MoGua

OAX 1.0.8.APK 分析报告

APP名称:	OAX

包名:	org.oax100.app
域名线索:	3条
URL线索:	2条
邮箱线索:	0条
分析日期:	2025年8月27日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: OAX(1).apk
文件大小: 3.3MB
MD5值: ea1d7e6d331135e58a87e043e2627b03
SHA1值: f664f7fd14193ef84e46a4ec11f93010961d9e38
SHA256值: 9248c6044bd33930157e37816486697634bea803eadf543ec67d653612e294b9

APP 信息

App名称: OAX
包名: org.oax100.app
主活动Activity: com.lt.app.MainActivity
安卓版本名称: 1.0.8
安卓版本: 108

域名线索

域名	服务器信息
www.baidu.com	**IP**: 110.242.68.3 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
1.12.12.12	**IP**: 1.12.12.12 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
dns.alidns.com	**IP**: 223.6.6.6 **所属国家**: China

dns.alidns.com	**地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583

URL线索

URL信息	Url所在文件
https://www.baidu.com/favicon.ico?\	g4/f1.java
https://dns.alidns.com/dns-query	h4/q.java
https://1.12.12.12/dns-query	h4/q.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: False
找到 1 个唯一证书
主题: C=CN, O=COM, OU=IT, CN=QMMI
签名算法: rsassa_pkcs1v15
有效期自: 2024-06-17 12:56:37+00:00
有效期至: 2124-05-24 12:56:37+00:00

发行人: C=CN, O=COM, OU=IT, CN=QMMI
序列号: 0x5a364296
哈希算法: sha256
md5值: 45503e9e70cb6c9caeb7d736dfd448e5
sha1值: 6c8f0d1ccfa93309278d525b892fe764bf4c8cde
sha256值: 37fbb153fa89b4085a84a7ee093348e63387e4ff287be63e4d50a51885844016
sha512值: c453e7cc0fb45cd621294ce6df0b776983a2d89c9d2417a023ac49e1cdcf76fd611cca1e50c064713d753115a6e529eecc40fd6675ef683740946ce3a8930ce6
公钥算法: rsa
密钥长度: 2048
指纹: 503acb10372ad0f5ba877aded26b7a58e97cdfb5e209a404a36571b422dd2c64

🔑 硬编码敏感信息

可能的敏感信息
"http_auth" : "HTTP Authentication"
"http_auth_p" : "Password"
"http_auth_u" : "User Name"
"p_rcpush_mzAppKey" : ""
"p_rcpush_opAppKey" : ""
"p_rcpush_opAppSecret" : ""
"p_rcpush_vvAppKey" : ""
"p_rcpush_xmAppKey" : ""
"p_weibo_appkey" : ""
"http_auth" : "HTTP 身份验证"

"http_auth_p" : "密码"
"http_auth_u" : "用户名"
"http_auth" : "HTTP 身份驗證"
"http_auth_p" : "密碼"
"http_auth_u" : "用戶名"
"http_auth" : "HTTP 身份驗證"
"http_auth_p" : "密碼"
"http_auth_u" : "用戶名"

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.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.ACCESS_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_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
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。
org.oax100.app.permission.YM_APP	未知	Unknown permission	Unknown permission from android reference
org.oax100.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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.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.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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference

android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.lt.app.JumpActivity	Schemes: ltapp417892://,
