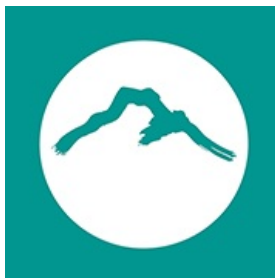




MoGua

玉山银行（中国） 2.12.10.APK 分析报告



APP名称:

玉山银行（中国）

包名:	com.csii.yushanbank
域名线索:	6条
URL线索:	3条
邮箱线索:	0条
分析日期:	2025年7月16日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 玉山银行（中国）.apk

文件大小: 124.22MB
MD5值: 7da2c58a17682b6659422aa937f19ce4
SHA1值: 6ec1c96d5ef87fdfdebc2dbaecef9dcd3db531bd
SHA256值: 86e4c15a4846b6824a720c13cac562e259fd78b986e90768b377be11158d3bb6

i APP 信息

App名称: 玉山银行（中国）
包名: com.csii.yushanbank
主活动Activity: com.csii.yushanbank.ui.main.activity.SplashActivity
安卓版本名称: 2.12.10
安卓版本: 430

🔍 域名线索

域名	服务器信息
29k88m0314.wicp.vip	IP: 146.56.248.213 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
210.75.13.102	IP: 210.75.13.102 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545673 经度: 114.068108
120.78.145.220	IP: 120.78.145.220 所属国家: China 地区: Zhejiang 城市: Hangzhou

	纬度: 30.293650 经度: 120.161583
g3wena.natappfree.cc	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
pbankuat.esun-bank.com.cn	IP: 221.15.70.53 所属国家: China 地区: Henan 城市: Luoyang 纬度: 34.683289 经度: 112.453911
testesunbank.natapp1.cc	没有服务器地理信息.

 URL线索

URL信息	Url所在文件
http://29k88m0314.wicp.vip	摸瓜V2引擎
http://210.75.13.102	摸瓜V2引擎
https://pbankuat.esun-bank.com.cn	摸瓜V2引擎
http://g3wena.natappfree.cc	摸瓜V2引擎
http://testesunbank.natapp1.cc	摸瓜V2引擎
http://29k88m0314.wicp.vip/pmobilebank/index.html	摸瓜V2引擎

http://210.75.13.102/pmobilebank/index.html	摸瓜V2引擎
https://pbankuat.esun-bank.com.cn/pmobilebank/index.html	摸瓜V2引擎
http://g3wena.natappfree.cc/pmobilebank/index.html	摸瓜V2引擎
http://120.78.145.220/pmobilebank/index.html	摸瓜V2引擎
http://testesunbank.natapp1.cc/pmobilebank/index.html	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/zhzl2.png	摸瓜V2引擎
http://120.78.145.220/app/company/index.html	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/zhzl3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/zhzl1.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/jymx2.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/jymx3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/jymx1.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/dzhdcx2.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/dzhdcx3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/dzhdcx1.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/dzhdyz2.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/dzhdyz3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/vadz2.png	摸瓜V2引擎

http://120.78.145.220/esunimage/menu_icon/ent/yqdz2.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/yqdz3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/yqdz1.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/zhyledz2.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/zhyledz3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/zhyledz1.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/hnzz2.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/hnzz3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/hnzz1.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/khzz2.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/khzz3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/khzz1.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/yylzzcx2.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/yylzzcx3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/yylzzcx1.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/plzzcx2.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/plzzcx3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/plzzcx1.png	摸瓜V2引擎

http://120.78.145.220/esunimage/menu_icon/ent/ywsqcx2.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/ywsqcx3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/ywsqcx1.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/ywsq2.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/ywsq3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/ywsq1.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/jgxck2.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/jgxck3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/jgxck1.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/mxcx2.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/mxcx3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/mxcx1.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/ckcp2.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/ckcp3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/ckcp1.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/wdyy2.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/wdyy3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/wdyy1.png	摸瓜V2引擎

http://120.78.145.220/esunimage/menu_icon/ent/wdyq1.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/ckjsq2.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/ckjsq3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/ckjsq1.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/dkjsq2.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/dkjsq3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/dkjsq1.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/lcjsq2.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/lcjsq3.png	摸瓜V2引擎
http://120.78.145.220/esunimage/menu_icon/ent/lcjsq1.png	摸瓜V2引擎

 邮箱线索

 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=CN, ST=GD, L=Shenzhen, O=E.Sun Bank(China)Co.,Ltd, OU=E.Sun Bank(China)Co.,Ltd, CN=E.Sun Bank(China)Co.,Ltd
签名算法: rsassa_pkcs1v15
有效期自: 2018-12-11 11:22:07+00:00
有效期至: 2073-09-13 11:22:07+00:00
发行人: C=CN, ST=GD, L=Shenzhen, O=E.Sun Bank(China)Co.,Ltd, OU=E.Sun Bank(China)Co.,Ltd, CN=E.Sun Bank(China)Co.,Ltd
序列号: 0x2c6c5ec7
哈希算法: sha256
md5值: 2b645a4cfa152e79d819879e5e71fa09
sha1值: 83c313b46e4460f496e5e11c3d7b55c3eb5ec8ba
sha256值: e2be131bde934ffbeeb1168bc4f16eb4aee3bf945b07d25efbae2a2244bea744a
sha512值: 3babbc491ec3a3902087f99c4283cb42bd956b3a67c1973845e5800308a0cbea5533e52b86e7238354db3e05177f2fe0d164db0f65dbd1face40b67490773a1a
公钥算法: rsa
密钥长度: 2048
指纹: 3437ea5ca4e8235f5b2f2af8b436c9fdec6dea114e0f143b3bd704d250ee0d01

硬编码敏感信息

可能的敏感信息
"username" : "姓名"

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.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.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_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_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference

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.USE_FINGERPRINT	正常	allow use of指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
com.fingerprints.service.ACCESS_FINGERPRINT_MANAGER	未知	Unknown permission	Unknown permission from android reference
com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
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
com.csii.yushanbank.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference

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。