MoGua

蜜穴B城 v1.0.4.APK 分析报告

APP名称: 蜜穴B城

包名:	cc.assadd.xssdaj
域名线索:	8条
URL线索:	9条
邮箱线索:	1条
分析日期:	2025年5月23日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: E48GBCZL.apk
文件大小: 7.82MB
MD5值: 54ab86f2ae75c18d1059e114925ecf93
SHA1值: 22c63e0e15dc2e45ccd06079053f5c1315374ed3
SHA256值: 64a9593970bc15320b2aff4ec83d3c8cb3427d928f0acafcd4f4c3902441ce6e

APP 信息

App名称: 蜜穴B城
包名: cc.assadd.xssdaj
主活动Activity: cc.assadd.xssdaj.MainActivity
安卓版本名称: v1.0.4
安卓版本: 4

域名线索

域名	服务器信息
8.136.101.204	**IP**: 8.136.101.204 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
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
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
www.openssl.org	**IP**: 23.221.101.16 **所属国家**: Colombia **地区**: Distrito Capital de Bogota **城市**: Bogota **纬度**: 4.609710 **经度**: -74.081749
exoplayer.dev	**IP**: 185.199.111.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
ns.adobe.com	没有服务器地理信息.
jojolive-test.s3.ap-southeast-1.amazonaws.com	**IP**: 52.219.184.42 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
wememao.com	**IP**: 172.67.155.53 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

URL线索

URL信息	Url所在文件
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	p016implements/Cprotected.java
http://8.136.101.204/v/	p024protected/Cif.java
http://www.w3.org/ns/ttml	l0/Cfor.java
https://wememao.com	cc/assadd/xssdaj/WebActivity.java
http://ns.adobe.com/xap/1.0/	j/Cdo.java
http://xml.apache.org/xslt	com/blankj/utilcode/util/LogUtils.java
https://jojolive-test.s3.ap-southeast-1.amazonaws.com/vip/2022-02-25/14/4c053e1ca87d459ea9d19b73d7297a0f.mp4	com/casx/lib_jzvideo/tiktok/TikTokRecyclerViewAdapter.java
https://exoplayer.dev/issues/cleartext-not-permitted	q0/Cthrows.java
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so

邮箱线索

邮箱地址	所在文件
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so

手机线索

手机号	所在文件
18222222222	k/Cnew.java
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.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: C=11, ST=11, L=11, O=11, OU=11, CN=11
签名算法: rsassa_pkcs1v15
有效期自: 2023-08-18 13:08:11+00:00
有效期至: 2048-08-11 13:08:11+00:00
发行人: C=11, ST=11, L=11, O=11, OU=11, CN=11
序列号: 0x5c88e96
哈希算法: sha256
md5值: 7da1eaace28ee292a63e8d6a4257d2d0
sha1值: fbf498fbead1af3dc6172bbe58c1e5343ce1135c
sha256值: c46f3be3331fcb19a7f965786b315a1f8c2658644e75452c7415abd357ea56a2
sha512值: 36e74e3f9182a4aa2a81dd55a5bc9f0377fa25e58a98ebc792b19f3b0a2b8c59924cff9d014d963922e40edbbcdf96b69e8251d47204a7423227a80311ec332a
公钥算法: rsa
密钥长度: 2048
指纹: f31029eed123691e8c685b29d2fbc0924b7737b58f9fb130c7f5591569685d09

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.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.ACCESS_DOWNLOAD_MANAGER	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由

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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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

应用内通信
