青莲云
qinglianyun.com

# 青莲云

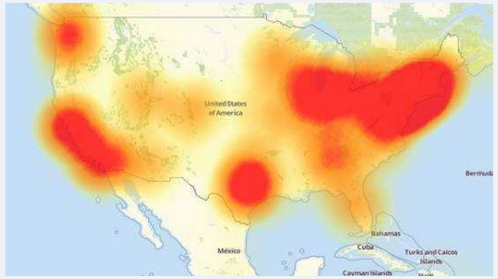
# 物联网固件安全检测平台产品介绍（TinyScan）

# 近年来物联网安全事件

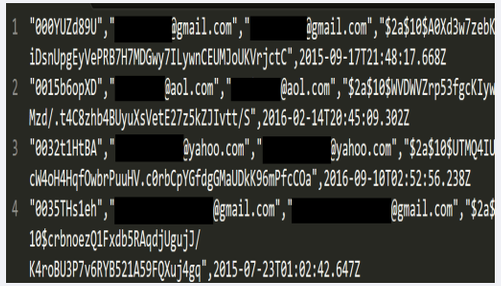
近年来，国内外发生了多起物联网信息安全事故，涉及设备、云端、APP等各类安全漏洞的利用

2008年
波兰罗兹市电车被黑客通过物联网设备入侵并发生脱轨事故

2015年
黑客通过SkyJack技术入侵无人机系统并通过智能手机组建“僵尸机队”




