MoGua

西铁行 1.4.1.APK 分析报告

APP名称:	西铁行

包名:	com.bwton.xitie
域名线索:	0条
URL线索:	0条
邮箱线索:	0条
分析日期:	2025年10月2日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 西铁行_1.4.1_Apkpure.apk
文件大小: 26.1MB
MD5值: 34d9e31390d2211e21ed6388792f946e
SHA1值: c3f41a5f18a8f41450fe3e1f68699f2f6ff7fca6
SHA256值: 891f850a1a5efa529a51b87b5098eb24932f898fe1aad73c0e0156ccf7b9ff2b

APP 信息

App名称: 西铁行
包名: com.bwton.xitie
主活动Activity: com.bwton.xitie.MainActivity
安卓版本名称: 1.4.1
安卓版本: 59

域名线索

URL线索

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: C=CN, ST=ZJ, L=HZ, O=bwt, OU=bwt, CN=ChuanqiJiang

签名算法: rsassa_pkcs1v15
有效期自: 2019-01-26 08:09:50+00:00
有效期至: 2044-01-20 08:09:50+00:00
发行人: C=CN, ST=ZJ, L=HZ, O=bwt, OU=bwt, CN=ChuanqiJiang
序列号: 0x7ebf43f3
哈希算法: sha256
md5值: bd03ff0602f1bda5c1e0a32c50f432bc
sha1值: f054a8fb48a2f2cf01041739563c8a54cb212ec6
sha256值: 170e6c564d5ee8e9450bb6d2816ec3b903b93f66bc69d6c92b8b4999e8ada3c1
sha512值: 149fe0428dbb68b75c85b49cb310e409709562c50dcc0604e3cf5d8a3ae21985aa83479121b73bcc37238b22f4170404e315dd1b4077a00f1a0b984854ee7f25
公钥算法: rsa
密钥长度: 2048
指纹: 58c49503030ddeb2b6d3e461ae824aba89498de30cb117f0151bd85002c761fc

硬编码敏感信息

可能的敏感信息
"umcsdk_oauth_version_name" : "v1.4.1"

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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.bwton.xitie.MainActivity	Schemes: um.61d93285e014255fcbe0e6b0://,

---