



MoGua

意昂体育 1.0.7.APK 分析报告



APP名称:	意昂体育
包名:	com.eon1.app
域名线索:	36条
URL线索:	35条
邮箱线索:	1条
分析日期:	2025年6月8日
分析平台:	摸瓜APK反编译平台

📁 文件信息

文件名: eon1_v107.apk
文件大小: 29.94MB
MD5值: 8587763051f5650bdd4c02086457e512
SHA1值: a477a40b87b3577966e7040bbb13208f0a621c21
SHA256值: a2edcc6915e388b32d985cc1a3688435d834fa0238d0d8ca62371fec491f48e6

i APP 信息

App名称: 意昂体育
包名: com.eon1.app
主活动Activity: com.xtree.main.ui.SplashActivity
安卓版本名称: 1.0.7
安卓版本: 107

🔍 域名线索

域名	服务器信息
h22.l3q2ur.xyz	IP: 20.243.33.151 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
h61.xuanwujx.com	没有服务器地理信息.
h32.f9o4qf.xyz	IP: 20.247.125.45 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
h61.aaagx.com	没有服务器地理信息.
	IP: 20.50.73.10 所属国家: Ireland

mobile.events.data.microsoft.com	地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
h12.i2n5wp.xyz	IP: 185.135.74.18 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
www.eon2.org	IP: 198.16.61.27 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052570 经度: -118.243904
h52.s4z9il.xyz	IP: 185.135.74.96 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
h61.saaen.com	没有服务器地理信息.
www.baidu.com	IP: 110.242.70.57 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
h22.k2a5dg.xyz	IP: 143.92.48.63 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
api.mixpanel.com	IP: 130.211.34.183 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
h32.r3v9ve.xyz	IP: 20.247.125.45 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
schemas.android.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000

o4507447554539520.ingest.us.sentry.io	IP: 34.120.195.249 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
h61.baafj.com	没有服务器地理信息.
wap.cq.10086.cn	IP: 218.201.25.130 所属国家: China 地区: Chongqing 城市: Chongqing 纬度: 29.562780 经度: 106.553101
h51.c4z6me.viphttps	没有服务器地理信息.
in.appcenter.ms	IP: 52.247.72.241 所属国家: United States of America 地区: Virginia 城市: Boydton 纬度: 36.667641 经度: -78.387497
h61.bfangwang.com	IP: 119.45.242.37 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
h61.caaau.com	没有服务器地理信息.
h32.p7i9lh.xyz	IP: 20.247.125.45 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
scdnapp.b4k4p3.com	IP: 185.135.74.77 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
ns.adobe.com	没有服务器地理信息.
10.0.2.2	IP: 10.0.2.2 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
119.28.21.69	IP: 119.28.21.69 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521

	经度: 114.157692
h61.yhlims.com	IP: 122.152.230.133 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
h12.y7e8nr.xyz	IP: 185.135.74.34 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
h22.k2h9ae.xyz	IP: 119.9.94.119 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
github.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
h42.q7s1iu.xyz	IP: 45.60.66.210 所属国家: United States of America 地区: California 城市: Redwood City 纬度: 37.532440 经度: -122.248833
psowoexvd.n2vu8zpu2f6.com	IP: 45.61.226.143 所属国家: United States of America 地区: Colorado 城市: Denver 纬度: 39.730984 经度: -104.981453
www.hiwalletapp.com	IP: 61.4.114.189 所属国家: Malaysia 地区: Wilayah Persekutuan Kuala Lumpur 城市: Kuala Lumpur 纬度: 3.141301 经度: 101.686623
h12.h8h8pm.xyz	IP: 185.135.74.34 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
h51.u2z9wj.vip	IP: 106.74.25.198 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223

app1.b9a1xp.viphttps	没有服务器地理信息.
----------------------	------------

🌐 URL线索

URL信息
http://schemas.android.com/apk/res/android
https://psowoexvd.n2vu8zpu2f6.com/chatWindow.aspx?planId=1e906220-bcfb-4f17-a5eb-bf7e9ab74be9&siteId=65000194
https://www.hiwalletapp.com/download
https://www.hiwalletapp.com/download
https://github.com/mixpanel/mixpanel-android/issues/567)
https://api.mixpanel.com
http://www.baidu.com
https://api.mixpanel.com
https://www.eon2.org
http://schemas.android.com/apk/res/android
http://ns.adobe.com/xap/1.0/\u0000
https://github.com/danikula/AndroidVideoCache/issues/88.
https://github.com/danikula/AndroidVideoCache/issues/43.
https://github.com/danikula
https://github.com/danikula/AndroidVideoCache/issues.
http://%s:%d/%s
https://github.com/danikula/AndroidVideoCache/issues/134.
http://undefined/
https://in.appcenter.ms
http://%s:%d/%s
https://mobile.events.data.microsoft.com/OneCollector/1.0
https://wap.cq.10086.cn/mapp/activities/fanzha2021/html-phone-yd/index.html
https://h12.i2n5wp.xyz