2016年
美国东海岸断网，主要为物联网僵尸网络发起的DDOS攻击




2017年
智利知名智能玩具Spiral Toys的云端服务泄露200万个人信息


2017年
恶意软件BrickerBot造成数百万物联网设备永久失效


2018年
台积电工业安全事件

# 智慧城市系统安全准入机制缺乏

**智慧城市包含多种应用场景，设备及系统安全建设情况参差不齐**

**智慧社区**

**智慧水务**

**智慧停车**

**智能充电桩**

**智慧工业**

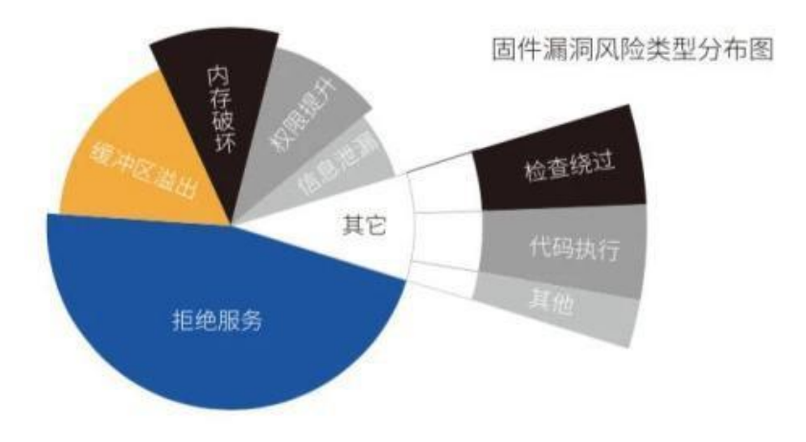

**智慧门禁**

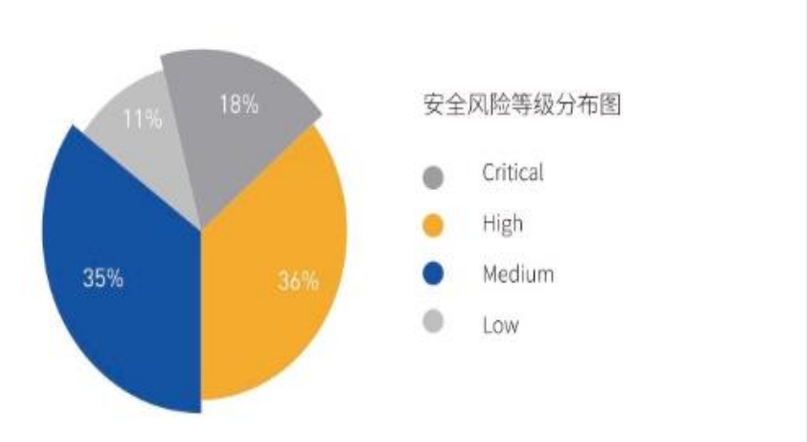
**智慧城市设备例举：**

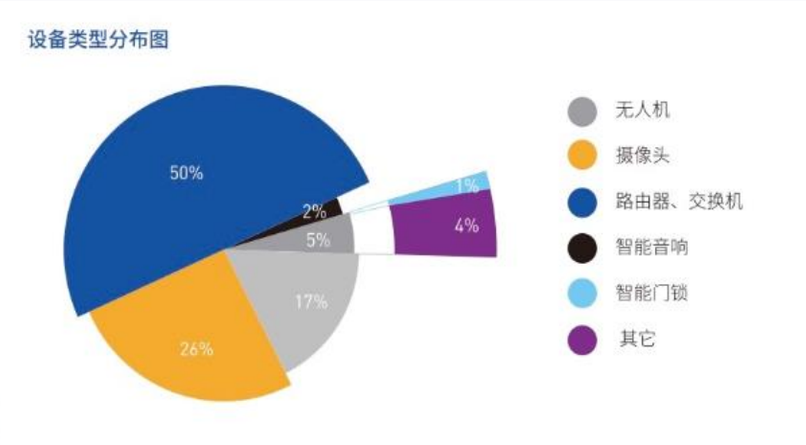
| | | |
|---|---|---|
| 警戒摄像机 | 水位监测仪 | 环保数采仪 |
| 智慧门禁 | 物联网网关 | DTU |
| 电梯卫士 | 消防监控主机 | 边缘网关 |
| 数字管理机 | 液位计 | LORA网关 |
| 智能消防 | 道口边缘网关 | 4G网关 |
| 4G路由器 | 智能公交站主机 | 车载终端 |
| 监控摄像机 | 数据遥传设备 | 信号控制器 |
| 消防控制主机 | 监控摄像机 | 数据采集仪 |
| 人脸抓拍 | 智慧路灯控制仪 | 摄像机 |
| 温湿度传感器 | 烟感报警器 | …… |

