



招银理财 1.30.1.APK 分析报告



APP名称:

招银理财

包名:	com.cmbchinawm.ds
域名线索:	35条
URL线索:	23条
邮箱线索:	1条
分析日期:	2025年10月3日
分析平台:	摸瓜APK反编译平台

文件名: zylc_prd-2025-07-29-200422.apk
文件大小: 72.36MB
MD5值: 20438a90670139627ad484664d80d272
SHA1值: 18de7a4ed04d04dd73ca188f3514601e1f2a95ca
SHA256值: 5fd5bca4864dee9f94f7761b77dcf6912f9eee50d8c46dbf37e3e7c2365bc064

i APP 信息

App名称: 招银理财
包名: com.cmbchinawm.ds
主活动Activity: com.cmbchina.cmf.ui.splash.SplashActivity
安卓版本名称: 1.30.1
安卓版本: 34

🔍 域名线索

域名	服务器信息
example.com	IP: 23.220.75.245 所属国家: United States of America 地区: California 城市: El Segundo 纬度: 33.919201 经度: -118.416580
sizzlejs.com	IP: 104.17.99.190 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
beian.miit.gov.cn	IP: 119.39.205.85 所属国家: China 地区: Hunan

	城市: Zhuzhou 纬度: 27.833330 经度: 113.150002
www.jrcpcx.cn	IP: 114.247.175.3 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
download-ds-app.paas.cmbchina.com	IP: 58.250.104.44 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545673 经度: 114.068108
url.spec.whatwg.org	IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton 纬度: 40.858585 经度: -74.163605
developer.mozilla.org	IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
bit.ly	IP: 67.199.248.11 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.750134 经度: -73.997009
	IP: 50.116.11.184

feross.org	所属国家: United States of America 地区: California 城市: Fremont 纬度: 37.548271 经度: -121.988571
apps.apple.com	IP: 60.26.220.36 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
ds-gateway.paas.cmbchina.com	IP: 58.250.104.44 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545673 经度: 114.068108
vuejs.org	IP: 3.33.186.135 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
jquery.com	IP: 104.18.155.119 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

tc39.github.io	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
hammerjs.github.io	IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
lf12-32-gateway-st.csst.cmburl.cn	没有服务器地理信息.
storage.googleapis.com	IP: 142.250.73.155 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
lf12-32-gateway-st.paasst.cmbchina.cn	没有服务器地理信息.
next.vuex.vuejs.org	IP: 3.33.186.135 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
goo.gl	IP: 142.250.69.174 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514

sj.qq.com	IP: 123.125.246.121 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
mswjs.io	IP: 216.150.16.65 所属国家: Canada 地区: Ontario 城市: Etobicoke 纬度: 43.623768 经度: -79.559723
lf12-32-gateway-dev.paas.cmbchina.cn	没有服务器地理信息.
jianwei.paas.cmbchina.com	IP: 58.250.105.1 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545673 经度: 114.068108
opensource.org	IP: 172.66.171.169 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
m.cmbchina.com	IP: 58.33.159.53 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
	IP: 43.196.8.153 所属国家: China

www.cmbchinawm.com	地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
clipboardjs.com	IP: 172.67.168.158 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
lf12-32-gateway.paas.cmbchina.com	IP: 58.250.104.117 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545673 经度: 114.068108
lf12-32-gateway-biz.paas.cmbchina.cn	没有服务器地理信息.
js.foundation	IP: 104.131.8.164 所属国家: United States of America 地区: New Jersey 城市: Clifton 纬度: 40.858585 经度: -74.163605
jquery.org	IP: 104.17.176.200 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
fmcrm-gateway.paas.cmbchina.com	没有服务器地理信息.
	IP: 20.205.243.166

github.com	所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
------------	---

 URL线索

URL信息	Url所在文件
https://m.cmbchina.com	摸瓜V1引擎
https://github.com/mswjs/msw	摸瓜V2引擎
https://mswjs.io/docs/recipes/mocking-error-responses\	摸瓜V2引擎
https://goo.gl/nhQhGp	摸瓜V2引擎
https://goo.gl/2aRDsh	摸瓜V2引擎
https://storage.googleapis.com/workbox-cdn/releases/4.3.1/workbox-sw.js	摸瓜V2引擎
https://goo.gl/S9QRab	摸瓜V2引擎
https://lf12-32-gateway-st.paasst.cmbchina.cn	摸瓜V2引擎

