MoGua

职校家园 v1.6.3.APK 分析报告

APP名称: 职校家园

包名:	com.wyl.exam
域名线索:	2条
URL线索:	1条
邮箱线索:	0条
分析日期:	2025年9月29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: 56.99MB
MD5值: f73c9f7d6e9f5e09f32754d1056aaef0
SHA1值: 8e7e5ef7d3fe8a2aa8d6b43bcd97e68c1ba3683e
SHA256值: 8786b1359ddc40ec2fc9bea5a192044bc8da9807aef6950b237e9e82189d4ad7

APP 信息

App名称: 职校家园
包名: com.wyl.exam
主活动Activity: com.wyl.exam.SplashActivity
安卓版本名称: v1.6.3
安卓版本: 79

域名线索

域名	服务器信息
login.hnzwfw.gov.cn	**IP**: 222.143.32.187 **所属国家**: China **地区**: Henan **城市**: Zhengzhou **纬度**: 34.757778 **经度**: 113.648613
xlrz.vae.ha.cn	**IP**: 211.67.168.65 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

URL线索

URL信息	Url所在文件
https://xlrz.vae.ha.cn/00/1002_m0.aspx	摸瓜V1引擎
https://login.hnzwfw.gov.cn/tacs-uc/login/index	摸瓜V1引擎

邮箱线索

手机线索

手机号	所在文件
16369591640	摸瓜V1引擎

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=henan, L=zhengzhou, O=anxinkeji, OU=cn, CN=anxinkeji
签名算法: rsassa_pkcs1v15
有效期自: 2019-04-25 08:28:41+00:00
有效期至: 2044-04-18 08:28:41+00:00
发行人: C=cn, ST=henan, L=zhengzhou, O=anxinkeji, OU=cn, CN=anxinkeji
序列号: 0x4cfb4b8b
哈希算法: sha256
md5值: 93199d556dea834af9d099382bc253fb
sha1值: b53163d235a87a338046d86e6284ab2edb590ee7
sha256值: 4f1b8b20eddcd351181a87a39eea9b331c1d9767d594db96307e1dfd95ca66fe

sha512值: 526d77e3bbc5a1ab83ca23ce962c4bafea14a081d6b898be1ff23b27927a3545bc3a3da0680c0be96cb29ff0533217f6e2eece23d57705f19ed434443b4b91e5
公钥算法: rsa
密钥长度: 2048
指纹: fc83809d6aff77d47d3cb0b2c31ed554ed26d5dae69524d95a1944c0dd1c9fcb

硬编码敏感信息

可能的敏感信息
"home_user" : "欢迎您：%s"
"wbcf_user_auth_protocol_name" : "《个人信息处理授权书》"

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.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.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_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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器

android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.wyl.exam.permission.haotian.RECEIVE	未知	Unknown permission	Unknown permission from android reference
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
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.KILL_BACKGROUND_PROCESSES	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.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.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.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.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.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置

应用内通信