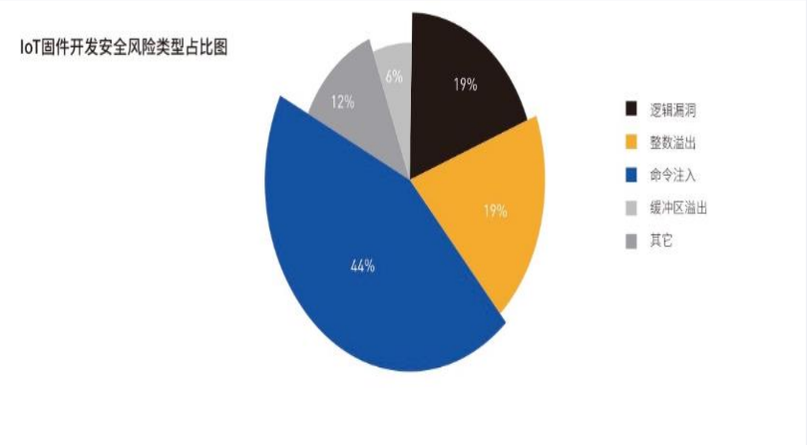
# 物联网设备端安全漏洞

## 目前市场上平均一款的IoT设备包含33.96个安全漏洞




数据来源：腾讯IoT安全白皮书

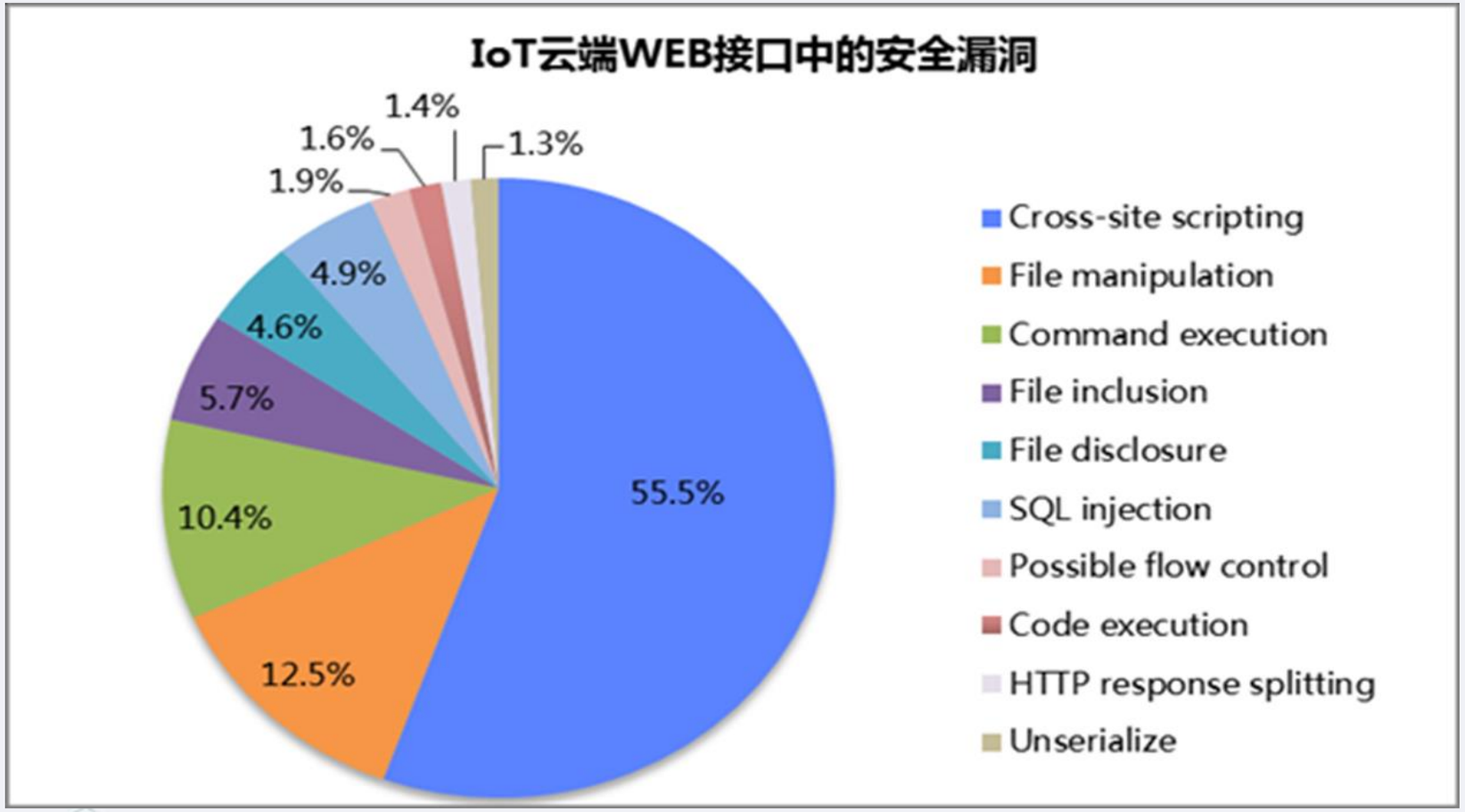
## 物联网设备常见的安全漏洞

- 非必要网络连接
- 开放的调试接口
- 弱密码
- 系统漏洞
- 硬编码口令
- 不安全的第三方库
- 明文传输
- 不安全的OTA机制

