



MoGua

智能身份验证 4.0.0.APK 分析报告



APP名称:

智能身份验证

包名: com.websinda.sccd.user

域名线索: 28条

URL线索: 26条

邮箱线索: 0条

分析日期: 2025年10月7日

分析平台: [摸瓜APK反编译平台](#)

文件名: member-40-v4.0.0.apk
文件大小: 18.38MB
MD5值: 7252e93eff1b414e3eaa23c8d789ba03
SHA1值: c7648e3ceef4d522849cf9e6f0cdea8c230e2519
SHA256值: 2f2009a5e7eedd5f17a4ba0666b154290bd9234431c065602625b3a03809e854

i APP 信息

App名称: 智能身份验证
包名: com.websinda.sccd.user
主活动Activity: com.websinda.sccd.user.ui.login.Loading_Activity
安卓版本名称: 4.0.0
安卓版本: 40

🔍 域名线索

域名	服务器信息
gcc.gnu.org	IP: 8.43.85.97 所属国家: United States of America 地区: North Carolina 城市: Raleigh 纬度: 35.773994 经度: -78.632759
tsis.jpush.cn	IP: 123.60.218.46 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.
	IP: 108.177.98.82

android.googleusercontent.com	所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
encrypted-tbn0.gstatic.com	IP: 142.250.73.142 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
gd-stats.jp.push.cn	IP: 120.233.34.157 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545673 经度: 114.068108
sdk-verify.n.shifen.com	IP: 110.242.69.180 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
face.baidu.com	IP: 112.34.111.253 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
aip-developer.n.shifen.com	IP: 111.206.210.12 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501

	经度: 116.397102
ai.baidu.com	IP: 110.242.69.34 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
10.138.32.176	IP: 10.138.32.176 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
stats.jpush.cn	IP: 119.147.121.245 所属国家: China 地区: Guangdong 城市: Dongguan 纬度: 23.048780 经度: 113.745003
app.caintel.cn	IP: 140.143.186.190 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
googlehosted.l.googleusercontent.com	IP: 142.250.73.129 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
	IP: 203.208.39.226 所属国家: China 地区: Beijing

www.gstatic.com	城市: Beijing 纬度: 39.907501 经度: 116.397102
web.ccyunmai.com	IP: 60.204.154.112 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
verify.baidubce.com	IP: 153.3.238.231 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
aip.baidubce.com	IP: 111.206.210.12 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
connectivitycheck.gstatic.com	IP: 203.208.50.98 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
182.92.20.189	IP: 182.92.20.189 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

i2.ytimg.com	IP: 216.239.38.60 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
brain.baidu.com	IP: 110.242.69.34 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
s.jpush.cn	IP: 1.94.190.95 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
sdkss.shitu.baidu.com	IP: 180.101.49.104 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
www.baidu.com	IP: 110.242.69.21 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
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
lh5.googleusercontent.com	IP: 142.250.73.129 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
ali-stats.jppush.cn	IP: 119.147.121.151 所属国家: China 地区: Guangdong 城市: Dongguan 纬度: 23.048780 经度: 113.745003

URL线索

URL信息	Url所在文件
http://182.92.20.189:9099/	cn/jiguang/a/a/c/i.java
https://tsis.jppush.cn	cn/jiguang/d/a.java
http://10.138.32.176:8518/api/v3/person/verify_sec?appid=7758258	com/baidu/idl/face/platform/ui/utils/SecRequest.java
http://face.baidu.com/openapi/v2/stat/sdkdata	com/baidu/idl/face/platform/network/LogRequest.java
http://face.baidu.com/gate/api/userverifydemo	com/baidu/idl/face/platform/network/NoMotionRequest.java
https://brain.baidu.com/record/api	com/baidu/idl/face/platform/stat/Ast.java
https://ai.baidu.com/activation/key/activate	com/baidu/idl/main/facesdk/FaceAuth.java

