



MoGua

审计助手 1.0.1.APK 分析报告



APP名称:

审计助手

包名:	cn.com.bonc.client
域名线索:	12条
URL线索:	15条
邮箱线索:	3条
分析日期:	2025年6月26日
分析平台:	摸瓜APK反编译平台

文件名: sjzs.apk
文件大小: 24.23MB
MD5值: 409da12d53f9f3512a3ca6bac95fa02d
SHA1值: ae0872ba2ba5845319847fda5022ae61b1703c01
SHA256值: a369e9b3d9acc0a3e8cc7e2b90037f5a1aad3f045b0f0036a8942e689f1f7e5f

i APP 信息

App名称: 审计助手
包名: cn.com.bonc.client
主活动Activity: cn.com.bonc.client.view.activity.WelcomeActivity
安卓版本名称: 1.0.1
安卓版本: 2024121201

🔍 域名线索

域名	服务器信息
abroad.apilocate.amap.com	IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
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
www.smpte-ra.org	IP: 52.20.185.129 所属国家: United States of America 地区: Virginia

	城市: Ashburn 纬度: 39.039474 经度: -77.491806
adiu.amap.com	IP: 110.253.189.146 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
lbs.amap.com	IP: 110.253.188.148 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
apilocate.amap.com	IP: 59.82.31.183 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
136.96.228.6	IP: 136.96.228.6 所属国家: United States of America 地区: Michigan 城市: Dearborn 纬度: 42.311520 经度: -83.191322
xml.org	IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246

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
restapi.amap.com	IP: 106.11.43.113 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
219.148.201.62	IP: 219.148.201.62 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877

 URL线索

URL信息	Url所在文件
http://xml.apache.org/xslt	cn/hutool/core/util/XmlUtil.java
http://apache.org/xml/features/disallow-doctype-decl	cn/hutool/core/util/XmlUtil.java

http://xml.org/sax/features/external-general-entities	cn/hutool/core/util/XmlUtil.java
http://xml.org/sax/features/external-parameter-entities	cn/hutool/core/util/XmlUtil.java
http://apache.org/xml/features/nonvalidating/load-external-dtd	cn/hutool/core/util/XmlUtil.java
https://136.96.228.6:8083/api/	cn/com/bonc/client/comm/URLs.java
https://136.96.228.6:8083	cn/com/bonc/client/comm/URLs.java
https://136.96.228.6:8083/dist/	cn/com/bonc/client/comm/URLs.java
https://219.148.201.62	cn/com/bonc/client/utils/AndroidInterface.java
https://219.148.201.62	cn/com/bonc/client/view/activity/LoginActivity.java
https://136.96.228.6:8083/dist/	cn/com/bonc/client/view/activity/LoginActivity.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/	com/amap/api/location/AMapLocation.java
http://www.smpte-ra.org/schemas/2052-1/2010/smpte-tt	com/googlecode/mp4parser/authoring/tracks/ttml/TtmlHelpers.java
http://xml.apache.org/xslt	com/googlecode/mp4parser/authoring/tracks/ttml/TtmlHelpers.java
https://adiu.amap.com/ws/device/adius	com/loc/bi.java
http://apilocate.amap.com/mobile/binary	com/loc/dg.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/dg.java
http://restapi.amap.com	com/loc/t.java
http://restapi.amap.com/v3/place/text?	com/loc/a.java
http://restapi.amap.com/v3/config/district?	com/loc/a.java

http://restapi.amap.com/v3/place/around?	com/loc/a.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/dk.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/cz.java
http://restapi.amap.com/v3/geocode/regeo	com/loc/db.java
https://restapi.amap.com/v3/iasdkauth	com/loc/m.java
http://restapi.amap.com/v3/iasdkauth	com/loc/m.java

 邮箱线索

邮箱地址	所在文件
auth-agent@openssh.com	cn/hutool/extra/ssh/ChannelType.java
ftp@example.com	lib/arm64-v8a/libsangforsdk.so
ftp@example.com	lib/armeabi-v7a/libsangforsdk.so

 手机线索

 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=710000, ST=shannxi, L=xian, O=bonc, OU=bonc, CN=bonc
签名算法: rsassa_pkcs1v15
有效期自: 2020-03-16 06:32:56+00:00
有效期至: 2119-02-21 06:32:56+00:00
发行人: C=710000, ST=shannxi, L=xian, O=bonc, OU=bonc, CN=bonc
序列号: 0x36f9aaf6
哈希算法: sha256
md5值: 82f84538609bc6d7b1747cfa5ae9ff5b
sha1值: 385bfef841358b07a74826cb835f1a9b60411643
sha256值: e1e84e7eb58805d87e2e9107ca8b5d6d31f4b1cbfd5c76e838cacab7f88140d3
sha512值: d1571cc755aed8092f37ee74b4ac18e89a57041b130d8cf325fed6163e84fca88e16a2785be18d676c0458b324862c595805a6e8e2854f9120dda58dd31458b7
公钥算法: rsa
密钥长度: 2048
指纹: 36e683bb4e8749d9e6479c892ac6cb8cfa1bf81ad770096dc72c27abde626a20

 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.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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字

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.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.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令, 恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.RESTART_PACKAGES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
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.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

应用内通信

活动(ACTIVITY)	通信(INTENT)
cn.com.bonc.client.view.activity.IdentificationActivity	Schemes: bonc://, Hosts: xj.gcsj,