MoGua

畅享世界 1.0.8.APK 分析报告

APP名称: 畅享世界

包名:	com.dunshen.enjoy.app
域名线索:	44条
URL线索:	37条
邮箱线索:	1条
分析日期:	2025年6月7日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 1.0.8.apk
文件大小: 33.6MB
MD5值: e8dee42970eb8af8c39050ac97ce206a
SHA1值: bb52cd23abd3db0f5e5297724638c9f6678e5534
SHA256值: a8b399d049dc81f93cbcba7de1442b95c8e2451adcef6e0f623110fb8555ec91

APP 信息

App名称: 畅享世界
包名: com.dunshen.enjoy.app
主活动Activity: com.dunshen.enjoy.mod.login.view.SplashActivity
安卓版本名称: 1.0.8
安卓版本: 1

域名线索

域名	服务器信息
render.alipay.com	**IP**: 221.207.101.98 **所属国家**: China **地区**: Heilongjiang **城市**: Jiamusi **纬度**: 46.833328 **经度**: 130.350006
mclient.alipay.com	**IP**: 116.142.235.203 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
api.changxiangworld.com	**IP**: 125.39.27.206 **所属国家**: China **地区**: Tianjin

	城市: Tianjin **纬度**: 39.142181 **经度**: 117.176102
mp.weixin.qq.com	IP: 140.207.176.25 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
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
google.com	IP: 108.177.98.138 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
image.cnamedomain.com	没有服务器地理信息.
oss.aliyuncs.com	IP: 118.178.29.5 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
h.trace.qq.com	IP: 113.56.189.162 **所属国家**: China **地区**: Hubei **城市**: Huangshi **纬度**: 30.204170

	经度: 115.077606
tbsrecovery.imtt.qq.com	IP: 60.28.172.122 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
oss-cn-.aliyuncs.comor	没有服务器地理信息.
long.open.weixin.qq.com	IP: 112.65.193.150 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
wappaygw.alipay.com	IP: 111.202.5.210 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
mcgw.alipay.com	IP: 111.202.5.210 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.google.com	IP: 31.13.94.37 **所属国家**: Argentina **地区**: Ciudad Autonoma de Buenos Aires **城市**: Buenos Aires **纬度**: -34.603600 **经度**: -58.381554

www.google	没有服务器地理信息.
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
mobilegw.alipaydev.com	**IP**: 110.75.132.131 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
open.weixin.qq.com	**IP**: 140.207.176.25 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
mobilegw.alipay.com	**IP**: 203.209.243.27 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
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
	IP: 119.42.231.21 **所属国家**: China **地区**: Zhejiang

loggw-exsdk.alipay.com	**城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
www.googleapis.com	IP: 173.194.203.95 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
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
oss-cn-chengdu.aliyuncs.com	IP: 47.108.5.150 **所属国家**: China **地区**: Sichuan **城市**: Chengdu **纬度**: 30.666670 **经度**: 104.066269
oss-cn-hangzhou.aliyuncs.com	IP: 118.31.219.249 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
astat.bugly.qcloud.com	IP: 119.28.121.133 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281

203.107.1.1	IP: 203.107.1.1 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
debugtbs.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
astat.bugly.cros.wr.pvp.net	IP: 170.106.118.26 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
mobilegw.dl.alipaydev.com	IP: 110.75.132.25 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
mobilegwpre.alipay.com	IP: 110.75.138.35 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
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
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
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
h5.m.taobao.com	IP: 101.72.202.199 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
android.bugly.qq.com	IP: 124.95.225.146 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
h5.changxiangworld.com	IP: 125.39.27.209 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
	IP: 202.160.129.164 **所属国家**: Singapore

zxing.appspot.com	**地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
mqqad.html5.qq.com	IP: 0.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
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
tbs.imtt.qq.com	IP: 211.93.212.236 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.example.com	IP: 23.197.49.24 **所属国家**: Japan **地区**: Osaka **城市**: Ibaraki **纬度**: 34.816425 **经度**: 135.568909
cx2025.oss-cn-chengdu.aliyuncs.com	IP: 116.169.131.134 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

URL线索

URL信息	Url所在文件
http://books.google.	a1/a.java
http://oss.aliyuncs.com	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://127.0.0.1	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://oss-cn-****.aliyuncs.com',or	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://image.cnamedomain.com'!	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://oss-cn-hangzhou.aliyuncs.com	com/alibaba/sdk/android/oss/common/OSSConstants.java
https://203.107.1.1/181345/d?host=	com/alibaba/sdk/android/oss/common/utils/HttpdnsMini.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://mobilegwpre.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/m/m/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/m/m/a.java
https://mobilegw.dl.alipaydev.com/mgw.htm	com/alipay/sdk/m/m/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/m/m/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	com/alipay/sdk/m/m/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/m/m/a.java

