



MoGua

扩大内需 1.0.0.APK 分析报告



APP名称:

扩大内需

包名:	j6bf2.xvvn_.nbxbz
域名线索:	1条
URL线索:	1条
邮箱线索:	0条
分析日期:	2025年6月18日
分析平台:	摸瓜APK反编译平台

文件名: KDNX6828.apk
文件大小: 10.53MB
MD5值: c1a2d941c1c6e63808cf813ea4257470
SHA1值: 38b975ea2e04daf18f1c6866a6e8d27dd7956510
SHA256值: 3054e1ad407b15a2d2bec4d0ff94c656b7e7b149cd0eb64c1bd1ded4d1df09fa

i APP 信息

App名称: 扩大内需
包名: j6bf2.xvvn_.nbxbz
主活动Activity: com.myapp.app.MainActivity
安卓版本名称: 1.0.0
安卓版本: 1

🔍 域名线索

域名	服务器信息
wx.tenpay.com	IP: 210.22.240.151 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948

🌐 URL线索

URL信息	Url所在文件
https://wx.tenpay.com	IMuAHx_6/QxJ9d_1/IFxWkV_5/QxJ9d_1/KQgRr5e_0.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=adminhg131u, ST=adminhg131u, L=adminhg131u, O=adminhg131u, OU=adminhg131u, CN=adminhg131u

签名算法: rsassa_pkcs1v15

有效期自: 2025-06-05 06:49:22+00:00

有效期至: 2125-05-12 06:49:22+00:00

发行人: C=adminhg131u, ST=adminhg131u, L=adminhg131u, O=adminhg131u, OU=adminhg131u, CN=adminhg131u

序列号: 0x541bac6b

哈希算法: sha256

md5值: 8a5619186c7435df906d07a5d997d8b6

sha1值: d6d9cd938122719b70b6188bba135065e4fbd3f

sha256值: c59162e3d485152da5a2660c82348bdd07b591cbb109d23d94df085470d9d0b8

sha512值: bc2e28cc7907a8168584c2a22b5eae7dbd7e4cfb17d7c1c15fb0cccead5dfea2cda1d23e7ae1cd980977afed3aec3bb815343756b81ce1adecd152b834a3e084

公钥算法: rsa

密钥长度: 1024

指纹: c073af9eb0c74ff256bd479275357c0dd5fe2b2ca9c0365d51672aae0b711088

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.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

应用内通信