MoGua

世梅链 2.0.2.APK 分析报告

APP名称:	世梅链
包名:	com.appheader.zhxf.pro.sml
域名线索:	8条
URL线索:	5条

邮箱线索:	1条
分析日期:	2025年3月29日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: shimei2.0.1.apk
文件大小: 38.05MB
MD5值: 4252e7babb0d6acdd9ef9bfe5e2bdae0
SHA1值: 3cd24f7c9c255b4dd54a8700ddadaec61d827e13
SHA256值: 699a07307cd83c68862204749a3c69db51ae60deb405f2e9479dd3cccf92beb7

APP 信息

App名称: 世梅链
包名: com.appheader.zhxf.pro.sml
主活动Activity: com.lt.app.MainActivity
安卓版本名称: 2.0.2
安卓版本: 202

域名线索

域名	服务器信息
opensource.org	**IP**: 199.16.172.170 **所属国家**: United States of America **地区**: Texas **城市**: San Antonio **纬度**: 29.425426 **经度**: -98.489349
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
www.w3.org	**IP**: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
api.xiangkanwang.com	**IP**: 47.92.158.243 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
img.yzcdn.cn	**IP**: 112.84.130.73 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
m.baidu.com	**IP**: 110.242.68.10 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
cdn.xiangkanwang.com	**IP**: 175.22.9.220 **所属国家**: China **地区**: Jilin **城市**: Changchun **纬度**: 43.880001 **经度**: 125.322777

img.alicdn.com	**IP**: 125.39.135.47 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102

URL线索

URL**信息**	Url**所在文件**
https://img.alicdn.com/imgextra/i3/O1CN01yaPRML1GyyqsOZP7R_!!6000000000692-1-tps-1200-432.gif	Mogua Engine V2
http://www.w3.org/200/svg	Mogua Engine V2
https://m.baidu.com/s?from=100&word=%E9%A6%99%E6%B8%AF%E5%90%8D%E5%AA%9B%E9%81%AD%E8%B0%8B%E6%9D%80%E8%AD%A6%E6%96%B9%E5%B7%B2%E6%8B%98%E6%8D%953%E4%BA%BA	Mogua Engine V2
https://m.baidu.com/s?from=100&word=%E5%86%8D%E7%8E%A9%E4%B8%8B%E5%8E%BB%E9%98%BF%E5%A7%A8%E5%B0%B1%E5%88%B0%E5%AE%B6%E4%BA%86	Mogua Engine V2
https://m.baidu.com/s?from=100&word=%E8%AE%B8%E5%B5%A9+%E6%BC%94%E5%94%B1%E4%BC%9A	Mogua Engine V2
https://m.baidu.com/s?from=100&word=%E8%B5%B5%E7%BB%A7%E4%BC%9F%E8%AF%B4%E4%B8%BB%E5%9C%BA%E6%89%93%E7%90%83%E5%A4%AA%E8%88%92%E6%9C%8D%E4%BA%86	Mogua Engine V2
https://m.baidu.com/s?from=100&word=%E5%A5%B3%E5%AD%90%E6%A8%A1%E4%BB%BF%E7%BD%91%E7%BA%A2%E7%A9%BF%E6%90%AD%E9%81%AD%E5%AF%B9%E6%96%B9%E7%B2%89%E4%B8%9D%E7%BD%91%E6%9A%B4	Mogua Engine V2
https://m.baidu.com/s?from=100&word=%E5%85%AD%E5%85%AC%E4%B8%BB%E8%B5%9E%E5%A4%8F%E8%8A%B1	Mogua Engine V2

https://m.baidu.com/s?from=100&word=%E6%9D%8E%E5%BC%BA%E8%A2%AB%E4%BB%BB%E5%91%BD%E4%B8%BA%E5%9B%BD%E5%8A%A1%E9%99%A2%E6%80%BB%E7%90%86	Mogua Engine V2
https://m.baidu.com/s?from=100&word=%E6%9D%A8%E7%B4%AB%E4%B8%8A%E6%B5%B7%E6%9C%BA%E5%9C%BA%E8%B7%AF%E9%80%8F	Mogua Engine V2
https://m.baidu.com/s?from=100&word=%E5%BC%A0%E7%9C%9F%E6%BA%90%E4%BE%A7%E6%8B%8D	Mogua Engine V2
https://m.baidu.com/s?from=100&word=%E5%8F%AA%E6%9C%89%E6%B1%AA%E5%B3%B0%E5%9C%A8%E6%89%93%E6%8A%98	Mogua Engine V2
https://m.baidu.com/s?from=100&word=%25INPUT_KEYWORD%25	Mogua Engine V2
https://api.xiangkanwang.com/v1/check_url?url=	Mogua Engine V2
https://cdn.xiangkanwang.com/frontend/static/warning.html?from=	Mogua Engine V2
https://img.yzcdn.cn/vant/coupon-empty.png	Mogua Engine V2
http://www.w3.org/2000/svg	Mogua Engine V2
https://img.yzcdn.cn/vant/empty-image-	Mogua Engine V2
https://img.yzcdn.cn/vant/share-icon-	Mogua Engine V2
https://github.com/Tencent/vConsole)	Mogua Engine V2
	Mogua

http://opensource.org/licenses/MIT	Engine V2
https://github.com/Tencent/vConsole	Mogua Engine V2
https://github.com/Tencent/vConsole.git	Mogua Engine V2
http://www.w3.org/1999/xlink	Mogua Engine V2
http://www.w3.org/2000/svg	Mogua Engine V2
http://www.w3.org/1998/Math/MathML	Mogua Engine V2

