MoGua

成都银行 7.0.4.APK 分析报告

APP名称:	成都银行

包名:	com.yitong.cd.mbank.android
域名线索:	19条
URL线索:	6条
邮箱线索:	0条
分析日期:	2024年7月27日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 成都银行.apk
文件大小: 159.25MB
MD5值: d63cb64c6a1bc19cec7a6490c7f8eb3c
SHA1值: 7ba27b42f8386421731a600bdea564b875f2ed9b
SHA256值: df0ce8ae5a49950d811ca26262572a6346bc69d27fa4245f6a16058464fb680b

APP 信息

App名称: 成都银行
包名: com.yitong.cd.mbank.android
主活动Activity: com.yitong.mobile.biz.launcher.app.SplashActivity
安卓版本名称: 7.0.4
安卓版本: 7004

域名线索

域名	服务器信息
metrics1-drcn.dt.dbankcloud.cn	**IP**: 111.202.16.252 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
facebook.github.io	**IP**: 185.199.111.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
reactjs.org	**IP**: 76.76.21.21 **所属国家**: United States of America **地区**: California

	城市: Walnut **纬度**: 34.015400 **经度**: -117.858223
metrics2.data.hicloud.com	IP: 80.158.2.190 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
data-drcn.push.dbankcloud.com	IP: 49.4.40.58 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
data-drru.push.dbankcloud.com	IP: 159.138.202.31 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
grs.dbankcloud.cn	IP: 121.36.116.8 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
fb.me	IP: 163.70.159.35 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249
	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
grs.dbankcloud.eu	没有服务器地理信息.
grs.dbankcloud.asia	IP: 49.4.40.185 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
www.yitong.com.cn	IP: 120.193.95.245 **所属国家**: China **地区**: Anhui **城市**: Hefei **纬度**: 31.863815 **经度**: 117.280830
grs.platform.dbankcloud.ru	没有服务器地理信息.
data-dre.push.dbankcloud.com	IP: 80.158.49.244 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
grs.dbankcloud.com	IP: 113.201.107.54 **所属国家**: China **地区**: Shaanxi **城市**: Baoji **纬度**: 34.353611 **经度**: 107.375275
	IP: 119.8.163.189

data-dra.push.dbankcloud.com	**所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
metrics5.data.hicloud.com	IP: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
metrics-dra.dt.hicloud.com	IP: 94.74.88.100 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
metrics5.dt.dbankcloud.ru	IP: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499

URL线索

URL信息	Url所在文件
https://github.com/vinc3m1	Mogua Engine V1
https://github.com/vinc3m1/RoundedImageView	Mogua Engine V1

https://github.com/vinc3m1/RoundedImageView.git	Mogua Engine V1
https://data-drcn.push.dbankcloud.com	Mogua Engine V2
https://data-dra.push.dbankcloud.com	Mogua Engine V2
https://data-dre.push.dbankcloud.com	Mogua Engine V2
https://data-drru.push.dbankcloud.com	Mogua Engine V2
https://metrics1-drcn.dt.dbankcloud.cn:443	Mogua Engine V2
https://metrics-dra.dt.hicloud.com:6447	Mogua Engine V2
https://metrics2.data.hicloud.com:6447	Mogua Engine V2
https://metrics5.data.hicloud.com:6447	Mogua Engine V2
https://metrics5.dt.dbankcloud.ru:6447	Mogua Engine V2
https://grs.dbankcloud.com	Mogua Engine V2
https://grs.dbankcloud.cn	Mogua Engine V2
https://grs.dbankcloud.asia	Mogua Engine V2
https://grs.platform.dbankcloud.ru	Mogua Engine V2
https://grs.dbankcloud.eu	Mogua Engine V2
http://www.yitong.com.cn:10080/ares-inte-gateway/page/client.html	Mogua Engine V2
https://reactjs.org/docs/error-decoder.html?invariant=	Mogua Engine V2
https://fb.me/nolistview	Mogua Engine V2