http://lf12-32-gateway-st.paasst.cmbchina.cn	摸瓜V2引擎
https://lf12-32-gateway-st.csst.cmburl.cn	摸瓜V2引擎
http://lf12-32-gateway-st.csst.cmburl.cn	摸瓜V2引擎
https://lf12-32-gateway-biz.paas.cmbchina.cn	摸瓜V2引擎
http://lf12-32-gateway-biz.paas.cmbchina.cn	摸瓜V2引擎
https://lf12-32-gateway.paas.cmbchina.com	摸瓜V2引擎
http://lf12-32-gateway.paas.cmbchina.com	摸瓜V2引擎
http://lf12-32-gateway-dev.paas.cmbchina.cn	摸瓜V2引擎
https://lf12-32-gateway-dev.paas.cmbchina.cn	摸瓜V2引擎
http://a	摸瓜V2引擎
http://a/c%20d?a=1&c=3	摸瓜V2引擎
https://a@b	摸瓜V2引擎
	摸瓜V2引擎

http://x	摸瓜V2引擎
http://feross.org >	摸瓜V2引擎
https://github.com/Tencent/vConsole)	摸瓜V2引擎
http://opensource.org/licenses/MIT	摸瓜V2引擎
https://github.com/zloirock/core-js/blob/v3.21.1/LICENSE	摸瓜V2引擎
https://github.com/zloirock/core-js	摸瓜V2引擎
https://bit.ly/3cXEKWf	摸瓜V2引擎
https://next.vuex.vuejs.org/	摸瓜V2引擎
https://vuejs.org/images/icons/favicon-96x96.png	摸瓜V2引擎
https://github.com/zloirock/core-js/blob/v3.25.0/LICENSE	摸瓜V2引擎
http://hammerjs.github.io/	摸瓜V2引擎
https://feross.org/opensource >	摸瓜V2引擎
https://www.rmhchinawm.com	摸瓜V2引擎

https://www.cmbchinawm.com	引擎
https://www.cmbchinawm.com	摸瓜V2引擎
https://www.jrcpcx.cn	摸瓜V2引擎
https://www.jrcpcx.cn	摸瓜V2引擎
http://cmf/revokeFaceAgreement	摸瓜V2引擎
http://cmf/exitApp	摸瓜V2引擎
http://cmf/picture	摸瓜V2引擎
http://cmf/revokeAgreement	摸瓜V2引擎
http://cmf/exitApp	摸瓜V2引擎
https://sj.qq.com/appdetail/	摸瓜V2引擎
https://clipboardjs.com/	摸瓜V2引擎
https://sj.qq.com/appdetail/	摸瓜V2引擎
https://clipboardjs.com/	摸瓜V2引擎

http://cmf/imageClipper	摸瓜V2引擎
https://example.com	摸瓜V2引擎
http://cmf/topBarUI	摸瓜V2引擎
http://cmf/apiOcr	摸瓜V2引擎
http://a	摸瓜V2引擎
http://a/c%20d	摸瓜V2引擎
https://jquery.com/	摸瓜V2引擎
https://sizzlejs.com/	摸瓜V2引擎
https://jquery.org/license	摸瓜V2引擎
https://js.foundation/	摸瓜V2引擎
https://github.com/WebReflection/url-search-params/blob/master/src/url-search-params.js\r\n	摸瓜V2引擎
https://url.spec.whatwg.org/	摸瓜V2引擎
	摸瓜V2引擎

https://github.com/arv/DOM-URL-Polyfill/blob/master/src/url.js\r\n	摸瓜V2引擎
http://a');\r\n	摸瓜V2引擎
http://a/c%20d')	摸瓜V2引擎
http://foo:8080\r\n	摸瓜V2引擎
https://tc39.github.io/ecma262/	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/Array/includes\r\nif	摸瓜V2引擎
http://cmf/picture	摸瓜V2引擎
http://cmf/apiOcr	摸瓜V2引擎
https://ds-gateway.paas.cmbchina.com/api	摸瓜V2引擎
https://fmcrm-gateway.paas.cmbchina.com/commonsvr/api/v1	摸瓜V2引擎
https://jianwei.paas.cmbchina.com/front-rest-log/v2/encrypt_batch_upload	摸瓜V2引擎
https://jianwei.paas.cmbchina.com/front-rest-log/v3/batchTrace	摸瓜V2引擎
https://download-ds-app.paas.cmbchina.com	摸瓜V2引擎

