MoGua

小太妹 1.9.8.APK 分析报告

APP名称: 小太妹

包名:	com.ytmomoiw.yrcaodbbvineleiesulibmffipfqdbggxnteb
域名线索:	33条
URL线索:	43条
邮箱线索:	1条
分析日期:	2025年10月9日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: wam03df1.apk
文件大小: 15.52MB

MD5值: df4e3c6a3032d7a621263edb099f2dcf
SHA1值: 34891fabfae997d746471aeaa308810515706316
SHA256值: 7168cd4edb565f95ee9079b7ac13a6d7d12721293e53e28bb8b4c17e08605d61

APP 信息

App名称: 小太妹
包名: com.ytmomoiw.yrcaodbbvineleiesulibmffipfqdbggxnteb
主活动Activity: com.limit.cache.ui.page.main.WelComeActivity
安卓版本名称: 1.9.8
安卓版本: 198

域名线索

域名	服务器信息
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
errnewlog.umeng.com	**IP**: 223.109.148.180 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
developer.umeng.com	**IP**: 59.82.29.249 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583

weibo.com	**IP**: 116.133.8.18 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
pslog.umeng.com	**IP**: 59.82.60.44 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
alist.ttpvi.com	**IP**: 52.139.152.67 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
ulogs.umeng.com	**IP**: 223.109.148.176 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
plus.google.com	**IP**: 108.160.162.109 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
alist.dglago.com	**IP**: 20.189.74.77 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong

	纬度: 22.285521 **经度**: 114.157692
1.1.1.1	**IP**: 1.1.1.1 **所属国家**: United States of America **地区**: California **城市**: San Jose **纬度**: 37.339390 **经度**: -121.894958
alist.6ay26b.com	**IP**: 154.19.167.111 **所属国家**: United States of America **地区**: District of Columbia **城市**: Washington **纬度**: 38.901566 **经度**: -77.050781
alogsus.umeng.com	**IP**: 223.109.148.130 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
xtm99.top	**IP**: 91.195.240.12 **所属国家**: Germany **地区**: Nordrhein-Westfalen **城市**: Koeln **纬度**: 50.933346 **经度**: 6.949720
ulogs.umengcloud.com	**IP**: 223.109.148.176 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
	IP: 203.119.145.45 **所属国家**: China

ucc.umeng.com	**地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
cnlogs.umeng.com	IP: 223.109.148.176 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
alist.wyx0429.com	IP: 112.28.188.240 **所属国家**: China **地区**: Anhui **城市**: Hefei **纬度**: 31.863815 **经度**: 117.280830
resolve.umeng.com	IP: 223.109.148.176 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
alist.zhwizh.com	IP: 202.79.172.132 **所属国家**: Korea (Republic of) **地区**: Seoul-teukbyeolsi **城市**: Seoul **纬度**: 37.566311 **经度**: 126.977203
ns.adobe.com	没有服务器地理信息.
h5.dev.test.ggbba.top	没有服务器地理信息.
	IP: 223.109.148.180 **所属国家**: China **地区**: Jiangsu

errlog.umeng.com	**城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
aspect-upush.umeng.com	**IP**: 223.109.148.176 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
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
aria.laoyuyu.me	没有服务器地理信息.
utoken.umeng.com	**IP**: 223.109.148.139 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
schemas.android.com	没有服务器地理信息.
errnewlogos.umeng.com	**IP**: 47.246.110.96 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
	IP: 47.246.110.96 **所属国家**: Singapore **地区**: Singapore

errlogos.umeng.com	**城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
www.obao22.com	没有服务器地理信息.
alogus.umeng.com	**IP**: 223.109.148.176 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
alist.hbhaojing.com	**IP**: 218.11.6.230 **所属国家**: China **地区**: Hebei **城市**: Shijiazhuang **纬度**: 38.041599 **经度**: 114.478081
alist.zhangdaer.com	**IP**: 218.11.6.230 **所属国家**: China **地区**: Hebei **城市**: Shijiazhuang **纬度**: 38.041599 **经度**: 114.478081

URL线索

URL**信息**	Url**所在文件**
https://aria.laoyuyu.me/aria_doc/create/any_java.html	com/arialyy/aria/core/Aria.java
https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/download/DownloadReceiver.java

https://github.com/AriaLyy/Aria/issues/597	com/arialyy/aria/core/download/m3u8/M3U8Option.java
https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/upload/UploadReceiver.java
https://errnewlogos.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/controller/ControllerCenter.java
https://errnewlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/controller/ControllerCenter.java
https://errnewlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/d/c.java
http://xml.apache.org/xslt	com/blankj/utilcode/util/f.java
http://schemas.android.com/apk/res/android	com/limit/cache/widget/MoMoTabLayout.java
https://h5.dev.test.ggbba.top/dd/%E6%97%B6%E9%97%B4%E9%97%AA%E7%83%81%E6%88%90%E5%93%81.png	com/limit/cache/widget/MoMoTabLayout.java
https://alist.hbhaojing.com	com/limit/cache/ui/page/main/WelComeActivity.java
https://alist.zhangdaer.com	com/limit/cache/ui/page/main/WelComeActivity.java
https://alist.wyx0429.com	com/limit/cache/ui/page/main/WelComeActivity.java
https://alist.6ay26b.com	com/limit/cache/ui/page/main/WelComeActivity.java
https://alist.dglago.com	com/limit/cache/ui/page/main/WelComeActivity.java
https://alist.ttpvi.com	com/limit/cache/ui/page/main/WelComeActivity.java
https://alist.zhwizh.com	com/limit/cache/ui/page/main/WelComeActivity.java
https://h5.dev.test.ggbba.top/dd/%E4%BB%B7%E6%A0%BC%E6%88%90%E5%93%81.png	com/limit/cache/ui/page/seckill/SeckillAdapter.java
https://h5.dev.test.ggbba.top/dd/%E4%BB%B7%E6%A0%BC%E6%88%90%E5%93%81.png	com/limit/cache/ui/page/seckill/SeckillDetailActivity.java
https://www.obao22.com/?i_code=	com/limit/cache/ui/fragment/web/AppWebFragment.java