## 造成的危害

- IOT僵尸网络
- 设备失效/变砖
- 向平台发起攻击
- 工业停产
- 隐私数据泄露

# 物联网云平台安全漏洞




数据来源自互联网

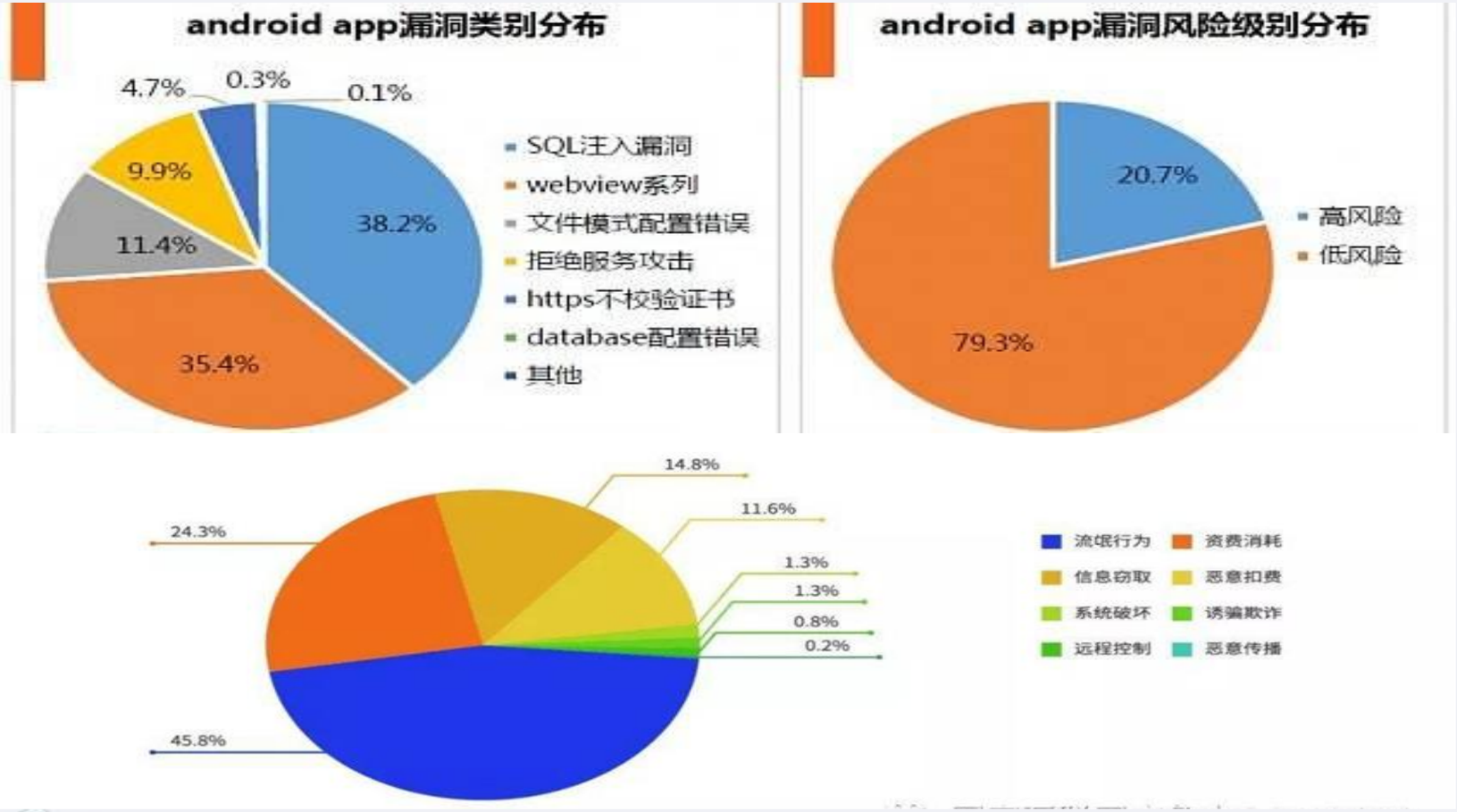
## 物联网云平台常见的安全漏洞

- 身份认证漏洞；
- 不合理的权限设置；
- API（应用程序编程接口）漏洞；
- 不安全的第三方库/服务；
- 不安全的数据机制；
- DDoS攻击威胁；
- 服务滥用；
- Web攻击；

