



MoGua

税惠2025 1.0.1.APK 分析报告



APP名称:

税惠2025

包名:	com.cytsh.sh
域名线索:	8条
URL线索:	6条
邮箱线索:	1条
分析日期:	2025年6月13日
分析平台:	摸瓜APK反编译平台

文件名: 税惠2025v1.apk
文件大小: 10.15MB
MD5值: 6caab86131e77f3ad5d59726e68b0a40
SHA1值: cd07ea46fa9aa90f5f575eb63569ead2aba457e7
SHA256值: 7440084138e26c58aa623b5d882f9d93a2151086cdf5ff623d39a6bfe80938f4

i APP 信息

App名称: 税惠2025
包名: com.cytsh.sh
主活动Activity: com.sourcemuch.androidapk.LauncherActivity
安卓版本名称: 1.0.1
安卓版本: 1

🔍 域名线索

域名	服务器信息
log.tbs.qq.com	IP: 124.95.231.218 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
www.taxingapp.cc	IP: 45.117.8.139 所属国家: China 地区: Jiangsu 城市: Yangzhou 纬度: 32.397221 经度: 119.435600
	IP: 60.29.240.122 所属国家: China 地区: Tianjin

debugtbs.qq.com	城市: Tianjin 纬度: 39.142181 经度: 117.176102
cfg.imtt.qq.com	IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
tbs.imtt.qq.com	IP: 119.167.147.56 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
mdc.html5.qq.com	IP: 116.130.223.178 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
debugx5.qq.com	IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
pms.mb.qq.com	IP: 60.28.172.238 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
http://www.taxingapp.cc:1618	com/cytsh/sh/BuildConfig.java
https://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugtbs.qq.com?10000\	com/tencent/smtt/sdk/WebView.java
https://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/k.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/stat/MttLoader.java
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/o.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/o.java
https://tbs.imtt.qq.com/plugin/DebugPlugin_v2.tbs	com/tencent/smtt/utils/d.java

邮箱线索

邮箱地址	所在文件
x5tbs@tencent.com	com/tencent/smtt/sdk/X5Downloader.java

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: CN=333, OU=333, O=333, L=333, ST=333, C=333
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-27 12:20:59+00:00
有效期至: 2050-04-21 12:20:59+00:00
发行人: CN=333, OU=333, O=333, L=333, ST=333, C=333
序列号: 0x1
哈希算法: sha256
md5值: 5528ada3999e2812b3f5d06452ae9e46
sha1值: b9d70eac22edddb094c96c6dee0cecc2d7753920
sha256值: 71f763ceb4eb16f7e8c230f2c4d4deb90fd3481e29b04da9b4383682f6d320a9
sha512值: 558b95d6660bea518018faf178cafe722e6d2f94877a5cedb212df682d3e6bf0e752ee4c0230c938e5ff83d2df06d31679ba1ec6b5d28c3110cfb762bcb3d711
公钥算法: rsa
密钥长度: 2048
指纹: cfe0564a02cbf143d202d54f2a62a019848114a77f9d8c83cf636978b620d7c5

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
com.cytsh.sh.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信