MoGua

莘悦社区 24.16.92.APK 分析报告

APP名称:	莘悦社区

包名:	me.Srs1UgiD.MuUacID7
域名线索:	2条
URL线索:	6条
邮箱线索:	0条
分析日期:	2024年10月16日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: xinyueshequ.APK
文件大小: 25.66MB
MD5值: 9852ee61913acc86115b65556dba372c
SHA1值: 8ad9dc7e2b15de3bd8fec29db1b0daf445095ef5
SHA256值: f28795b5eba8853e457286b93183e7b311d6f4edd5f36bfd60ae54dd4442c96a

APP 信息

App名称: 莘悦社区
包名: me.Srs1UgiD.MuUacID7
主活动Activity: .main
安卓版本名称: 24.16.92
安卓版本: 509

域名线索

域名	服务器信息
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
schemas.android.com	没有服务器地理信息.

URL线索

URL**信息**	Url**所在文件**

https://github.com/kongzue/DialogX/wiki	com/kongzue/dialogx/DialogX.java
https://github.com/kongzue/DialogX	com/kongzue/dialogx/interfaces/BaseDialog.java
https://github.com/kongzue/DialogX	com/kongzue/dialogx/impl/ActivityLifecycleImpl.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.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: True
找到 1 个唯一证书
主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2024-10-15 08:18:14+00:00
有效期至: 2124-09-21 08:18:14+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x1d139060a25177fa
哈希算法: sha256
md5值: b235968feaa2775ef601f4f70a10efe0
sha1值: 9c03bfc68c3a1e4ec75c288bcaafa4a75145c8bc
sha256值: af001af9b62676e6bcdba15633cf7f00551ae0f66eba59884f4bb1e56a2195c2

sha512值: a312ce2db5bec9813b6931481cec84b1dd0e32e058ed157d595466816062687a61929dcc2fe69b046537b9f9752e9bd01453e77e1f98a6e46c223575fb2bd264
公钥算法: rsa
密钥长度: 2048
指纹: d6ed3c9f5e522196add6c6422a992d5a661cac2b00b90cedbbccc59f72483dfc

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.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_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.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.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_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.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_CALL_LOG	危险		允许应用程序读取用户的通话日志
android.permission.GET_PACKAGE_SIZE	正常	测量应用程序存储空间	允许应用程序找出任何包使用的空间

应用内通信