



MoGua

TPY-ALLIN 1.0.APK 分析报告



APP名称:	TPY-ALLIN
包名:	com.lfxrmuje
域名线索:	6条
URL线索:	42条
邮箱线索:	0条
分析日期:	2025年6月12日
分析平台:	摸瓜APK反编译平台

📁 文件信息

文件名: base.apk
文件大小: 20.65MB
MD5值: 1480dc8d19e6a370b3c0b521807393ff
SHA1值: fa359a022cbcb022361d4589d0c045ba9d0f6358
SHA256值: 852c530592dbb42749b305347e3be69e770f3216c4eb7e2892b2df3cc09e4bb7

i APP 信息

App名称: TPY-ALLIN
包名: com.lfxrmuje
主活动Activity: com.rummy.tttss.activity.MainActivity
安卓版本名称: 1.0
安卓版本: 1

🔍 域名线索

域名	服务器信息
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
service.nistock.com	没有服务器地理信息。
datacenter.eastmoney.com	IP: 125.39.135.216 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
ext.dcloud.net.cn	IP: 101.72.227.61 所属国家: China 地区: Hebei 城市: Langfang

	纬度: 39.509720 经度: 116.694717
127.0.0.1	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
api.nistock.com	没有服务器地理信息。

 URL线索

URL信息
http://a
http://a/c%20d?a=1&c=3
https://a@b
http://x
https://service.nistock.com/
https://api.nistock.com/pdf/web/viewer.html

http://127.0.0.1:50518/api

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

<https://ext.dcloud.net.cn>

<https://ext.dcloud.net.cn>

<https://ext.dcloud.net.cn>

<https://ext.dcloud.net.cn>

<https://ext.dcloud.net.cn>

<https://ext.dcloud.net.cn>

<https://ext.dcloud.net.cn>

<https://ext.dcloud.net.cn>

<https://ext.dcloud.net.cn>

<https://ext.dcloud.net.cn>

<https://ext.dcloud.net.cn>

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://datacenter.eastmoney.com/securities/api/data/get?
type=RPT_MUTUAL_QUOTA&sty=ALL&source=DataCenter&client=WAP&p=1&ps=200&sr=1&st=MUTUAL_TYPE&extraCols=status%7C07%7CBOARD_CODE,dayNetAmtIn%7C07%7CBOARD_CODE,dayAmtRemain%7C07%7CBOARD_CODE,dayAmtThreshold%7C07%7CBOARD_CODE,f104%
v=07561364306536871

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

https://ext.dcloud.net.cn

 邮箱线索

 手机线索

手机号	所在文件
17179869184	org/tukaani/xz/common/Util.java

 签名证书

APK已签名
v1 签名: True
v2 签名: False
v3 签名: False
找到 1 个唯一证书
主题: C=cn, ST=LQNDkDVw, L=LQNDkDVw, O=LQNDkDVw, OU=LQNDkDVw, CN=LQNDkDVw
签名算法: rsassa_pkcs1v15
有效期自: 2025-05-27 06:02:28+00:00
有效期至: 2125-05-03 06:02:28+00:00
发行人: C=cn, ST=LQNDkDVw, L=LQNDkDVw, O=LQNDkDVw, OU=LQNDkDVw, CN=LQNDkDVw
序列号: 0x78059012
哈希算法: sha256
md5值: fc61a7285c3f7b2dd940568f933cb56a
sha1值: 44b3edc505374a7c12a1bf888a1b68c7d13f7711
sha256值: f43a1c54d29ff276d238c543145e949cfeb78b3b2a590c0ccda8e848269755bf
sha512值: 6d8c7bef56ab0cdd3900314443ffb4c7b210715d6718fa8ba1b7a6d4e47e1385b7f07c5cb657c632b9a3e23674576e18e8a4f79269a1b989f366291d60a16e3

 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.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_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.READ_PRIVILEGED_PHONE_STATE	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.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.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
com.ifxrmuje.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信