MoGua

小嘿逗 2.1.0.APK 分析报告

APP名称:	小嘿逗
包名:	com.example.bddd
域名线索:	16条
URL线索:	21条
邮箱线索:	1条
分析日期:	2025年1月9日

分析平台: 摸瓜APK反编译平台

文件信息

文件名: 小嘿逗_2.1.0 (1).apk
文件大小: 10.06MB
MD5值: 2da21ca50cfb1639b68463a5b18d7e35
SHA1值: 2df46bc03e10f894a5426d27a62c308d9467ae03
SHA256值: f982a4acde03992431cd6988bbcdf9683fee0306c054f853e1ffc32b5a1bb1b5

APP 信息

App名称: 小嘿逗
包名: com.example.bddd
主活动Activity: com.example.bddd.MainActivity
安卓版本名称: 2.1.0
安卓版本: 1

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

live.douyin.comaid6383live	没有服务器地理信息.
127.0.0.1	IP: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
www.slf4j.org	IP: 195.15.222.169 **所属国家**: Switzerland **地区**: Geneve **城市**: Carouge **纬度**: 46.180931 **经度**: 6.138709
www.douyin.com	IP: 121.17.122.100 **所属国家**: China **地区**: Hebei **城市**: Hengshui **纬度**: 37.732220 **经度**: 115.701157
www.w3.org	IP: 104.18.22.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
dy.l9527.com	IP: 8.130.137.241 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
xml.apache.org	IP: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
groups.google.com	IP: 199.16.158.182 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
apache.org	IP: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

x.y	没有服务器地理信息.
jsoup.org	**IP**: 172.67.187.139 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.baidu.com	**IP**: 110.242.69.21 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
projectlombok.org	**IP**: 104.21.3.156 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
xml.org	**IP**: 104.239.240.11 **所属国家**: United States of America **地区**: Texas **城市**: Windcrest **纬度**: 29.499678 **经度**: -98.399246
live.douyin.com	**IP**: 61.182.131.172 **所属国家**: China **地区**: Hebei **城市**: Zhangjiakou **纬度**: 40.810024 **经度**: 114.879349

URL线索

URL**信息**	Url**所在文件**
http://xml.apache.org/xslt	cn/hutool/core/util/XmlUtil.java
http://apache.org/xml/features/disallow-doctype-decl	cn/hutool/core/util/XmlUtil.java
http://xml.org/sax/features/external-general-entities	cn/hutool/core/util/XmlUtil.java
http://xml.org/sax/features/external-parameter-entities	cn/hutool/core/util/XmlUtil.java
http://apache.org/xml/features/nonvalidating/load-external-dtd	cn/hutool/core/util/XmlUtil.java

https://dy.l9527.com/api/user/index	com/example/bddd/ui/common/Pfun.java
https://dy.l9527.com/api/user/login	com/example/bddd/ui/login/LoginActivity.java
https://live.douyin.com/	com/example/bddd/ui/service/FetchDouYin.java
https://live.douyin.com&aid=6383&live_id=1&did_rule=3&debug=false&maxCacheMessageNumber=20&endpoint=live_pc&support_wrds=1&im_path=/webcast/im/fetch/&user_unique_id=	com/example/bddd/ui/service/FetchDouYin.java
https://live.douyin.com/webcast/im/fetch/? version_code=180800&resp_content_type=protobuf&did_rule=3&device_id=&device_platform=web&cookie_enabled=true&screen_width=1536&screen_height=864&browser_language=zh-CN&browser_platform=Win32&browser_name=Mozilla&browser_version=5.0	com/example/bddd/ui/service/FetchDouYin.java
https://www.baidu.com	com/example/bddd/ui/home/HomeFragment.java
https://live.douyin.com/	com/example/bddd/ui/home/HomeFragment.java
https://www.douyin.com/root/live/	com/example/bddd/ui/home/HomeFragment.java
https://www.douyin.com/follow/live/	com/example/bddd/ui/home/HomeFragment.java
https://dy.l9527.com/index/index/paiduan?hex=	com/example/bddd/ui/home/HomeFragment.java
https://live.douyin.com/(\\d+)	com/example/bddd/ui/api/DouyinApis.java
https://live.douyin.com/	com/example/bddd/ui/api/DouyinApis.java
https://dy.l9527.com/api/user/login	com/example/bddd/data/LoginDataSource.java
https://projectlombok.org/LICENSE	lombok/core/Main.java
http://x.y/a/	lombok/core/configuration/ConfigurationFile.java
https://projectlombok.org	lombok/installer/Installer.java
http://groups.google.com/group/project-lombok	lombok/installer/eclipse/EclipseProductLocation.java
https://projectlombok.org/not/calculated	lombok/javac/JavacAST.java
https://projectlombok.org/features/experimental/FieldNameConstants	lombok/javac/handlers/HandleFieldNameConstants.java
https://projectlombok.org/not/calculated	lombok/eclipse/EclipseAST.java
https://projectlombok.org	lombok/eclipse/agent/PatchFixesShadowLoaded.java
https://projectlombok.org/	lombok/eclipse/agent/PatchFixesShadowLoaded.java
https://projectlombok.org/features/experimental/FieldNameConstants	lombok/eclipse/handlers/HandleFieldNameConstants.java
https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection	org/java_websocket/AbstractWebSocket.java

http://'	org/jsoup/helper/HttpConnection.java
https://'.	org/jsoup/helper/HttpConnection.java
https://jsoup.org/cookbook/extracting-data/working-with-urls	org/jsoup/helper/HttpConnection.java
http://undefined/	org/jsoup/helper/HttpConnection.java
http://127.0.0.1	org/mozilla/javascript/tools/debugger/Dim.java
http://www.slf4j.org/codes.html	org/slf4j/MDC.java
http://www.slf4j.org/codes.html	org/slf4j/LoggerFactory.java

邮箱线索

邮箱地址	所在文件
auth-agent@openssh.com	cn/hutool/extra/ssh/ChannelType.java

手机线索

手机号	所在文件
13027771553	com/example/bddd/data/LoginDataSource.java
17179869184	lombok/javac/handlers/JavacHandlerUtil.java
17179869184	lombok/javac/handlers/HandleDelegate.java
17179869184	lombok/delombok/PrettyPrinter.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=1, OU=1, O=1, L=1, ST=1, C=1
签名算法: rsassa_pkcs1v15
有效期自: 2024-12-06 07:12:16+00:00
有效期至: 2049-11-30 07:12:16+00:00
发行人: CN=1, OU=1, O=1, L=1, ST=1, C=1

序列号: 0x1
哈希算法: sha256
md5值: 8f6df00e3caed924cc0366bc2c754585
sha1值: 72808480aa155395ced87cd49e78d6cdfeed53b1
sha256值: 8837805192e35da162fd8dec063fce75b55184dd4f37c4d3a9fc12340572c3fb
sha512值: b13cbf4d1319d419d20c524ee14eedc3f37f2abc5ae95dd7507e23f0bb057fc90b3dcd5cb29e5adc0f76334bd303bd28a567dc27beaa016ddb95cfccfa31db21
公钥算法: rsa
密钥长度: 2048
指纹: 44b3d75431061c1b5410c611758786c544b7f7111316bb6af4658f87ab19dc40

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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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.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.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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。

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
android.permission.REQUEST_COMPANION_RUN_IN_BACKGROUND	正常		允许配套应用在后台运行。
android.permission.REQUEST_COMPANION_USE_DATA_IN_BACKGROUND	正常		允许配套应用在后台使用数据。
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.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
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.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.BLUETOOTH_CONNECT	未知	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH_SCAN	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.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference
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

应用内通信