Evaluation Warning: The document was created with Spire.Doc for Python.

**考务棒（ 0.0.1版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 考务棒 |
| 版本 | 0.0.1 |
| 包名 | com.zakww.A1933860496406478849 |
| 域名线索 | 14条 |
| URL线索 | 11条 |
| APP图标 |  |
| 分析日期 | 2024年12月30日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | 4.2.apk |
| 文件大小 | 86.98MB |
| MD5值 | 2699bb4e637e87c966d536c7e63eeadd |
| SHA1值 | 0945b2df36fa34e9e8b6b7f25c3dee43b4f3239e |
| SHA256值 | 19d754dae4628e99da456a2b1dd0eac7777c549047bdb56338cd55aca6fd66bc |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 考务棒 |
| 包名 | com.zakww.A1933860496406478849 |
| 主活动Activity | com.uzmap.pkg.LauncherUI |
| 安卓版本名称 | 0.0.1 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| xmlpull.org | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| www.ccil.org | IP: 172.217.163.51 所属国家: United States of America 地区: California 城市: Mountain View  |
| s.app3c.com | 没有服务器地理信息.  |
| schemas.openxps.org | IP: 134.0.30.204 所属国家: Germany 地区: Nordrhein-Westfalen 城市: Koeln  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| as.app3c.com | 没有服务器地理信息.  |
| schemas.android.com | 没有服务器地理信息.  |
| schemas.microsoft.com | IP: 13.107.213.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| ops.fun.mipm | 没有服务器地理信息.  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| xml.org | IP: 104.239.240.11 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| iuap-yonbuilder-mamservice.yyuap.com | IP: 59.110.247.93 所属国家: China 地区: Beijing 城市: Beijing  |
| p.app3c.cn | 没有服务器地理信息.  |
| d.app3c.cn | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android  | com/apicloud/third/gif/GifTextureView.java  |
| http://schemas.android.com/apk/res/android  | com/apicloud/third/gif/GifTextView.java  |
| http://schemas.android.com/apk/res/android  | com/apicloud/third/gif/GifViewUtils.java  |
| http://www.w3.org/TR/SVG11/feature  | com/deepe/c/c/a/a/n.java  |
| http://www.w3.org/1999/xlink  | com/deepe/c/c/a/a/n.java  |
| http://www.w3.org/2000/svg  | com/deepe/c/c/a/a/n.java  |
| http://xmlpull.org/v1/doc/features.html  | com/deepe/c/c/a/a/n.java  |
| http://xml.org/sax/features/external-general-entities  | com/deepe/c/c/a/a/n.java  |
| http://xml.org/sax/features/external-parameter-entities  | com/deepe/c/c/a/a/n.java  |
| http://xml.org/sax/properties/lexical-handler  | com/deepe/c/c/a/a/n.java  |
| http://www.ccil.org/  | com/deepe/c/i/p.java  |
| https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection  | com/deepe/c/l/a.java  |
| http://ops.fun.mipm/sync  | com/uzmap/pkg/openapi/SuperWebview.java  |
| http://ops.fun.mipm/sync  | com/uzmap/pkg/uzcore/f.java  |
| https://iuap-yonbuilder-mamservice.yyuap.com/iuap-yonbuilder-mobile/v2  | compile/Properties.java  |
| https://d.app3c.cn  | compile/Properties.java  |
| https://s.app3c.com  | compile/Properties.java  |
| https://p.app3c.cn  | compile/Properties.java  |
| https://as.app3c.com  | compile/Properties.java  |
| http://%s:%s/activev3/charge  | lib/armeabi/libarcsoft\_face\_engine.so  |
| http://schemas.microsoft.com/xps/2005/06/fixedrepresentation  | lib/armeabi/libmupdf\_java.so  |
| http://schemas.openxps.org/oxps/v1.0/fixedrepresentation  | lib/armeabi/libmupdf\_java.so  |
| http://schemas.microsoft.com/xps/2005/06/documentstructure  | lib/armeabi/libmupdf\_java.so  |
| http://schemas.openxps.org/oxps/v1.0/documentstructure  | lib/armeabi/libmupdf\_java.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| 123@app3c.com  | com/uzmap/pkg/uzmodules/uzxml/UzXml.java  |
| x@j.9υ\_1  | Mogua Engine V2  |
| r@uh.kx  | Mogua Engine V2  |
| ų@e.cg ﱧ@rdlm\_72ks6.yy  | Mogua Engine V2  |
| ftp@example.com  | lib/armeabi/libarcsoft\_face\_engine.so  |
| 6h@fo.lwft w9oi\_2nhels4u@dlilycclglhl.5jlcg\_bqh yay@y.u5vcghyy  | lib/armeabi/libiconv.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | com/deepe/c/c/a/a/j.java  |
| 17179869184  | com/deepe/c/c/a/a/o.java  |