https://1.1.1.1/	com/limit/cache/apphttp/DNSClient.java
https://aspect-upush.umeng.com/occa/v1/event/report	com/umeng/analytics/pro/aq.java
https://cnlogs.umeng.com/ext_event	com/umeng/analytics/pro/aq.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/l.java
https://resolve.umeng.com/resolve	com/umeng/analytics/pro/bt.java
https://ucc.umeng.com/v2/inn/fetch	com/umeng/analytics/pro/ar.java
https://ulogs.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://developer.umeng.com/docs/119267/detail/182050	com/umeng/commonsdk/debug/UMLogCommon.java
https://developer.umeng.com/docs/119267/detail/118637	com/umeng/commonsdk/debug/UMLogCommon.java
https://ulogs.umeng.com	com/umeng/commonsdk/stateless/a.java
https://alogus.umeng.com	com/umeng/commonsdk/stateless/a.java
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.java
https://errnewlog.umeng.com	com/umeng/umcrash/UMCrashContent.java

https://errnewlogos.umeng.com	com/umeng/umcrash/UMCrashContent.java
https://developer.umeng.com/docs/193624/detail/194590	com/umeng/umcrash/UMCrash.java
https://errnewlogos.umeng.com/upload	com/umeng/umcrash/UMCrash.java
https://errnewlogos.umeng.com	com/umeng/umcrash/UMCrash.java
https://errnewlog.umeng.com/upload	com/umeng/umcrash/UMCrash.java
https://errnewlog.umeng.com	com/umeng/umcrash/UMCrash.java
https://utoken.umeng.com	com/umeng/umzid/ZIDManager.java
https://pslog.umeng.com/ablog	com/umeng/cconfig/UMRemoteConfig.java
https://ucc.umeng.com/v1/fetch	com/umeng/cconfig/UMRemoteConfig.java
https://ucc.umeng.com/v1/fetch	com/umeng/cconfig/c/b.java
https://pslog.umeng.com/ablog	com/umeng/cconfig/c/b.java
https://errlogos.umeng.com	com/uc/crashsdk/a/d.java
https://errlog.umeng.com	com/uc/crashsdk/a/d.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SegmentTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SlidingTabLayout.java
http://schemas.android.com/apk/res/android	com/alimuzaffar/lib/pin/PinEntryEditText.java

https://github.com/danikula/AndroidVideoCache/issues/88.	f4/h.java
https://github.com/danikula/AndroidVideoCache/issues/43.	f4/h.java
https://github.com/danikula	f4/h.java
https://github.com/danikula/AndroidVideoCache/issues.	f4/h.java
http://%s:%d/%s	f4/k.java
http://%s:%d/%s	f4/f.java
https://github.com/danikula/AndroidVideoCache/issues/134.	f4/f.java
https://plus.google.com/	q5/t0.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	sd/b.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	sd/d.java
https://weibo.com	y5/a.java
http://schemas.android.com/apk/res/android	z0/h.java
http://ns.adobe.com/xap/1.0/\u0000	t1/a.java
https://xtm99.top	aa/e.java

邮箱线索

邮箱地址	所在文件

u0013android@android.com0 u0013android@android.com	m5/n.java

手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java
17512775099	p7/a.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=y, ST=y, L=y, O=y, OU=y, CN=y
签名算法: rsassa_pkcs1v15
有效期自: 2024-02-01 08:03:23+00:00
有效期至: 2124-01-08 08:03:23+00:00
发行人: C=y, ST=y, L=y, O=y, OU=y, CN=y
序列号: 0x24c2cf8c
哈希算法: sha256
md5值: f6d29e95f5ed16c785b4fa8923a6d834
sha1值: adc5f2bc96110a02ed69702b6a09dd9bbf4360fa
sha256值: 2a46efa90f56da1c5a73d2fe6e6a9662639e69b0aa9f70b19c5f9a591c1575f4
sha512值: ec719a7c87ba0a3008dc0cb88a901950ac90e81c333d4d4bdf9956b52479e98be91ff0bf0d327aa03a6ce3c23b5ff4253e14705b67993318d2b36106de57b37e
公钥算法: rsa
密钥长度: 2048
指纹: adc2795979ec41e44411ed7f1c496405f05179f5246722108e18bcb32b47c8a9

硬编码敏感信息

可能的敏感信息
"digits_username" : "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"
"modify_pwd" : "修改密码"
"pwd_inconsistent" : "密码不一致"
"pwd_not_rule" : "密码不符合规则"

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.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.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.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.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.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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用

		的外部存储	
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
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.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.REQUEST_DELETE_PACKAGES	正常		允许应用程序请求删除包
android.permission.READ_MEDIA_IMAGES	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.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码

android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.ytmomoiw.yrcaodbbvineleiesulibmffipfqdbggxnteb.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

应用内通信