## 造成的危害

- 隐私数据泄露
- 平台无法提供正常服务
- 勒索与敲诈
- 数据完全丢失，业务停摆
- 页面被篡改
- 企业信誉受损

# 物联网APP端（安卓）安全漏洞




数据来源自互联网

## 物联网安卓APP常见的安全漏洞

- 不安全的设置
- 硬编码
- 不安全的第三方库组件
- 未进行反编译保护
- 身份认证漏洞
- 数据溢出
- 敏感数据泄露
- 不合理的权限设置

## 造成的危害

- APP二次打包
- 敏感数据泄露
- IOT设备非法控制
- 企业信誉受损
- 金融刑事案件

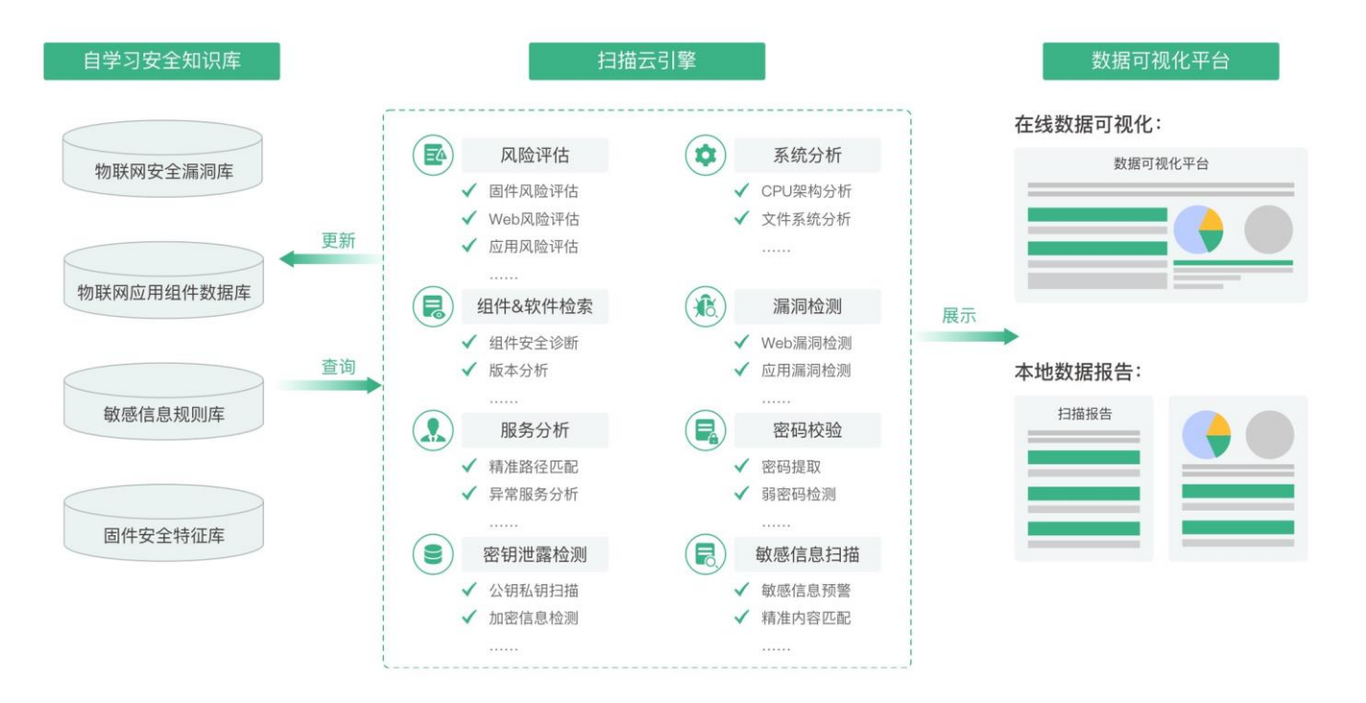
# 青莲云物联网固件安全检测平台介绍

**平台地址：tinyscan.qinglianyun.com**

**1个小时深度分析，出具专业检测报告，全面发现设备固件、APP的安全漏洞**

**助力企业建立专属安全测试流程**

# 青莲云物联网固件安全检测平台介绍




**平台地址：**https://tinyscan.qinglianyun.com

**平台简介：**提供覆盖设备固件、客户端APP的远程自动化安全检测服务，并出具可下载、可复测的 企业专属安全检测报告，帮助企业建立属于自己的安全测试流程， 定期监测产品安全漏洞。平台内含数百种检测项目，如：

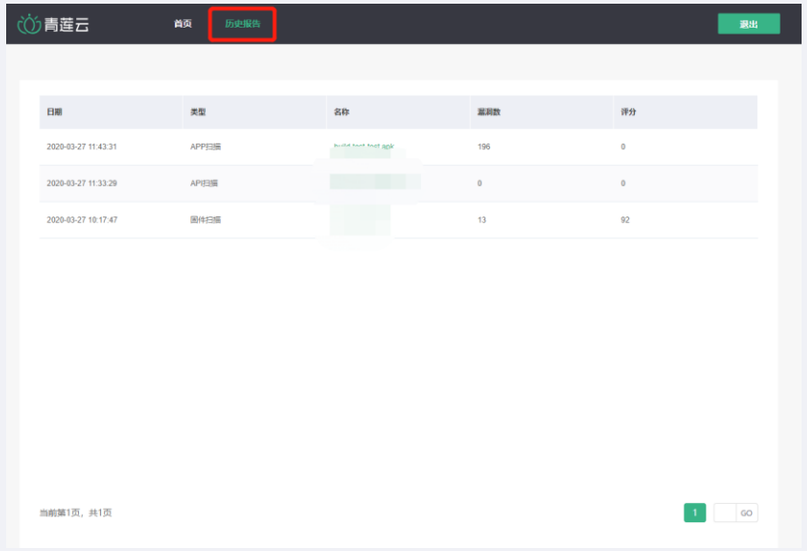
- **设备固件检测：**软件漏洞检测、组件漏洞检测、CVE漏洞识别、敏 感信息检测、硬编码检测、加密安全检测、认证安全检测、系统服 务检测、远程溢出漏洞检测、用户密码检测等等。

