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

**手心输入法（ 3.6.1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 | 手心输入法 |
| 版本 | 3.6.1 |
| 包名 | com.xinshuru.inputmethod |
| 域名线索 | 0条 |
| URL线索 | 0条 |
| APP图标 |  |
| 分析日期 | 2025年9月8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 | Ftinput-13514-o\_1hgde8b4k3ba1h7813s21l7l197n13-uid-479539.apk |
| 文件大小 | 39.31MB |
| MD5值 | 628333cccc4651c8c0689e108c6b01ce |
| SHA1值 | 380878dc103f7ba86698515cd2c6f68a4cc51486 |
| SHA256值 | f74a5b384f703321a8638c331daed9baa8f74cd3efdb73a5f1e754d8ded5ff87 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 手心输入法 |
| 包名 | com.xinshuru.inputmethod |
| 主活动Activity | com.xinshuru.inputmethod.FTInputSplashActivity |
| 安卓版本名称 | 3.6.1 |
| 安卓版本 | 1019 |

## **4. 线索情况**

### **4.1 域名线索**

### **4.2 URL线索**

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=86, ST=beijing, L=beijing, O=palminput, OU=xinshuru.com, CN=Unknown 签名算法: rsassa\_pkcs1v15 有效期自: 2014-10-13 04:00:29+00:00 有效期至: 2069-07-16 04:00:29+00:00 发行人: C=86, ST=beijing, L=beijing, O=palminput, OU=xinshuru.com, CN=Unknown 序列号: 0x179bc806 哈希算法: sha256 md5值: 244a3265f6ea018cc91477fe2969d40b sha1值: 4dc88475596878b01e49ea450feca77a8e357234 sha256值: f893213b99275c4f72da18a435ac6b4f2971bd253c43193e956c3343fba5bbf6 sha512值: 44de3b9187e9507ee31cdb99412c9529824b83e03115124d19405ced9346027cd7ab9c9280555d03f4144478cb8e44ef6e3c09120c7e4715d1ca81d68c2b189c 公钥算法: rsa 密钥长度: 2048 指纹: ee881aa6244d60e385b69148ab372f8719c9c29549e5f79538a5e93dd7baf3fb**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "qihoo\_accounts\_auth\_360" : "360账号登录"  |
| "qihoo\_accounts\_auth\_alipay" : "支付宝"  |
| "qihoo\_accounts\_auth\_loading" : "正在加载…"  |
| "qihoo\_accounts\_auth\_phone" : "短信登录"  |
| "qihoo\_accounts\_auth\_phone\_pwd" : "手机密码登录"  |
| "qihoo\_accounts\_auth\_qq" : "QQ"  |
| "qihoo\_accounts\_auth\_sina" : "微博"  |
| "qihoo\_accounts\_auth\_wechat" : "微信"  |
| "qihoo\_accounts\_chang\_pwd" : "立即修改"  |
| "qihoo\_accounts\_findpwd\_by\_mobile" : "通过手机号找回 >"  |
| "qihoo\_accounts\_findpwd\_by\_mobile\_reset" : "找回密码"  |
| "qihoo\_accounts\_findpwd\_by\_other" : "通过邮箱找回 >"  |
| "qihoo\_accounts\_findpwd\_sub\_mobile" : "请输入您要找回密码的手机号"  |
| "qihoo\_accounts\_findpwd\_sub\_other" : "请输入您要找回密码的邮箱"  |
| "qihoo\_accounts\_findpwd\_valid\_phone" : "账号或密码错误"  |
| "qihoo\_accounts\_leak\_pwd" : "系统检测到您账号存在安全风险，请先修改密码"  |
| "qihoo\_accounts\_leak\_pwd\_limit" : "系统检测到您账号存在安全风险，请先修改密码"  |
| "qihoo\_accounts\_login\_forget\_password" : "找回密码"  |
| "qihoo\_accounts\_modify\_pwd\_by\_other" : "其他方式修改"  |
| "qihoo\_accounts\_modify\_pwd\_enter\_tv\_content" : "请选择你注册用的账号类型是"  |
| "qihoo\_accounts\_modify\_pwd\_title" : "修改密码"  |
| "qihoo\_accounts\_modify\_pwd\_tv\_content" : "您正在修改当前账号的密码，请先进行身份验证"  |
| "qihoo\_accounts\_plant\_auth\_cancel" : "您已取消授权，请重新登录"  |
| "qihoo\_accounts\_quick\_login\_email\_pwd" : "邮箱登录"  |
| "qihoo\_accounts\_quick\_login\_phone\_pwd" : "手机登录"  |
| "qihoo\_accounts\_reset\_pwd" : "重置密码"  |
| "qihoo\_accounts\_tips\_last\_login\_Phone\_Pwd" : "您上次使用手机号登录"  |
| "qihoo\_accounts\_weak\_pwd" : "系统检测到您账号安全等级较低，建议立即修改密码"  |
| "qihoo\_accounts\_webview\_chpwd" : "修改密码"  |
| "qihoo\_accounts\_webview\_findpwd" : "找回密码"  |

## **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.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\_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.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.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.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.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.MANAGE\_DOCUMENTS | 合法 |  | 允许应用程序管理对文档的访问,通常作为文档选择器的一部分 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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。 |
| com.xinshuru.inputmethod.permission.NEWS\_SDK\_BROADCAST | 未知 | Unknown permission | Unknown permission from android reference |
| com.xinshuru.inputmethod.V5\_SDK\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.xinshuru.inputmethod.V5\_SDK\_BROAD\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.xinshuru.inputmethod.V5\_SDK\_PROX\_BROAD\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.xinshuru.inputmethod.permission.PROCESS\_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.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| 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。 |
| xmpp.permission.ACCESS\_API | 未知 | Unknown permission | Unknown permission from android reference |
| xmpp.permission.RECEIVE\_NOTIFICATION | 未知 | Unknown permission | Unknown permission from android reference |
| com.xinshuru.inputmethod.permission.GOLD\_BROADCAST | 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.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| 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 |
| com.xinshuru.inputmethod.permission.LDSDK\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.xinshuru.inputmethod.FTInputSettingsActivity | **Schemes**: file://, http://, content://, **Hosts:** \*, **Mime Types:** \*/\*, **Path Patterns:** .\*.piska,  |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent1109910694://,  |
| com.xinshuru.inputmethod.DeepLinkActivity | **Schemes**: xinshuru://,  |

**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。**