MoGua

药 1.0.APK 分析报告

APP名称: 药

包名:	com.yaolwly.xzapp
域名线索:	0条
URL线索:	0条
邮箱线索:	0条
分析日期:	2025年6月17日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: yao.apk
文件大小: 3.09MB
MD5值: 20b7633f750f48c9c5be2cd898fbc439
SHA1值: 68bb55a13c3f469480ac2c028ce9862ea4a47ff7
SHA256值: 9d3b89c37c079eebcfd896c40a4defcdd4bf1495e0e8170d4cc6607c97d73147

APP 信息

App名称: 药
包名: com.yaolwly.xzapp
主活动Activity: mt.webapp.MainActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

URL线索

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=CN, CN=yaolwly

签名算法: rsassa_pkcs1v15
有效期自: 2025-05-01 00:40:06+00:00
有效期至: 2125-04-07 00:40:06+00:00
发行人: C=CN, CN=yaolwly
序列号: 0x4ae9b8a8
哈希算法: sha256
md5值: f45bce90788c4be7439e44034ce35c86
sha1值: d77101048a0da776ba71c21857d6d64241cb9003
sha256值: 5a3034a5dc3000ae71eb9710f5fc334f655ca68da54a0de2a25af9b9fd058a65
sha512值: 044e20db9339d8c4b85ead0b92f6ad0a6c8f35650bc9b5cc9bfbd9d629f0359042c716f6235a127f6ec22fa0cb9157ce73bb5530a9adf9f4eaf838a750c72326
公钥算法: rsa
密钥长度: 2048
指纹: 4752de5857ba645c4a0e00f7557d7e9402402b3b09c3aa9bf70457995a27b815

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.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.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_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.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_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径

android.permission.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
mt.webapp.MainActivity	Schemes: http://, https://, mtapp://,