邮箱线索

邮箱地址	所在文件
hilongjw@gmail.com	Mogua Engine V2

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: E=sdudhans@gmail.com, L=chengdu, ST=sichuan, C=CN, OU=sm, O=shimei, CN=shimeikeji
签名算法: rsassa_pkcs1v15
有效期自: 2024-04-20 17:33:45+00:00
有效期至: 2054-04-21 17:33:45+00:00
发行人: E=sdudhans@gmail.com, L=chengdu, ST=sichuan, C=CN, OU=sm, O=shimei, CN=shimeikeji

序列号: 0x594d0000000000e0737f
哈希算法: sha256
md5值: 1161dccbb429da83adb5561c1cf33f67
sha1值: 5bc2f1b3bb7f42fca43b180b766497fde5051dfe
sha256值: 537437948325e609ec5948c62a5777ab97a477ca50b70ae7b41ef1b833fb3a27
sha512值: b2b847171f053097fd05fc5895579a89d88936a24abf6872b9104c480b252860642fda5022c78c563195865260df993995dec3d58750bb298897fc1ee3f3aaad
公钥算法: rsa
密钥长度: 2048
指纹: 1ae0ab8bb66d6fd3e75f45259c92003103cc9fad7db58916ea278c36bd7badae

🔑 硬编码敏感信息

可能的敏感信息
"bdreader_author" : "作者"
"common_menu_authority_management" : "权限管理"
"err_proxy_auth_desc_txt" : "407-代理需要认证"
"http_auth" : "HTTP Authentication"
"http_auth_p" : "Password"
"http_auth_u" : "User Name"
"ksad_ad_default_author" : "@可爱的广告君创造的原声"
"ksad_ad_default_username" : "@可爱的广告君"
"novel_buy_free_ad_auth_dialog_btn" : "800书豆开通"
"novel_buy_free_ad_auth_dialog_desc" : "30天内免广告畅读正版小说"
"novel_buy_free_ad_auth_dialog_rule_desc" : "1.充值并支付800书豆，即可开通免广告特权，享受30天免广告权益。 2.iOS平台仅限AppStore支付方式购买，您可前往AppStore账户设置选择支付宝、微信、银联卡等支付方式。 3.安卓平台通过小说书豆充值中心，充值并支付800书豆购买。 4.购买后即可免广告阅读全场小说，原有付费小说仍需付费购买，购买后免广告阅读。 5.扣款完成后免广告特权即刻生效，有效期30天；若未直接生效，请等待30分钟，请勿在短时间内重复尝试购买。 6.购买后特权剩余有效期可通过书籍详情页上方书籍介绍部分实时查看。 7.通过AppStore充值购买的免广告特权，在非iOS端的百度APP不能使用；在安卓书豆充值中心充值购买的免广告特权，在非安卓端的百度APP不能使用。 8.本特权开通后不支持退款，敬请谅解。 9.本特权不支持百度帮你付折扣和使用书券。 10.若有其他特权购买相关问题，可咨询百度APP客服。 11.在法律允许范围内，百度对本特权产品享有解释权。 "
"novel_buy_free_ad_auth_dialog_rule_title" : "规则说明"
"novel_buy_free_ad_auth_dialog_title" : "开通免广告特权"
"novel_buy_free_ad_auth_remind_time_postfix" : "后到期，续费>"

"novel_buy_free_ad_auth_remind_time_prefix" : "免广告有效期还剩： "

"novel_buy_free_ad_auth_remind_time_prefix_1" : "去广告特权倒计时：%1$s"

"novel_buy_free_ad_auth_rule_dialog_title" : "规则说明"

"novel_layout_buy_free_ad_auth_remind_time_1" : "209"

"novel_layout_buy_free_ad_auth_remind_time_2" : "37"

"novel_layout_buy_free_ad_auth_remind_time_unit_1" : "小时"

"novel_layout_buy_free_ad_auth_remind_time_unit_2" : "分钟"

"open_histroy_private_mode" : "搜索历史"

"p_rcpush_mzAppKey" : ""

"p_rcpush_opAppKey" : ""

"p_rcpush_opAppSecret" : ""

"p_rcpush_vvAppKey" : ""

"p_rcpush_xmAppKey" : ""

"p_u_appkey" : "66249356cac2a664de20e2e6"

"p_weibo_appkey" : ""

"reader_setting_volume_key" : "音量键翻页"

"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"

"http_auth" : "HTTP 身份验证"

"http_auth_p" : "密码"
"http_auth_u" : "用户名"

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。
android.permission.PACKAGE_USAGE_STATS	合法	更新组件使用统计	允许修改收集的组件使用统计。不供普通应用程序使用

android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
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.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.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
com.appheader.zhxf.pro.sml.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	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
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.SET_WALLPAPER	正常	设置壁纸	允许应用程序设置系统壁纸
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
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
com.appheader.zhxf.pro.sml.permission.YM_APP	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_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
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

com.google.android.gms.permission.AD_ID	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: ltapp410483://,
com.baidu.searchbox.discovery.novel.SchemeTransferActivity	Schemes: baiduboxsdk://, Hosts: novel,
com.hzcj.activityComm.SchemeActivity	Schemes: com.appheader.zhxf.pro.sml.hzcj.novel://,
com.aggregate.searchlibrary.search.AggregateSearchActivity	Schemes: aggregatesearch://, Hosts: keyword,