- **客户端APP检测：**组件安全检测、任意调试检测、任意备份检测、 加密检测、文件读写检测、系统漏洞检测、认证安全检测、端口安 全检测、恶意代码执行检测等等。

# 简单三步使用青莲云物联网固件安全检测平台


第一步：登录平台选择要检测的项目， 点击“立即检测”按钮


第二步：上传需要检测固件、APP文件，检测 过程一般在20~40分钟左右




第三步：等待云端检测完毕，检测结 果可在页面顶部历史报告处查看，支 持PDF报告下载

# 物联网固件安全检测平台（TinyScan）

## 固件检测——类linux系统固件

| | |
|---|---|
| 类型支持 | CPU架构支持：Alpha, ARM, Intel x86, IA64, MIPS, MIPS 64 bit, PowerPC, IBM S390, SuperH,Sparc, Sparc 64 bit, M68K, Nios-32, MicroBlaze, Nios-II, Blackfin, AVR,STMicroelectronics, ST200 |
| | 操作系统支持：OpenBSD, NetBSD, FreeBSD, 4.4BSD, Linux, SVR4, Esix, Solaris, Irix, SCO, Dell,NCR, LynxOS, VxWorks, pSOS, QNX, Firmware,RTEMS, ARTOS, Unity OS |
| CVE漏洞检测 | 自动检测、获取固件中包含的CVE（Common Vulnerabilities and Exposures，公共暴露和漏洞）信息，包括CVE-ID、发布时间、风险描述、漏洞等级，有助于规避因已知漏洞导致的安全性问题。 |
| 软件&组件检测 | 自动检测、获取固件中的组件&软件信息，包括软件路径、软件描述、官方网址。 |
| 加密认证文件检测 | 自动检测、获取加密认证文件信息，包括加密认证文件路径、加密信息、加密认证文件类型（公钥、私钥、证书等），有助于规避私钥泄露导致的安全性问题。 |
| 用户密码检测 | 自动检测、获取用户密码信息，包括密码相关文件路径、密码信息；自动判断密码安全等级，有助于规避因弱口令导致的系统安全性问题。 |
| 系统服务检测 | 自动检测、获取系统服务信息，包括系统服务路径和MD5值，有助于规避因篡改系统服务导致的安全性问题。 |
| CWE漏洞检测 | 支持ARM、Intel x86、MIPS、PowerPC架构，可自动检测可执行文件的整数溢出漏洞、安全缓解机制风险、调试信息泄露风险、chroot Jail错误设置漏洞、未捕获异常风险、伪随机数使用漏洞、条件竞争漏洞、不受信任的搜索路径风险、使用未 初始化变量风险、sizeof()使用不当漏洞、空指针错误引用漏洞、不安全函数调用风险、IOCTL调用无权限控制风险、umask()参数不正确风险 |
| 敏感信息检测 | 硬编码IP地址检测、硬编码Token/Key检测、配置型硬编码密码检测、硬编码URL检测、缓存文件检测 |

# 物联网固件安全检测平台（TinyScan）

## 固件检测——无系统或小微型系统固件

| | |
|---|---|
| 类型支持 | CPU架构支持：6502、68HC08、68HC11、8051、Alpha、ARcompact、ARM64、ARMeb、ARMel、ARMhf、AVR、AxisCris、Blackfin、Cell-SPU、CLIPPER、CompactRISC、Cray、CUDA、Epiphany、FR-V 、FR30、FT32、H8-300、H8S、HP-Focus、HP-PA、i860、IA-64、IQ2000、M32C、M32R、M68k、M88k 、MCore、Mico32、MicroBlaze、MIPS16、MIPSeb、MIPSel、MMIX、MN10300、Moxie、MSP430、NDS32、NIOS-II、OCaml、PDP-11、PIC10、PIC16、PIC18、PIC24、PPCeb、PPCel、RISC-V、RL78、ROMP、RX、S-390、SPARC、STM8、Stormy16、SuperH、TILEPro、TLCS-90、TMS320C2x、TMS320C6x、TriMedia、V850、VAX、Visium、WASM、WE32000、X86-64、X86、Xtensa、Z80、78k、TriCore |
| 固件指纹信息提取 | 自动获取固件基本信息，包括固件上传时间、固件名、固件大小、固件SHA256值、CPU架构、存储模式。 |
| 敏感信息检测 | 硬编码IP地址检测、硬编码Token/Key检测、配置型硬编码密码检测、硬编码URL检测、缓存文件检测；自动检测、获取固件中存在的敏感信息，包括敏感文件路径、敏感信息所在行、敏感信息类型、风险等级，有助于规避密码泄露、URL泄露等安全性问题。 |