	引擎
https://beian.miit.gov.cn/	摸瓜V2引擎
https://clipboardjs.com/	摸瓜V2引擎
http://cmf/picture	摸瓜V2引擎
http://cmf/apiOcr	摸瓜V2引擎
https://clipboardjs.com/	摸瓜V2引擎
http://cmf/revokeAgreement	摸瓜V2引擎
http://cmf/exitApp	摸瓜V2引擎
http://cmf/eventHandle	摸瓜V2引擎
http://cmf/crypto	摸瓜V2引擎
https://download-ds-app.paas.cmbchina.com/	摸瓜V2引擎
http://cmf/patternLockAuth	摸瓜V2引擎
http://cmf/exitApp	摸瓜V2引擎

https://ds-gateway.paas.cmbchina.com/api	摸瓜V2 引擎
https://fmcrm-gateway.paas.cmbchina.com/commonsvr/api/v1	摸瓜V2 引擎
http://cmf/gestureToBack	摸瓜V2 引擎
http://cmf/backPressed	摸瓜V2 引擎
http://cmf/secureStorage	摸瓜V2 引擎
http://cmf/storage	摸瓜V2 引擎
http://cmf/deviceInfo	摸瓜V2 引擎
http://cmf/jumpToBrowser	摸瓜V2 引擎
http://cmf/openAppByPackage	摸瓜V2 引擎
http://cmf/systemSetting	摸瓜V2 引擎
http://cmf/installedApp	摸瓜V2 引擎
http://cmf/uiMode	摸瓜V2 引擎
	摸瓜V2

http://cmf/networkStatus	摸瓜V2引擎
http://cmf/safeAreaInsets	摸瓜V2引擎
http://cmf/networkListener	摸瓜V2引擎
http://cmf/faceIdentification	摸瓜V2引擎
http://cmf/topBarUI	摸瓜V2引擎
http://cmf/goBackToRoot	摸瓜V2引擎
http://cmfweb/webviewReturn	摸瓜V2引擎
http://cmf/filePreview	摸瓜V2引擎
https://ds-gateway.paas.cmbchina.com/api/dsmac/file/commonPreview/	摸瓜V2引擎
https://__bridge_loaded__	摸瓜V2引擎
https://apps.apple.com/cn/app/%E4%B8%AD%E5%9B%BD%E5%B7%A5%E5%95%86%E9%93%B6%E8%A1%8C/id423514795	摸瓜V2引擎
https://apps.apple.com/cn/app/%E4%B8%AD%E5%9B%BD%E5%BB%BA%E8%AE%BE%E9%93%B6%E8%A1%8C/id391965015	摸瓜V2引擎
https://apps.apple.com/cn/app/%E4%B8%AD%E5%9B%BD%E5%86%9C%E4%B8%9A%E9%93%B6%E8%A1%8C/id515651240	摸瓜V2引擎

https://apps.apple.com/cn/app/%E6%B0%91%E7%94%9F%E9%93%B6%E8%A1%8C%E6%89%8B%E6%9C%BA%E9%93%B6%E8%A1%8C/id523091708	引擎
https://apps.apple.com/cn/app/%E5%85%89%E5%A4%A7%E9%93%B6%E8%A1%8C%E6%89%8B%E6%9C%BA%E9%93%B6%E8%A1%8C/id447733826	摸瓜V2引擎
https://apps.apple.com/cn/app/%E9%82%AE%E5%82%A8%E6%89%8B%E6%9C%BA%E9%93%B6%E8%A1%8C/id493489515	摸瓜V2引擎
https://apps.apple.com/cn/app/%E4%B8%AD%E5%9B%BD%E9%93%B6%E8%A1%8C/id399608199	摸瓜V2引擎
https://apps.apple.com/cn/app/%E4%BA%A4%E9%80%9A%E9%93%B6%E8%A1%8C/id337876534	摸瓜V2引擎
https://apps.apple.com/cn/app/%E6%8B%9B%E5%95%86%E9%93%B6%E8%A1%8C/id392899425	摸瓜V2引擎
https://apps.apple.com/cn/app/%E4%B8%AD%E4%BF%A1%E9%93%B6%E8%A1%8C%E6%89%8B%E6%9C%BA%E9%93%B6%E8%A1%8C/id422844108	摸瓜V2引擎
https://apps.apple.com/cn/app/%E5%8D%8E%E5%A4%8F%E6%89%8B%E6%9C%BA%E9%93%B6%E8%A1%8C/id1473728816	摸瓜V2引擎
https://apps.apple.com/cn/app/%E6%B5%A6%E5%8F%91%E9%93%B6%E8%A1%8C/id471855847	摸瓜V2引擎
https://apps.apple.com/cn/app/%E5%B9%BF%E5%8F%91%E9%93%B6%E8%A1%8C%E6%89%8B%E6%9C%BA%E9%93%B6%E8%A1%8C/id415872960	摸瓜V2引擎
https://apps.apple.com/cn/app/%E5%85%B4%E4%B8%9A%E9%93%B6%E8%A1%8C%E6%89%8B%E6%9C%BA%E9%93%B6%E8%A1%8C/id433592972	摸瓜V2引擎
https://apps.apple.com/cn/app/%E5%B9%B3%E5%AE%89%E5%8F%A3%E8%A2%8B%E9%93%B6%E8%A1%8C-%E6%9B%B4%E6%87%82%E6%82%A8%E7%9A%84%E6%99%BA%E8%83%BD%E9%93%B6%E8%A1%8C/id1085016815	摸瓜V2引擎

