/">https://plus.google.com/</a>	a2/p1.java
<a href="https://developer.android.com/guide/topics/permissions/overview">https://developer.android.com/guide/topics/permissions/overview</a>	io/flutter/plugin/platform/c.java
<a href="https://github.com/flutter/flutter/issues">https://github.com/flutter/flutter/issues</a> .	lib/armeabi-v7a/libflutter.so
<a href="https://paktor1103.s3.ap-northeast-1.amazonaws.com/paktor">https://paktor1103.s3.ap-northeast-1.amazonaws.com/paktor</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://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://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">https://github.com/flutter/flutter/issues</a> .	lib/x86_64/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
u0013android@android.com0 u0013android@android.com	x1/q.java
_cookie@13463476.fromsetcoo authenticationscheme@13463476.fromstring storationinformation@633124995.fromserial _list@0150898.of  _httpparser@13463476.responsepa _typeerror@0150898._create _list@0150898._ofgrowabl _list@0150898._ofefficie	

\_growablelist@0150898.\_ofarray  
\_double@0150898.fromintege  
\_growablelist@0150898.\_literal3  
\_future@4048458.immediate  
\_growablelist@0150898.\_literal  
\_growablelist@0150898.\_ofother  
\_link@14069316.fromrawpat  
\_growablelist@0150898.withcapaci  
\_timer@1026248.\_internal  
\_growablelist@0150898.\_literal6  
\_growablelist@0150898.\_literal5  
\_receiveportimpl@1026248.fromrawrec  
\_list@0150898.\_ofarray  
\_timer@1026248.periodic  
\_growablelist@0150898.\_literal2  
\_bigintimpl@0150898.from  
\_list@0150898.empty  
\_list@0150898.\_ofother  
\_bytebuffer@7027147.\_new  
\_directory@14069316.fromrawpat  
\_casterror@0150898.\_create  
\_compressednode@240137193.single  
\_invocationmirror@0150898.\_withtype  
ngstreamssubscription@4048458.zoned  
\_assertionerror@0150898.\_create  
\_nativesocket@14069316.normal  
\_growablelist@0150898.\_literal1  
\_uri@0150898.file  
\_uri@0150898.directory  
\_growablelist@0150898.\_literal8  
\_file@14069316.fromrawpat  
\_growablelist@0150898.\_literal4  
\_growablelist@0150898.\_ofgrowabl  
\_growablelist@0150898.of  
\_growablelist@0150898.generate  
\_uri@0150898.notsimple  
\_growablelist@0150898.\_literal7  
\_growablelist@0150898.\_ofefficie  
  
\_hashcollisionnode@240137193.fromcollis  
\_future@4048458.immediatee

lib/armeabi-v7a/libapp.so

receivenortimnl@1026248 fromrawrec

lib/x86\_64/libapp.so

_receiveportimpl@1026248.fromrawrec	lib/arm64-v8a/libflutter.so
appro@openssl.org	lib/arm64-v8a/libflutter.so
_receiveportimpl@1026248.fromrawrec	lib/arm64-v8a/libapp.so

## 手机线索

## 签名证书

APK已签名

v1 签名: True

v2 签名: True

v3 签名: True

找到 1 个唯一证书

主题: C=beijing, ST=beijing, L=beijing, O=ct1730794359713, OU=so1730794359713, CN=qqvi

签名算法: rsassa\_pkcs1v15

有效期自: 2024-11-05 08:12:41+00:00

有效期至: 2074-10-24 08:12:41+00:00

发行人: C=beijing, ST=beijing, L=beijing, O=ct1730794359713, OU=so1730794359713, CN=qqvi

序列号: 0x25aef004

哈希算法: sha512

md5值: a7a5e64e26d84322b742167de1b02604

sha1值: 5742d535e5a364bc4f1f0c1378c26be321123e2c

sha256值: fcbe7d01713d8b8237da7228d17ac483051dcdee9c6f532c9f405a120ab380db

sha512值: cfbcab271689487e4d254e95bab7a1a334c77c0ed5bf4483f49813a6cd46bd133264e37ae52120a617ca0b960ff580f577dd9aeeb06109357d06b4137f2aed82

公钥算法: rsa

密钥长度: 4096

指纹: ab3167d51aa9aec7a850456b3d0e864f45e52125af0761aaf6dee5b22e30d590

## 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.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.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.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前



android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
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.READ_PHONE_NUMBERS	危险		允许到设备的读访问的电话号码。这是 READ_PHONE_STATE 授予的功能的一个子集,但对即时应用程序公开
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.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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
android.permission.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
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
com.example.fwwzpxhng.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

---

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。