



MoGua

盈达智汇 1.0.APK 分析报告



APP名称:

盈达智汇

包名:	com.ydzhlyls.xzapp
域名线索:	16条
URL线索:	16条
邮箱线索:	2条
分析日期:	2025年10月3日
分析平台:	摸瓜APK反编译平台

文件名: 盈达智汇.apk
文件大小: 13.6MB
MD5值: 463e19d7dd2bfae14fc2d3279b3a033c
SHA1值: 302aa7bb32ab61070ac35052c9d25d8038b51429
SHA256值: 0fa0058fadaef67b9d8855302a3b555df627e8420dc73206a5972d45fde1a737

i APP 信息

App名称: 盈达智汇
包名: com.ydzhlyls.xzapp
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0
安卓版本: 1

🔍 域名线索

域名	服务器信息
er.dcloud.net.cn	IP: 43.142.57.168 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
gac1.dcloud.net.cn	IP: 114.55.242.34 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
m3w.cn	IP: 123.6.37.172 所属国家: China 地区: Henan

	城市: Zhengzhou 纬度: 34.757778 经度: 113.648613
app.ydzh999.com	IP: 8.134.123.235 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
er.dcloud.io	没有服务器地理信息.
sdk.api.oaid.wocloud.cn	没有服务器地理信息.
sdk.api.oaid.wocloud.cn.local	没有服务器地理信息.
c.tenor.com	IP: 185.60.219.36 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
googlehosted.l.googleusercontent.com	IP: 142.251.215.225 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
ns.adobe.com	没有服务器地理信息.
ask.dcloud.net.cn	IP: 123.125.244.81 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501

	经度: 116.397102
schemas.android.com	没有服务器地理信息.
media.tenor.com	IP: 162.125.2.3 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
cdn.dcloud.net.cn	IP: 121.4.61.130 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
android.googlesource.com	IP: 192.178.163.82 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
edgedl.me.gvt1.com	IP: 34.104.35.123 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514

URL线索

URL信息	Url所在文件

https://ask.dcloud.net.cn/article/35627	b/a.java
https://ask.dcloud.net.cn/article/35877	b/a.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
https://er.dcloud.io/rv	d/c.java
https://er.dcloud.net.cn/rv	d/c.java
https://ask.dcloud.net.cn/article/283	j/b.java
https://ask.dcloud.net.cn/article/36199	摸瓜V1引擎
https://m3w.cn/s/	摸瓜V3引擎
http://schemas.android.com/apk/res/android00androidx.appcompat.widget.FitWindowsLinearLayout	摸瓜V3引擎

http://schemas.android.com/apk/res/android	摸瓜V3引擎
https://android.googlesource.com/toolchain/clang	摸瓜V3引擎
https://ask.dcloud.net.cn/article/35627	摸瓜V3引擎
http://schemas.android.com/apk/res-auto00androidx.appcompat.widget.ActionBarOverlayLayout	摸瓜V3引擎
https://er.dcloud.net.cn/rv	摸瓜V3引擎
https://er.dcloud.net.cn/sc	摸瓜V3引擎
googlehosted.l.googleusercontent.com	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
http://schemas.android.com/apk/res-auto((androidx.appcompat.widget.ActionMenuView	摸瓜V3引擎
tenor.googleapis.com	摸瓜V3引擎
cdn.dcloud.net.cn	摸瓜V3引擎
http://schemas.android.com/apk/res/android00androidx.appcompat.widget.FitWindowsLinearLayout((androi	摸瓜V3引擎
https://ask.dcloud.net.cn/article/282	摸瓜V3引擎
sdk.api.oaid.wocloud.cn	摸瓜V3引擎
c.tenor.com	摸瓜V3引擎
https://ask.dcloud.net.cn/article/283	摸瓜V3引擎
media.tenor.com	摸瓜V3引擎

gac1.dcloud.net.cn	摸瓜V3引擎
app.ydzh999.com	摸瓜V3引擎
https://ask.dcloud.net.cn/article/35058	摸瓜V3引擎
https://er.dcloud.io/sc	摸瓜V3引擎
sdk.api.oaid.wocloud.cn.local	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm	摸瓜V3引擎
http://schemas.android.com/apk/res-autoAAio.dcloud.feature.gallery.imageedit.view.WindowInsertLinear	摸瓜V3引擎
https://er.dcloud.io/rv	摸瓜V3引擎
content-autofill.googleapis.com	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm-project	摸瓜V3引擎
https://ask.dcloud.net.cn/article/35877	摸瓜V3引擎
edgedl.me.gvt1.com	摸瓜V3引擎

 邮箱线索

邮箱地址	所在文件
np@1.f1e	摸瓜V2引擎
np@1.f1e	摸瓜V2引擎

☰ 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: True
找到 1 个唯一证书
主题: C=CN, O=ydzhlyls, OU=IT, CN=ydzhlyls
签名算法: rsassa_pkcs1v15
有效期自: 2025-01-03 15:35:40+00:00
有效期至: 2124-12-10 15:35:40+00:00
发行人: C=CN, O=ydzhlyls, OU=IT, CN=ydzhlyls
序列号: 0x7498444b
哈希算法: sha256
md5值: d3bfebe4c2a924a8704a122e27315b64
sha1值: d329edbba1772d3882b7a64be1018bae76a45ddc
sha256值: b3fbdff792b501641b54a8f86c5974eff6874918444d0a128d4ed3ead6dbbb1
sha512值: 0d8ad68bcc6fa0bc1506a97b94cfa9087f5626f13aca5121cc83bccb745c765f080ced26d975ccf0e2d3aefbb5281c79161d1741323424f19f081d52acd6bf50
公钥算法: rsa
密钥长度: 2048
指纹: ba5c50d914370767c9ecff236599090932949d5417350b3d0c93bad68873d8d1

🔑 硬编码敏感信息

可能的敏感信息
"dcloud_common_user_refuse_api" : "the user denies access to the API"
"dcloud_feature_confusion_exception_no_private_key_input" : "no private key input"
"dcloud_io_without_authorization" : "not authorized"
"dcloud_oauth_authentication_failed" : "failed to obtain authorization to log in to the authentication service"
"dcloud_oauth_empower_failed" : "the Authentication Service operation to obtain authorized logon failed"
"dcloud_oauth_logout_tips" : "not logged in or logged out"
"dcloud_oauth_oauth_not_empower" : "oAuth authorization has not been obtained"
"dcloud_oauth_token_failed" : "failed to get token"
"dcloud_permissions_reauthorization" : "reauthorize"
"dcloud_tips_certificate" : "certificate"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"dcloud_feature_confusion_exception_no_private_key_input" : "私钥数据为空"
"dcloud_io_without_authorization" : "没有获得授权"
"dcloud_oauth_authentication_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_empower_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_logout_tips" : "未登录或登录已注销"
"dcloud_oauth_oauth_not_empower" : "尚未获取oauth授权"

"dcloud_oauth_token_failed" : "获取token失败"
"dcloud_permissions_reauthorization" : "重新授权"
"dcloud_tips_certificate" : "证书"

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_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_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
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.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
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.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
com.asus.msa.SupplementaryDID.ACCESS	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
android.permission.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序

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.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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
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.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。

应用内通信

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。