MoGua

落花伊人 1.1.1.APK 分析报告

APP名称: 落花伊人

包名:	com.example.demo
域名线索:	2条
URL线索:	2条
邮箱线索:	1条
分析日期:	2025年7月17日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 10_base.apk
文件大小: 47.6MB
MD5值: 06ae9b40afaf3824cc43199e61ef2981
SHA1值: a5ec0962e83ab9062c4755f0523bb2d9f1f9ed8c
SHA256值: cbc337a0b21f5615d037d0fb70480e0765cdb4bb78e67f30ed3afad66c12058f

APP 信息

App名称: 落花伊人
包名: com.example.demo
主活动Activity: com.example.demo.MainActivity
安卓版本名称: 1.1.1
安卓版本: 1

域名线索

域名	服务器信息
developer.android.com	**IP**: 142.251.33.78 **所属国家**: Canada **地区**: Ontario **城市**: Toronto **纬度**: 43.653660 **经度**: -79.382927
plus.google.com	**IP**: 157.240.21.9 **所属国家**: United States of America **地区**: California **城市**: Menlo Park **纬度**: 37.436935 **经度**: -122.193604

URL线索

URL信息	Url所在文件
https://plus.google.com/	a2/p1.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/c.java

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	x1/q.java

手机线索

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: C=lndedpyiryoco, ST=hczlfedurodwv, L=xmxuctzktqugn, O=trh1735383128655, OU=lcb1735383128655, CN=TG@apkfangdujiagu
签名算法: rsassa_pkcs1v15
有效期自: 2024-12-28 10:52:08+00:00
有效期至: 2074-12-16 10:52:08+00:00
发行人: C=lndedpyiryoco, ST=hczlfedurodwv, L=xmxuctzktqugn, O=trh1735383128655, OU=lcb1735383128655, CN=TG@apkfangdujiagu

序列号: 0x15b758bd
哈希算法: sha1
md5值: f0fa12df01e1bfcee2dfdb1c28247802
sha1值: b26f3a6880258935bdeac8a51152f4aea28bd4c4
sha256值: 749734517a7095502f776e8539c5c3b5719e9eac612503fa485ae2886a88a66d
sha512值: 4a034df22ae197ff25d9259c9cd1db31991904e6c01c032f918928faf53ec075645dc8f4c417741aab2e01a7d7fd4760cbd315c54574f152218684c51a5aad2d
公钥算法: rsa
密钥长度: 1024
指纹: 6b44f793d156bb9e4bacd527686b4b87d57592a6e2cf803e6fc20c60917ad093

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

	是		

向手机申请的权限	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.demo.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信