MoGua

兴业管家 2.4.43.APK 分析报告

APP名称:	兴业管家

包名:	com.yitong.mbank.xy
域名线索:	3条
URL线索:	2条
邮箱线索:	1条
分析日期:	2025年2月6日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 兴业管家安卓.apk
文件大小: 169.3MB
MD5值: 21ec2f6b88680eeaf8b9e97f3133bd8d
SHA1值: 1e772c4870a7695b465d31a6681ce004c456641e
SHA256值: 741dbf398336ae4317936cff045421f291d8bfae487329ab954746a37c0c8fa5

APP 信息

App名称: 兴业管家
包名: com.yitong.mbank.xy
主活动Activity: com.yitong.mbank.xy.android.activity.SplashActivity
安卓版本名称: 2.4.43
安卓版本: 89

域名线索

域名	服务器信息
code.google.com	**IP**: 142.250.217.78 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
play.google.com	**IP**: 142.251.215.238 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.gnu.org	**IP**: 209.51.188.116 **所属国家**: United States of America **地区**: Massachusetts

	城市: Somerville **纬度**: 42.387600 **经度**: -71.099503

URL线索

URL信息	Url所在文件
https://play.google.com/store/apps/details?id=me.pengpeng.ppme>	摸瓜V1引擎
http://www.gnu.org/licenses/>www.gnu.org/licenses	摸瓜V1引擎
http://code.google.com/p/nfcard/>code.google.com/p/nfcard	摸瓜V1引擎

邮箱线索

邮箱地址	所在文件
sinpowei@gmail.com	摸瓜V1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: False
找到 1 个唯一证书
主题: C=cn, ST=fujian, L=fuzhou, O=cib, OU=it, CN=cib
签名算法: rsassa_pkcs1v15
有效期自: 2015-11-22 10:14:43+00:00
有效期至: 2035-11-17 10:14:43+00:00
发行人: C=cn, ST=fujian, L=fuzhou, O=cib, OU=it, CN=cib
序列号: 0x42ceaa0a
哈希算法: sha256
md5值: 553679d3d2e2d2c13f41b8e2162ecdfe
sha1值: dc54ddd1f7ea352cadd86453068c48dfe63b0e0f
sha256值: b15406c0e7b80e0a5972228056216049c22ba4a2d28909b64fa02427a8690f1f
sha512值: ef68f6d1851068a9929d5abe1862521f04f51ea284534b0644fb8553207b187cbe6805dd5576876dd3d70520228a435418d27d6eabd4728348bbddf78f526e4e
公钥算法: rsa
密钥长度: 2048
指纹: e81a2de3351bd58c96e9421c515b461fa598b24f6d371d5e761ed38521ab959c

🔑 硬编码敏感信息

可能的敏感信息
"authorization_agree" : "同意"
"authorization_cancel" : "取消"
"authorization_title" : "隐私授权"
"blkey_reset_pwd" : "修改蓝牙网盾密码"
"blkey_set_pwd" : "设置蓝牙网盾密码"
"cer_authenticator_description" : "You can set up HUAWEI Digital Certificate Authenticator with Certification on your Android device to sign in the APP. It's secure and more convenient than signing in with your username and password."
"cer_ks_authenticator_description" : "You can set up Level 3 KeyStore Digital Certificate AUTHENTICATOR with Certification on your Android device to sign in the APP. It's secure and more convenient than signing in with your username and password."

"cer_ks_fingerprint_authenticator_description_sm2" : "You can set up Level 3 KeyStore Digital Certificate AUTHENTICATOR with Certification on your Android device to sign in the APP. It's secure and more convenient than signing in with your username and password."

"cib_fido_auth_warm_tip" : "手机盾使用的指纹/面容ID为您解锁时的使用的指纹/面容ID，请确保您的设备上没有录入他人的指纹/面容ID信息，否则可能影响您的账户安全。"

"cib_fido_auth_warm_tip_2" : "目前该功能处于试运行阶段，开通手机盾需使用蓝牙盾进行验证，开通后，可在对外支付、内部转账时使用指纹/面容ID进行认证。更换手机需重新开通。"

"cib_fido_blkey_manage_auth_warm_tip" : "为保障安全，开通手机盾请使用蓝牙网盾进行验证"

"cib_fido_finger_auth" : "指纹认证"

"cib_fido_please_choose_fido_auth_way" : "请选择手机盾认证方式"

"click_to_authorize" : "Authorize"

"draw_gestrue_auth_dentity" : "请绘制手势密码，以验证身份"

"each_cannot_session" : "对方已加入黑名单，不能进行会话"

"enable_user" : "激活用户"

"forget_pwd" : "忘记密码?"