# 物联网固件安全检测平台（TinyScan）

## APP应用检测

| | | |
|---|---|---|
| APP检测 | APK信息提取 | |
| | APP攻击demo下载 | |
| | 证书指纹 | |
| | 应用组件暴露 | Receiver组件暴露、Provider组件暴露、Service组件暴露、Activity组件暴露、Provider文件目录遍历、Intent Scheme URLs攻击 |
| | 文件信息检测 | 全局文件可读、全局文件可写、全局文件可读可写、配置文件可读、配置文件可写、配置文件可读可写、DEX文件动态加载、unzip解压缩 |
| | AndroidManifest文件检测 | 程序可被任意调试、程序数据任意备份、隐式意图调用、activity绑定browserable与自定义协议 |
| | Web组件安全 | Webview存在本地Java接口、WebView忽略SSL证书错误、webview明文存储密码、Webview组件远程代码执行（调用getClassLoader）、SSL通信服务端检测信任任意证书、SSL通信客户端检测信任任意证书 |
| | 网络通信安全 | 开放socket端口、HTTPS关闭主机名验证 |
| | 弱密码风险 | AES弱加密、AES/DES硬编码密钥、随机数不安全使用 |
| | 系统漏洞 | 动态注册广播、Fragment注入 |
| | So文件漏洞风险 | 未使用编译器堆栈保护技术、libupnp栈溢出漏洞、动态链接库中包含执行命令函数、未使用地址空间随机化技术、FFmpeg文件读取 |
| | 隐私权限检测 | 日历权限、相机权限、联系方式权限、位置权限、麦克风权限、电话权限、感应器权限、短信权限、存储权限 |
| | 隐私行为检测 | 获取系统信息、获取文件信息、手机卡相关信息、位置相关信息、设备相关信息 |

# 自动生成专业的安全检测结果（支持PDF报告下载）


设备固件安全检测结果展示


APP安全检测结果展示

# 青莲云物联网固件安全检测平台优势

**青莲云物联网固件安全检测平台与传统安全监测系统相比：产品定位不同，解决的安全问题不同，二者是完全互补的**

| 产品能力 | 青莲云TinyScan | 传统安全监测系统 |
| --- | --- | --- |
| 产品定位 | 漏洞检测类 | 态势感知类 |
| 产品形态 | SaaS服务 | 硬件设备 |
| 核心能力 | 自动化漏洞挖掘 | 网络流量安全分析 |
| 应用场景 | 系统研发环节 | 系统运营环节 |
| 监测对象 | 物联网设备/云/APP | 企业内/外网络流量 |
| 持续性监测 | 支持 | 支持 |
| 解决安全痛点 | 代码安全 | 流量安全 |
| 产品API | 支持 | 支持 |
| 部署方式 | 公有云服务 | 本地化部署 |
| IoT场景支持 | 优 | 一般 |
| IoT专家服务 | 支持 | 无 |

**产品优势（国内唯一的IoT端到端安全检测产品）**

- 动/静态双检测引擎
- 设备固件检测
- APK文件检测
- 云平台/API检测
- 数百种检测策略
- 自动更新的物联网安全漏洞库
- 标准的企业API支持
- 关联分析风险评估
- 云端扫描集群极速扫描
- 本地报告永久保存
- 详细的漏洞修复建议

# 通过企业API实现定期自动化安全监测

青莲云物联网固件安全检测平台提供标准的企业API，**企业客户可以通过API实现定期自动化安全监测**，也可以通过API将
TinySCan的自动化漏洞挖掘能力集成在企业内部的安全管理平台或运维平台中



