MoGua

黄浦分院掌医 1.6.APK 分析报告

APP名称:	黄浦分院掌医

包名:	com.wonders.android.apps.jyhpyy.employeesmanager
域名线索:	0条
URL线索:	0条
邮箱线索:	0条
分析日期:	2025年6月19日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 1.apk
文件大小: 24.24MB
MD5值: 060bc6ad70a8f30e5474b7a48f62b6d3
SHA1值: 083a3430635ba8172d56d4aa5462a66cdf58b1ee
SHA256值: c68ed9519bd49c6ce800a25bc961f946b7051a2f82f2954a02e1ccbc29b4cc2b

APP 信息

App名称: 黄浦分院掌医
包名: com.wonders.android.apps.jyhpyy.employeesmanager
主活动Activity: com.employeesmanager.MainActivity
安卓版本名称: 1.6
安卓版本: 7

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=86, ST=shanghai, L=shanghai, O=fugao, OU=fugao, CN=fugao

签名算法: rsassa_pkcs1v15
有效期自: 2016-11-03 03:21:43+00:00
有效期至: 2041-10-28 03:21:43+00:00
发行人: C=86, ST=shanghai, L=shanghai, O=fugao, OU=fugao, CN=fugao
序列号: 0x5a16332c
哈希算法: sha256
md5值: 1b15b9cdc49d8994b52d285dd72c2c3b
sha1值: 336958eb1618f4949380e525035211c0c2a29e4a
sha256值: 746a832c6f16cd0eed7d9fabd586fdb5ecf74c8bdc2c4bc64f296e1552c1ba9b
sha512值: b5cadbfd60b8071a9cd8f800e5d7d1b2f026115437157172e7a9cf12d2010a6f75d1dc2ae6f297ea9ecbd4357882029151171cb8e3d5b6479ede052ad65c0722
公钥算法: rsa
密钥长度: 2048
指纹: 80efe4447016b422b06e3b17e9db1f61e8cec9d962f840813383de225a50eb0a

硬编码敏感信息

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.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
com.employeesmanager.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
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_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
com.wonders.android.apps.jyhpyy.employeesmanager.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.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_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.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.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_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.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.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.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_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
	正	更改网络连	

android.permission.CHANGE_NETWORK_STATE	常	接	允许应用程序更改网络连接状态。
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.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限

应用内通信