https://apps.apple.com/cn/app/%E4%B8%8A%E6%B5%B7%E9%93%B6%E8%A1%8C%E6%89%8B%E6%9C%BA%E9%93%B6%E8%A1%8C/id631875777	摸瓜V2引擎
https://apps.apple.com/cn/app/%E4%BA%AC%E5%BD%A9%E7%94%9F%E6%B4%BB-%E5%8C%97%E4%BA%AC%E9%93%B6%E8%A1%8C%E6%89%8B%E6%9C%BA%E9%93%B6%E8%A1%8C%E5%AE%A2%E6%88%B7%E7%AB%AF/id434831001	摸瓜V2引擎
https://apps.apple.com/cn/app/%E5%AE%81%E6%B3%A2%E9%93%B6%E8%A1%8C/id531012674	摸瓜V2引擎
http://cmf/fingerprintAuth	摸瓜V2引擎
https://sj.qq.com/appdetail/	摸瓜V2引擎
https://clipboardjs.com/	摸瓜V2引擎
https://download-ds-app.paas.cmbchina.com/	摸瓜V2引擎

 邮箱线索

邮箱地址	所在文件
cmbwm_service@cmbchina.com	摸瓜V2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: True
找到 1 个唯一证书
主题: C=CN, ST=GD, L=SZ, O=CMB
签名算法: rsassa_pkcs1v15
有效期自: 2021-12-13 02:23:12+00:00
有效期至: 2046-12-07 02:23:12+00:00
发行人: C=CN, ST=GD, L=SZ, O=CMB
序列号: 0x3b45daac
哈希算法: sha256
md5值: f20e65d67eddcdb2ab56ea83690a6732d
sha1值: c01dfefe7562920c91c9650faee7140da67daca5
sha256值: 34329aab6fc5229cdaa12f7b255a0aa2c71b9581c0f5798de90e5a74d445238b
sha512值: 275e8ce4fcc9971662c8104de887a159944bc9e2b1e9531ba6eff8fdec3b394c87c004fb3acd945ab9118bf5b684188ac1abb1d0ede6693f51f6f51f07def95a
公钥算法: rsa
密钥长度: 2048
指纹: 1ed81d007729b55b430ab9f557b5dcd9c8c1497e032cd560717bcb9b4fbf1c49

🔑 硬编码敏感信息

可能的敏感信息
"cancel_more_auth" : "取消"
"face_authorized_msg" : "拒绝人脸识别验证将会无法继续操作，确定拒绝吗？"
"keyboard_secret" : "配置安全键盘密钥"
"keyboard_secret_info" : "自定义安全键盘密钥不能为空"
"login_pwd" : "密码登录"

"more_auth_btn" : "切换账号或登录方式"
"more_auth_verify_btn" : "更多"
"safe_keyboard_secret_title" : "请输入安全键盘密钥"
"keyboard_secret" : "配置安全键盘密钥"
"keyboard_secret_info" : "自定义安全键盘密钥不能为空"
"safe_keyboard_secret_title" : "请输入安全键盘密钥"
"keyboard_secret" : "配置安全鍵盤密鑰"
"keyboard_secret_info" : "自定義安全鍵盤密鑰不能為空"
"safe_keyboard_secret_title" : "請輸入安全鍵盤密鑰"

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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
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.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.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.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.USE_BIOMETRIC	正常		允许应用使用设备支持的生物识别模式。
android.permission.DETECT_SCREEN_CAPTURE	未知	Unknown permission	Unknown permission from android reference
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.READ_PRIVILEGED_PHONE_STATE	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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

应用内通信