MoGua

华瑞银行 8.0.6.APK 分析报告

APP名称:	华瑞银行
包名:	com.huaruibank.android.hulubank
域名线索:	19条
URL线索:	2条
邮箱线索:	0条
分析日期:	2025年6月26日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 华瑞银行.apk
文件大小: 66.65MB
MD5值: 6379e3d85c8fea628b5c30ea123eeed6
SHA1值: 1e0dd836a8290f28b5f44043da5172a83f343042
SHA256值: e510775d5dd4f8fb21bd5e719bed23d6cab2ddc70aafe47476766fb2cfab685a

APP 信息

App名称: 华瑞银行
包名: com.huaruibank.android.hulubank
主活动Activity: com.alipay.mobile.quinox.LauncherActivity
安卓版本名称: 8.0.6
安卓版本: 954

域名线索

域名	服务器信息
00000098.mobilebank	没有服务器地理信息.
render.alipay.com	**IP**: 27.221.78.204 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941
..mybank.cn	没有服务器地理信息.
..poseidong.com	没有服务器地理信息.
act.aligames.com	**IP**: 218.11.15.212 **所属国家**: China **地区**: Hebei **城市**: Shijiazhuang **纬度**: 38.041599 **经度**: 114.478081

..jimingkeji.com.cn	没有服务器地理信息.
00000014.mobilebank	没有服务器地理信息.
20000920.h5app.alipay.com	没有服务器地理信息.
a.alipayobjects.com	IP: 221.194.147.197 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
openauth.alipay.com	IP: 203.209.247.64 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
..mucfc.com	没有服务器地理信息.
..fapiao	没有服务器地理信息.
mpaas.shrbank.com	IP: 118.126.51.70 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
m.51yzone.com	IP: 121.199.193.25 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
..jss.com.cn	没有服务器地理信息.
a.idsuipai	没有服务器地理信息.
sky.vip.youku.com	IP: 116.196.142.207 **所属国家**: China **地区**: Zhejiang **城市**: Jinhua **纬度**: 30.013470 **经度**: 120.288658
as.alipayobjects.com	IP: 116.142.245.228 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
static.alipay.com	IP: 203.209.245.120 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583

URL线索

URL信息
https://mpaas.shrbank.com:443/E56672F051655_prd/v1.0.0.0/images/fail.png
https://mpaas.shrbank.com:443/E56672F051655-prd/00000098/1.0.0.39_all/nebula/00000098_1.0.0.39.amr
https://00000098.mobilebank_prd.shrbank.com
https://mpaas.shrbank.com:443/E56672F051655-prd/00000014/1.0.0.41_all/nebula/fallback/
https://mpaas.shrbank.com:443/E56672F051655-prd/00000014/1.0.0.41_all/nebula/00000014_1.0.0.41.amr
https://00000014.mobilebank_prd.shrbank.com
https://(.*[.]mybank[.]cn)$\
https://(jskp

https://m[.]51yzone[.]com$\

https://.*[.]((jimingkeji[.]com[.]cn)

https://.*[.]jimingkeji[.]com[.]cn$\

https://(((betaalipay

https://((a[.]idsuipai)

https://act[.]aligames[.]com$\

https://((www

https://((sky[.]vip[.]youku[.]com)

https://(sky[.]vip[.]youku[.]com

https://.*[.]jss[.]com[.]cn$\

https://.*[.](fapiao

https://((x

https://.*[.]mucfc[.]com$\

https://.*[.]poseidong[.]com$\

https://openauth.alipay.com/oauth2/publicAppAuthorize.htm?app_id=2016042601338846&scope=auth_userinfo&redirect_uri=http%3a%2f%2fjsfwpt.lsyypt.com%2fhkOrder%2fjshksqfwc&state=fwcljhk\

https://openauth.alipay.com/oauth2/publicAppAuthorize.htm?app_id=2016042601338846&scope=auth_userinfo&redirect_uri=http%3a%2f%2fjsfwpt.lsyypt.com%2fhkOrder%2fjshkjlfwc&state=fwchkjl\

https://openauth.alipay.com/oauth2/publicAppAuthorize.htm?app_id=2016042601338846&scope=auth_userinfo&redirect_uri=http%3A%2F%2Fjsfwpt.lsyypt.com%2FhkOrder%2Fjshksqcfw&state=csfw\

https://openauth.alipay.com/oauth2/publicAppAuthorize.htm?
app_id=2014042900005397&auth_skip=true&scope=auth_base&redirect_uri=https%3A%2F%2Foauth.cc.cmbchina.com%2FOauthPortal%2Falipay%2Fcallback%3Foauth_id%3D20405188%26callback_uri%3Dhttps%3A%2F%2Fxyk.cmbchina.com%2FmyAccount%2Fonekeyquery%2Findex

https://a.alipayobjects.com/amui/native/9.0/amui.css

https://as.alipayobjects.com/g/component/antbridge/1.1.3/antbridge.min.js

https://static.alipay.com/alibridge/1.0.0/alibridge.min.js

https://as.alipayobjects.com/g/h5-lib/antui/9.9.0-2/rem/antui.css

https://as.alipayobjects.com/g/h5-lib/vue/1.0.26/vue.min.js
https://a.alipayobjects.com/g/antui/antui/10.0.0/rem/antui.css
https://a.alipayobjects.com/g/antui/antui-img/1.0.0/page-result/error.png
https://a.alipayobjects.com/g/antui/antui-img/1.0.0/page-result/system_busy.png
https://a.alipayobjects.com/g/antui/antui-img/1.0.0/page-result/blank_page.png
https://a.alipayobjects.com/g/antui/antui-img/1.0.0/page-result/404.png\
https://render.alipay.com/p/f/result/index.html?type=result-busy&scene=industry_container_monitor\
https://20000920.h5app.alipay.com/www/error.htm?from=nebulaPageError\

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: False
找到 1 个唯一证书
主题: CN=HRDBank
签名算法: rsassa_pkcs1v15
有效期自: 2015-05-18 13:05:45+00:00
有效期至: 3014-09-18 13:05:45+00:00
发行人: CN=HRDBank
序列号: 0x1407b525
哈希算法: sha256
md5值: a28e28f69ae55299c0416149bc695e3d
sha1值: 3891a5b667ffc8302842dc63f704633f2aff6e1b
sha256值: e98ac6d432d397bba94846b80858e4a785307e4918b4c75f02d2067883756da8
sha512值: 92fad2f9ea9e0e5aa43181fe6251bfb64cab7c4e6657c2d754c0fb1a4567720d21134d7b53d40480816402cf1f9b7e58cd8c29eb278dfa2112261b2bb0c30854
公钥算法: rsa
密钥长度: 2048
指纹: ff1d7d686a04ffc7b0fd9c9caf34875a96fffc829a5b3a3ad7e4e26837ad33c2

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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
android.permission.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定
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.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.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
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.USE_BIOMETRIC	正常		允许应用使用设备支持的生物识别模式。
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
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.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
com.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
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.huaruibank.android.hulubank.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.FOREGROUND_SERVICE_MEDIA_PROJECTION	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.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
android.permission.ZTE_HEARTYSERVICE_MANAGEMENT	未知	Unknown permission	Unknown permission from android reference
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.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.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。

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.alipay.mobile.quinox.LauncherActivity	Schemes: shrbank://, Hosts: platformapi, Path Prefixes: /startapp,