http://brain.baidu.com/record/api	com/baidu/idl/main/facesdk/statistic/PostDeviceInfo.java
http://sdkss.shitu.baidu.com/cgi-bin/queryLicense.py	com/baidu/idl/license/License.java
http://sdkss.shitu.baidu.com/cgi-bin/sdkstat.py	com/baidu/idl/statistics/Statistics.java
http://schemas.android.com/apk/res/android	com/baidu/liantian/g/d.java
https://ai.baidu.com/activation/key/activate	com/baidu/vis/unified/license/BDLicenseActivator.java
https://verify.baidubce.com/verify/1.0/token/bin?sdkVersion=1_4_3	com/baidu/ocr/sdk/a.java
https://verify.baidubce.com/verify/1.0/sdk/report	com/baidu/ocr/sdk/c/b.java
http://www.baidu.com	com/websinda/sccd/user/client/NetworkUtil.java
http://app.caintel.cn/	com/websinda/sccd/user/client/RetrofitClient.java
http://xml.apache.org/xslt	com/websinda/sccd/user/utis/l.java
http://app.caintel.cn//agreement/social_agreement.html	com/websinda/sccd/user/utis/r.java
http://app.caintel.cn//agreement/ysxy.html	com/websinda/sccd/user/utis/r.java
http://app.caintel.cn//agreement/social_agreement.html	com/websinda/sccd/user/ui/usermanage/UserManageActivity.java
http://app.caintel.cn//agreement/ysxy.html	com/websinda/sccd/user/ui/usermanage/UserManageActivity.java
http://app.caintel.cn//agreement/ysxy.html	com/websinda/sccd/user/ui/login/Login_Activity.java
http://app.caintel.cn//agreement/social_agreement.html	com/websinda/sccd/user/ui/login/Login_Activity.java
http://app.caintel.cn//agreement/user_agreement.html	com/websinda/sccd/user/ui/login/fragment/RegisterFragment.java
http://app.caintel.cn//agreement/social_agreement.html	com/websinda/sccd/user/ui/login/fragment/RegisterFragment.java

https://aip.baidubce.com/oauth/2.0/token?	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//bvr/advertisement/c_advertise_login_after?pageIndex=1	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//sinda/member/face/artificial/verify	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn/	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//sinda/member/user/binding/code	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//bvr/system/collection/call_user	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//bvr/system/collection/update_phone	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//sinda/member/user/edit/info	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//sinda/member/user/binding/phone	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//sinda/member/user/edit/pwd	com/websinda/sccd/user/api/APIService.java
https://aip.baidubce.com/rest/2.0/face/v3/match	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//sinda/member/face/verify	com/websinda/sccd/user/api/APIService.java
https://aip.baidubce.com/rest/2.0/face/v3/search	com/websinda/sccd/user/api/APIService.java
https://aip.baidubce.com/rest/2.0/face/v3/person/verify	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//sinda/member/login	com/websinda/sccd/user/api/APIService.java
https://aip.baidubce.com/rest/2.0/face/v3/faceverify	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//sinda/member/operation/code	com/websinda/sccd/user/api/APIService.java

http://app.caintel.cn//sinda/member/user/proposal	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//sinda/member/register/id_card	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//sinda/member/register/code	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//sinda/member/face/register	com/websinda/sccd/user/api/APIService.java
https://aip.baidubce.com/rest/2.0/face/v3/faceset/user/add	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//sinda/member/pwd/result	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//answer/index.html	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//sinda/member/version/info	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//bvr/app/member/verify_face	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//bvr/app/member/face	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//sinda/member/face/status	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//sinda/member/user/info	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//sinda/member/voice/status	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn//sinda/member/voice/register	com/websinda/sccd/user/api/APIService.java
http://app.caintel.cn/	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm	摸瓜V3引擎
tsis.jp.push.cn	摸瓜V3引擎
instantmessaging-pa.googleapis.com	摸瓜V3引擎

http://face.baidu.com/gate/api/userverifydemo	摸瓜V3引擎
encrypted-tbn0.gstatic.com	摸瓜V3引擎
https://aip.baidubce.com/rest/2.0/face/v3/person/verify	摸瓜V3引擎
gd-stats.jp.push.cn	摸瓜V3引擎
sdk-verify.n.shifen.com	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
http://app.caintel.cn//agreement/ysxy.html	摸瓜V3引擎
http://xml.apache.org/xslt	摸瓜V3引擎
growth-pa.googleapis.com	摸瓜V3引擎
http://brain.baidu.com/record/api	摸瓜V3引擎
aip-developer.n.shifen.com	摸瓜V3引擎
http://10.138.32.176:8518/api/v3/person/verify_sec?appid=7758258	摸瓜V3引擎
http://sdkss.shitu.baidu.com/cgi-bin/queryLicense.py	摸瓜V3引擎
https://ai.baidu.com/activation/key/activate	摸瓜V3引擎
http://app.caintel.cn//agreement/social_agreement.html	摸瓜V3引擎
http://face.baidu.com/openapi/v2/stat/sdkdata	摸瓜V3引擎
googlehosted.l.googleusercontent.com	摸瓜V3引擎