https://github.com/react-native-community/react-native-masked-view	Mogua Engine V2
https://github.com/react-native-community/react-native-slider	Mogua Engine V2
https://github.com/react-native-community/react-native-viewpager	Mogua Engine V2
https://github.com/react-native-community/react-native-webview	Mogua Engine V2
https://github.com/react-native-community/react-native-async-storage	Mogua Engine V2
https://github.com/react-native-community/react-native-netinfo	Mogua Engine V2
http://facebook.github.io/react-native/docs/navigation.html	Mogua Engine V2
http://fb.me/use-check-prop-types	Mogua Engine V2
https://fb.me/react-refs-must-have-owner	Mogua Engine V2
https://fb.me/react-invalid-hook-call)	Mogua Engine V2
https://fb.me/react-polyfills	Mogua Engine V2
https://github.com/facebook/react-native/issues/11094	Mogua Engine V2
http://*','https://*'],extractOrigin:function(t)	Mogua Engine V2

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: CN=cdp_android
签名算法: rsassa_pkcs1v15
有效期自: 2013-10-21 12:37:35+00:00
有效期至: 3012-02-22 12:37:35+00:00
发行人: CN=cdp_android
序列号: 0x5265200f
哈希算法: sha1
md5值: 87c8c5d97e0de6d6bb5deac2a387e474
sha1值: f0ac87b8280cf3c0911207ff5e0ceb4752dfa07e
sha256值: cea19c9b0130d649d1a26b1fe94433636f68c744613e6758cb81ec0bc6d86b55
sha512值: f510faa58d0fd9434b86237aa4d9ef3c9dffe0768ed653a62d3bcb4130bc79cc31e1439536e69eda0e04a8a4c599fe48ca910f6a25a63fcef9eb7c0560422ee4
公钥算法: rsa
密钥长度: 1024
指纹: 704233185536eb4a5b5adab045e46a709e0a44e1c279547d773976db7d16dd32

硬编码敏感信息

可能的敏感信息
"cw_demo_app_secret_fail" : "AppSecret不能为空"
"cw_demo_ocr_authority" : "签发机关："
"cw_demo_server_app_key" : "App key："
"cw_demo_server_app_secret" : "App secret："
"library_roundedimageview_author" : "Vince Mi"

"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"login_forget_pwd_str" : "忘记密码?"
"login_input_pwd_str" : "请输入登录密码"
"login_pwd_min_eight" : "请输入8-20位由数字和字母组成的登录密码"
"login_pwd_min_six" : "请输入6位及以上的密码"
"login_pwd_str" : "请输入登录密码"
"upsdk_care_forget_password" : "忘记密码按钮"

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
com.yitong.cd.mbank.android.permission.HCE_PUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.NFC	正常	控制近场通信	允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信
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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
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_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.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
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.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.MANAGE_FINGERPRINT	未知	Unknown permission	Unknown permission from android reference
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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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
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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
	正	重新排序正在	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

android.permission.REORDER_TASKS	常	运行的应用程序	下将自己强加于前
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.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.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
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.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.ACCESS_GPS	未知	Unknown permission	Unknown permission from android reference
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.hardware.camera.autofocus	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_ASSISTED_GPS	未知	Unknown permission	Unknown permission from android reference

android.permission.ACCESS_LOCATION	未知	Unknown permission	Unknown permission from android reference
com.yitong.cd.mbank.android.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.yitong.cd.mbank.android.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
android.permission.SCHEDULE_EXACT_ALARM	正常		允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作
getui.permission.GetuiService.com.yitong.cd.mbank.android	未知	Unknown permission	Unknown permission from android reference
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
com.yitong.cd.mbank.android.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.yitong.mobile.biz.h5.container.WebViewActivity	Schemes: bocdonseractlink://, Hosts: bocd.com,
com.yitong.mobile.biz.launcher.app.SplashActivity	Schemes: cdbankphone://, bocdpersonal://, Hosts: cdbank, bocd.com.cn, Path Prefixes: /ebank,

---