## **5. 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=zh, ST=Beijing, L=Beijing, O=test, OU=test, CN=www.ctbri.com 签名算法: rsassa\_pkcs1v15 有效期自: 2024-02-19 08:47:06+00:00 有效期至: 2124-01-26 08:47:06+00:00 发行人: C=zh, ST=Beijing, L=Beijing, O=test, OU=test, CN=www.ctbri.com 序列号: 0x1824d7dd 哈希算法: sha1 md5值: 6f6e1a181919eac39d59a1d1d77de9c3 sha1值: ac02c116f88cdb5503346b4efd0233bb611a0eb7 sha256值: b0eaad2a0804ac3da4fbff6107385eddc439c75aa234b62c4eb37b28acdaec91 sha512值: 11fe43de1dfff8a973a48abe38285c702a8e96d1e3fc2663d54837e11bf749d72c827f765a205e949cef2b18b4803161b4bb629a45553196d9ac610274e4f115 公钥算法: rsa 密钥长度: 1024 指纹: 00d07f689127f06a90a0e33b15e1ccbf04f85b8e8a33c1a45cfa973bb14dc4dc**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "enter\_password" : "Enter Password"  |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| 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.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.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.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| android.permission.SEND\_SMS | 危险 | 发送短信 | 允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价 |
| 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.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.WRITE\_CONTACTS | 危险 | 写入联系人数据 | 允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.READ\_SMS | 危险 | 阅读短信或彩信 | 允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息 |
| android.permission.ACCESS\_MOCK\_LOCATION | 危险 | 用于测试的模拟位置源 | 创建模拟位置源进行测试。恶意应用程序可以使用它来覆盖由真实位置源（如 GPS 或网络提供商）返回的位置和/或状态 |
| 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.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.READ\_CALENDAR | 危险 | 读取日历事件 | 允许应用程序读取您手机上存储的所有日历事件。恶意应用程序可以借此将您的日历事件发送给其他人 |
| android.permission.WRITE\_CALENDAR | 危险 | 添加或修改日历事件并向客人发送电子邮件 | 允许应用程序添加或更改日历上的事件,这可能会向客人发送电子邮件。恶意应用程序可以使用它来删除或修改您的日历活动或向客人发送电子邮件 |
| android.permission.BODY\_SENSORS | 危险 |  | 允许应用程序访问来自传感器的数据,用户使用这些数据来测量他/她体内发生的事情,例如心率 |
| android.permission.RECEIVE\_SMS | 危险 | 接收短信 | 允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示 |
| android.permission.BLUETOOTH\_SCAN | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH\_ADVERTISE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH\_CONNECT | 未知 | Unknown permission | Unknown permission from android reference |
| 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.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| 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.SET\_WALLPAPER | 正常 | 设置壁纸 | 允许应用程序设置系统壁纸 |
| 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.artifex.mupdf.MuPDFActivity | **Schemes**: file://, **Hosts:** \*, **Mime Types:** \*/\*, **Path Patterns:** .\*\\.xps, .\*\\.pdf, .\*\\.cbz,  |

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**