https://h12.y7e8nr.xyz
https://h12.h8h8pm.xyz
https://h22.k2a5dg.xyz
https://h22.k2h9ae.xyz
https://h22.i3q2ur.xyz
https://h32.f9o4qf.xyz
https://h32.r3v9ve.xyz
https://h32.p7l9lh.xyz
https://h42.q7s1lu.xyz
https://h52.s4z9il.xyz
https://h61.saaen.com:16801
https://h61.caaau.com:16801
https://h61.baafj.com:16801
https://h61.aaagx.com:16801
https://h61.xuanwujx.com:16801
https://h61.yhlims.com:16801
https://h61.bfangwang.com:16801
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Error-Handling

https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0
https://github.com/ReactiveX/RxJava/wiki/Error-Handling
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0
http://10.0.2.2:8969/stream
http://119.28.21.69:36803
https://app1.b9a1xp.vip;https://app1.w1t2mg.vip;https://app1.k6o5br.vip;https://app1.k3g6hb.vip;https://app1.i5h2er.vip;https://app2.m9j2nc.vip;https://app2.v1p9eq.vip;https://app2.k3q4zz.vip;https://app2.o1a7ds.vip;https://app2.z2e4wz.vip;https://app3.ahyyclq.xyz;https://app3.xb
https://h51.u2z9wj.vip
https://h51.c4z6me.vip;https://h51.u2z9wj.vip;https://h51.a9i8gh.vip;https://h52.v8v9xb.vip;https://h52.z5q7qf.vip;https://h52.j4u9rb.vip;https://h53.n7j7ov.vip;https://h53.n9a8th.vip;https://h53.z4y3lx.vip;https://h54.u2e3uc.vip;https://h54.p7x3cn.vip;https://h61.hmsdjy.com:36801;htt
https://scdnapp.b4k4p3.com/e1/app_config_e1.json
https://383170354668314c6a6b6ca3527d1810@o4507447554539520.ingest.us.sentry.io/4507604245217280

✉ 邮箱线索

邮箱地址	所在文件
314c6a6b6ca3527d1810@o4507447554539520.ingest	摸瓜V1引擎

☎ 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=Ap, OU=RD, O=X C Sprot, L=HengBin, ST=TKO, C=JP
签名算法: rsassa_pkcs1v15
有效期自: 2023-11-28 13:05:57+00:00
有效期至: 2043-11-23 13:05:57+00:00
发行人: CN=Ap, OU=RD, O=X C Sprot, L=HengBin, ST=TKO, C=JP
序列号: 0x1
哈希算法: sha256
md5值: 77b5c190dfd508959bebf37512adfd65
sha1值: db74fa68d1cd6bf6427355ba43a2f9b7f8ab71ec
sha256值: 083f354fa2d1206712b76d30caf3c01eee9775ff061e6ea68250a854efbb6113
sha512值: 2c60f6177249a1b11a5af0d684ca7868a5deaeef71b552a5598cbe406c67afa58da871734c5b9063da5980456c58caca752c8671080cce9ecaf161e9e3620ead
公钥算法: rsa
密钥长度: 2048
指纹: c096de5025f28b1b66bea6bfe0f0b4d87ff9645d11fb7cbc4f6ea4587c6c9438

🔑 硬编码敏感信息

可能的敏感信息
"domain_api" : "http://119.28.21.69:36803"
"me_pwd_forget" : "忘记密码? "
"me_pwd_forget_title" : "忘记密码"
"me_pwd_remember" : "记住密码"
"mixpanel_token" : "cce6df315eee2c445da416c6b717f114"
"ms_secret_key" : "2cfde5ab-d271-462f-9b67-a6bdabf4c5ee"

🔑 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.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.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_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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	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
android.permission.INSTALL_SHORTCUT	正常		允许应用程序在启动器中安装快捷方式
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference

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.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.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.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.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	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

应用内通信