https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/m/m/a.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/m/n/a.java
https://render.alipay.com/p/s/i?scheme=%s	com/alipay/sdk/app/OpenAuthTask.java
https://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
https://h5.changxiangworld.com/user/user.html	com/dunshen/enjoy/mod/login/BuildConfig.java
https://h5.changxiangworld.com/user/yinsi.html	com/dunshen/enjoy/mod/login/BuildConfig.java
https://h5.changxiangworld.com/user/xiaofei.html	com/dunshen/enjoy/mod/home/BuildConfig.java
https://api.changxiangworld.com	com/dunshen/moon/lib/net/BuildConfig.java
https://cx2025.oss-cn-chengdu.aliyuncs.com	com/dunshen/moon/lib/net/BuildConfig.java
https://oss-cn-chengdu.aliyuncs.com	com/dunshen/moon/lib/net/BuildConfig.java

http://xml.apache.org/xslt	com/dunshen/moon/lib/log/klog/XmlLog.java
https://github.com/danikula/AndroidVideoCache/issues/88.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues/43.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues.	com/danikula/videocache/HttpUrlSource.java
http://%s:%d/%s	com/danikula/videocache/HttpProxyCacheServer.java
http://google.com/books	com/dushen/moon/lib/scan/client/LocaleManager.java
http://books.google.	com/dushen/moon/lib/scan/client/LocaleManager.java
http://zxing.appspot.com/scan	com/dushen/moon/lib/scan/client/CaptureActivity.java
http://www.google	com/dushen/moon/lib/scan/client/CaptureActivity.java
http://www.google.com/books?id=	com/dushen/moon/lib/scan/client/book/SearchBookContentsActivity.java
http://www.google.com/books?vid=isbn	com/dushen/moon/lib/scan/client/book/SearchBookContentsActivity.java
http://maps.google.	com/dushen/moon/lib/scan/client/result/ResultHandler.java
http://books.google.	com/dushen/moon/lib/scan/client/result/ResultHandler.java
http://www.google.	com/dushen/moon/lib/scan/client/result/ResultHandler.java
https://h.trace.qq.com/kv	com/tencent/bugly/proguard/ad.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/proguard/ac.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/proguard/ac.java

https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/f.java
https://open.weixin.qq.com/connect/sdk/qrconnect? appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/d.java
https://mp.weixin.qq.com/publicpoc/opensdkconf? action=GetShareConf&appid=%s&sdkVersion=%s&buffer=%s	com/tencent/mm/opensdk/openapi/WXAPiSecurityHelper.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/l.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://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047	com/tencent/smtt/sdk/ui/dialog/d.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041	com/tencent/smtt/sdk/ui/dialog/d.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://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/o.java
https://tbsrecovery.imtt.qq.com/getconfig	com/tencent/smtt/utils/o.java
https://tbs.imtt.qq.com/plugin/DebugPlugin_v2.tbs	com/tencent/smtt/utils/d.java
http://www.example.com	com/zjh/download/core/DownloadConfig.java
http://%s:%d/%s	z/f.java
https://github.com/danikula/AndroidVideoCache/issues/134.	z/f.java
https://www.google.	e1/b.java
https://www.googleapis.com/books/v1/volumes?q=isbn:	e1/a.java
http://www.google.	e1/a.java
https://ip.	f/a.java
http://oss-cn-****.aliyuncs.com',or	f/a.java
http://image.cnamedomain.com'!	f/a.java

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	o2/f.java

手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.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=(086), ST=(sc), L=(cd), O=(lanao), OU=(lanao), CN=(lanao)
签名算法: rsassa_pkcs1v15
有效期自: 2025-03-11 01:24:18+00:00
有效期至: 2026-03-11 01:24:18+00:00
发行人: C=(086), ST=(sc), L=(cd), O=(lanao), OU=(lanao), CN=(lanao)
序列号: 0xe74f4dcfe39e61fb
哈希算法: sha384
md5值: e12dc352dae4876adbd8752704423818
sha1值: e91be1b3aff30c6bbe5556b2e46989fa81c97bc8
sha256值: 87f832d75f554f7645f8f71b1b8c31ba29ed2b1b90f3c87e659aa1346714962b
sha512值: cfd7a22006894f01bdfae1f13fe2a70fe7e00f6fe0dc0234f908b3235085973d93a6487aa47bbfde4588ec81c7dff34ee1a559544b165a09ac238e56b1dced50
公钥算法: rsa
密钥长度: 1024
指纹: 32d1fdb77b8ceadf26bb4489cbd17d82e1dff322529201c8512b058ec1956fbc

硬编码敏感信息

可能的敏感信息
"loading_go_auth" : "Go to Alipay for authorization"
"mod_login_auth_read_agreement" : "进入应用之前,您需要先阅读和同意《用户协议》和《隐私政策》,否则将退出应用。"
"mod_me_account_list_token_expire" : "该账号令牌已经过期,是否跳转重新登录?"
"loading_go_auth" : "前往支付寶授權"
"loading_go_auth" : "去支付寶授權"
"loading_go_auth" : "去支付宝授权"

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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
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.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_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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
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.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.READ_MEDIA_IMAGES	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
com.android.browser.permission.READ_HISTORY_BOOKMARKS	未知	Unknown permission	Unknown permission from android reference

应用内通信