"gesture_pwd_login" : "手势密码登录"

"group_contains_username" : "本群里面已经含有此用户"

"inputpsd_auth_dentity" : "请输入您的登录密码，以验证身份"

"login_by_password" : "密码登录"

"login_pwd" : "登录密码"

"login_pwd_length_short" : "密码长度不能小于6位"

"mima_xinhan" : "密码信函"

"modify_gesture_pwd" : "修改手势密码"

"password" : "密码"

"pinpwdCheckPIn" : "验证网盾密码中..."

"pinpwdDoinit" : "正在初始化..."

"pinpwdGetData" : "正在获取数据..."

"pinpwdtip" : "插入支付棒"

"pinpwdtip_tip" : "请插入支付棒进行验证"

"pwdComputeFaile" : "密码计算失败"

"pwd_weak" : "设置密码安全程度较低，请勿将密码设置为姓名拼音、手机号或生日号码等信息"

"select_by_token" : "通过标签选择联系人"

"session" : "会话"

"tip_password" : "请输入登录密码"

"token" : "标签"

"umcsdk_oauth_version_name" : "v1.4.1"

"username" : "请输入登录名"

"cer_authenticator_description" : "您可以使用华为数字证书扩展来完成更安全认证"

"cer_ks_authenticator_description" : "You can set up Level 3 KeyStore Digital Certificate AUTHENTICATOR with Certification on your Android device to sign in the APP. It's sec ure and more convenient than signing in with your username and password."
"cer_ks_fingerprint_authenticator_description_sm2" : "You can set up Level 3 KeyStore Digital Certificate AUTHENTICATOR with Certification on your Android device to sign in the APP. It's secure and more convenient than signing in with your username and password."
"click_to_authorize" : "授权交易"
"cer_authenticator_description" : "您可以設置華為數字證書證書擴展來完成更安全認證"
"cer_ks_authenticator_description" : "You can set up Level 3 KeyStore Digital Certificate AUTHENTICATOR with Certification on your Android device to sign in the APP. It's sec ure and more convenient than signing in with your username and password."
"cer_ks_fingerprint_authenticator_description_sm2" : "You can set up Level 3 KeyStore Digital Certificate AUTHENTICATOR with Certification on your Android device to sign in the APP. It's secure and more convenient than signing in with your username and password."
"click_to_authorize" : "授權交易"

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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.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.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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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
com.yitong.mbank.xy.NetWorkChangeReceiver	未知	Unknown permission	Unknown permission from android reference
com.yitong.mbank.xy.UI.permission.MobUIShell	未知	Unknown permission	Unknown permission from android reference
com.yitong.mbank.xy.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.yitong.mbank.xy.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
android.permission.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加和删除帐户以及删除其密码等操作

android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
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.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.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.SENSOR_INFO	未知	Unknown permission	Unknown permission from android reference
android.permission.SENSOR_ENABLE	未知	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小
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.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
com.csii.ui.permission.SplashScreenActivity	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.PACKAGE_USAGE_STATS	合法	更新组件使用统计	允许修改收集的组件使用统计。不供普通应用程序使用
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。
	系统		允许应用程序在没有用户交互的情况下配对蓝牙设备,并允许或禁止电话簿访问或

android.permission.BLUETOOTH_PRIVILEGED	需要		消息访问。这不适用于第三方应用程序
android.permission.WRITE_USER_DICTIONARY	正常	写入用户定义的字典	允许应用程序将新词写入用户字典
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.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.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.FLAG_ACTIVITY_NEW_TASK	未知	Unknown permission	Unknown permission from android reference
com.huawei.permission.USE_TSM_AGENT	未知	Unknown permission	Unknown permission from android reference
com.huawei.ukey.permission.UEY_MANAGER	未知	Unknown permission	Unknown permission from android reference
org.simalliance.openmobileapi.SMARTCARD	未知	Unknown permission	Unknown permission from android reference
android.permission.USE_BIOMETRIC	正常		允许应用使用设备支持的生物识别模式。
com.huawei.permission.ACCESS_HW_KEYSTORE	未知	Unknown permission	Unknown permission from android reference
com.yitong.mbank.xy.permission.bridge	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.mob.tools.MobUIShell	Schemes: tencent100371282://,
com.yitong.mbank.xy.android.activity.browser.BrowserOperActivity	Schemes: app://, Hosts: xingyeguanjia,

---