MoGua

习讯宁夏 4.4.5.APK 分析报告

APP名称:	习讯宁夏

包名:	cn.vanber.xixunyun.xxnx
域名线索:	4条
URL线索:	1条
邮箱线索:	1条
分析日期:	2025年7月7日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: base.apk
文件大小: 11.07MB
MD5值: eef1c22832bb65c43322d3d629fb2857
SHA1值: 94f29017445bb3933f2118ccd140b0097627f630
SHA256值: 529d367eb28ceffeb328ba9f724e83282772c91c16acc8991c6180fc410ac4fa

APP 信息

App名称: 习讯宁夏
包名: cn.vanber.xixunyun.xxnx
主活动Activity: cn.vanber.xixun.login.AutoLoginActivity
安卓版本名称: 4.4.5
安卓版本: 44501

域名线索

域名	服务器信息
docs.jiguang.cn	**IP**: 120.46.166.88 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
xixunyun.com	**IP**: 8.133.170.158 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
[illegible]	**IP**: 121.36.35.166 **所属国家**: China

www.jiguang.cn	**地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.umeng.com	**IP**: 59.82.31.95 **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	Url所在文件
https://www.umeng.com/page/policy	摸瓜V1引擎
https://docs.jiguang.cn/	摸瓜V1引擎
https://www.jiguang.cn/license/privacy	摸瓜V1引擎
https://xixunyun.com	摸瓜V1引擎
http://xixunyun.com	摸瓜V1引擎

邮箱线索

邮箱地址	所在文件
你也可以将你的问题发送至lijie@vanber.cn或电话联系我们相	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=北京, L=北京, O=万博云信（北京）教育科技有限公司, OU=万博云信（北京）教育科技有限公司, CN=李杰
签名算法: rsassa_pkcs1v15
有效期自: 2015-11-06 07:00:47+00:00
有效期至: 2070-08-09 07:00:47+00:00
发行人: C=CN, ST=北京, L=北京, O=万博云信（北京）教育科技有限公司, OU=万博云信（北京）教育科技有限公司, CN=李杰
序列号: 0x46ab19ce
哈希算法: sha256
md5值: c7cf4d1ac9e309b5cece4d0d9614b72e
sha1值: c5351a8c884612820a47bca0816017b01d40e965
sha256值: 9f24729b7dd482c5dd6f937f906d97808e83fa222c9571c36a4196208b4513b1
sha512值: 2f873f0dae1474cbd5b87b8f95abc31377e96a34c2de6ee3ff4fcd0e7a49b0f90980aee327088e445a877e39ad716991f53f59a6efe6efb841429f45af56e525
公钥算法: rsa
密钥长度: 2048
指纹: 69c5abd27d1f1d14cff124af9cb08c347dbe5692fc5a217dc4dbb7697d2188bd

硬编码敏感信息

可能的敏感信息
"login_forget_password" : "忘记密码"

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.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.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_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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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_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.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_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
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.RECORD_VIDEO	未知	Unknown permission	Unknown permission from android reference
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.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.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.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.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。

应用内通信