app.caintel.cn	摸瓜V3引擎
stats.jppush.cn	摸瓜V3引擎
https://android.googlesource.com/toolchain/clang	摸瓜V3引擎
www.gstatic.com	摸瓜V3引擎
https://verify.baidubce.com/verify/1.0/token/bin?sdkVersion=1_4_3	摸瓜V3引擎
android.googleapis.com	摸瓜V3引擎
https://tsis.jppush.cn	摸瓜V3引擎
verify.baidubce.com	摸瓜V3引擎
http://schemas.android.com/apk/res/android\$I	摸瓜V3引擎
http://app.caintel.cn//agreement/user_agreement.html	摸瓜V3引擎
aip.baidubce.com	摸瓜V3引擎
connectivitycheck.gstatic.com	摸瓜V3引擎
http://sdkss.shitu.baidu.com/cgi-bin/sdkstat.py	摸瓜V3引擎
http://app.caintel.cn//sinda/member/version/info	摸瓜V3引擎
https://brain.baidu.com/record/api	摸瓜V3引擎
i2.ytimg.com	摸瓜V3引擎
http://schemas.android.com/aapt	摸瓜V3引擎
s.jppush.cn	摸瓜V3引擎

https://aip.baidubce.com/rest/2.0/face/v3/faceverify	摸瓜V3引擎
gmscompliance-pa.googleapis.com	摸瓜V3引擎
clientservices.googleapis.com	摸瓜V3引擎
http://182.92.20.189:9099/	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
https://verify.baidubce.com/verify/1.0/sdk/report	摸瓜V3引擎
https://aip.baidubce.com/oauth/2.0/token?	摸瓜V3引擎
http://app.caintel.cn//answer/index.html	摸瓜V3引擎
http://www.baidu.com	摸瓜V3引擎
lh5.googleusercontent.com	摸瓜V3引擎
http://gcc.gnu.org/bugs.html):	摸瓜V3引擎
ali-stats.jp.push.cn	摸瓜V3引擎
http://web.ccyunmai.com:81/SrvTimeChk?T=%s&M=%s&S=%s&V=%s&C=%d	lib/armeabi-v7a/libIDCardengine.so
https://aip.baidubce.com/public/2.0/license/face-api/app/querydevicelicense	lib/armeabi-v7a/libbd_unifylicense.so

 邮箱线索

 手机线索

手机号	所在文件
13000000000	com/baidu/idl/face/platform/ui/utis/SecRequest.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=sccd, CN=websinda
签名算法: rsassa_pkcs1v15
有效期自: 2018-07-06 07:35:26+00:00
有效期至: 2043-06-30 07:35:26+00:00
发行人: C=sccd, CN=websinda
序列号: 0x596b4d55
哈希算法: sha256
md5值: 79bb9f11c2d141c55fd7ceb2c96c5854
sha1值: 12cf21d4418fc160fc1cfa341c4a30951708b904
sha256值: 6a51b85c9beb5415bc30465a93467c9d72e69fe6a0a8d5835e510dd4c299a806
sha512值: f56e41d314ff5c3347cd602bae3d977c431180cae04125db3c28b0d63f6a0611609ab75b836571d6c8169ae3598d711d4dc958b2d566994f80bc17ece6d6c701
公钥算法: rsa
密钥长度: 2048
指纹: f351890d5df864bcd5ffd32bedb11593a6431bf969ab35aef7a1c2436ce19e77

🔑 硬编码敏感信息

可能的敏感信息
"authorization" : "账号正在审核中。。。"
"inputUserName" : "联系人"

"password" : "请设置您的密码"
"placeverifyuser" : "请确认是身份证本人将面部放入框内，以避免验证错误!"

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
	正常	读取系统安全设置	允许应用程序读取系统安全设置

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.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.hardware.camera.autofocus	未知	Unknown permission	Unknown permission from android reference
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。
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。
com.websinda.sccd.user.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
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.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.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
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

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。