TinySCan API 使用说明文档

版本记录：

| 版本 | 编写/修订说明 | 修订人 | 修订日期 | 备注 |
|---|---|---|---|---|
| 1.0.0 | 创建文档 | 吕帅江 | 20200220 | |
| 1.0.1 | 增加 web、APP | 吕帅江 | 20200305 | |
| 1.0.2 | 增加字段详细说明 | 吕帅江 | 20200325 | |
| | | | | |
| | | | | |



## 目录



### 2.1 固件任务创建

本 API 用来创建一个固件扫描任务，需要指定上传固件的路径、固件的 MD5 值和 token。任务创建成功，会返回一个 json 对象，其中包含状态码和任务 id。状态码正确的情况下，任务 id 才有效。任务 id 用于后续的结果查询，请自行保存好。

调用时一定要正确设置 Content-Type 值为 multipart/form-data，以表单的形式上传文件和相关参数。详细说明如下：

url: /v1/firmware/create

Content-Type: multipart/form-data

method: POST

**Form 格式请求参数：**

| 参数名 | 类型 | 说明 | 备注 | 必需 |
|---|---|---|---|---|
| firmware | string | 固件文件 | 指定文件的全路径或相对路径 | 是 |
| md5 | stirng | 固件的 md5 | 用于服务器对固件校验 | 否 |
| token | string | 用户口令 | 授权获取到的口令码 | 是 |

**命令行示例：**

```
curl "https://tinyscan-api.qinglianyun.com:8080/v1/firmware/create" -F "firmware=@hello.bin" -F "md5=6e44d44494446df0fff098f0a2da3418" -F "token=xxxxxx "
```

**响应参数：**

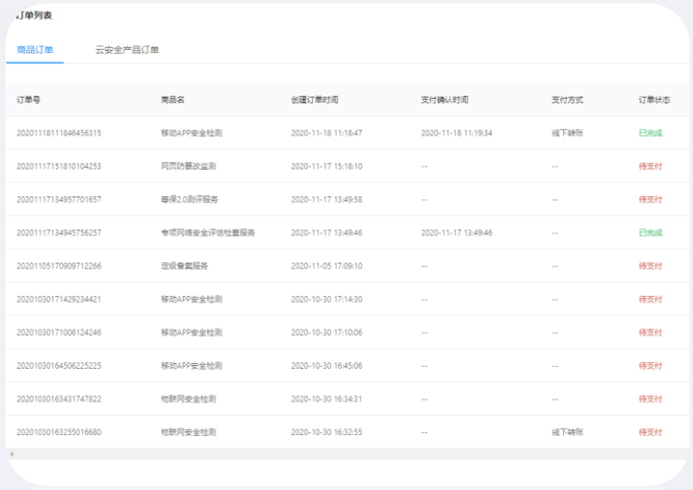
| 参数名 | 类型 | 说明 | 备注 | 必需 |
|---|---|---|---|---|
| code | string | API 调用执行的状态 | 状态码 | 是 |
| taskid | string | 唯一任务 id | 作为任务查的标识，请妥善自行保管。 | 是 |

青莲云
qinglianyun.com

# 平台运营

# 浙江省工业互联网网络安全公共服务平台





## ◆项目简介

浙江省工业互联网网络安全公共服务平台：iinssp.com

**客户介绍：**

浙江鹏信信息科技股份有限公司，是一家致力于移动互联网业务发展的高新科技企业，公司业务涉及移动互联网安全、综合解决方案、移动互联网业务运营等多个领域。

**项目概况：**

负责工业互联网网络安全公共服务平台中有关物联网安全检测部分的建设，实现工业互联网系统中设备固件安全检测、云平台 API 安全检测、APP 安全检测，通过对外提供物联网安全检测服务实现企业创收。

# 浙江省工业互联网网络安全公共服务平台

**青莲云IoT安全监测平台支持私有化部署，浙江省工业互联网网络安全公共服务平台通过SaaS服务形式对外提供检测服务，实现项目创收。**

| | | | | | | |
|---|---|---|---|---|---|---|
| **平台运营** | 用户注册 | 订单咨询 | 服务购买 | 检测服务 | 报告下载 | 安全咨询 |
| | **浙江省工业互联网网络安全公共服务平台** | | | | | |
| **检测能力** | **固件检测** | | **APP检测** | | **云平台/API检测** | |
| | CVE漏洞检测 | CWE漏洞检测 | APK信息提取 | 文件信息监测 | 定时检测任务 | 系统信息检测 |
| | 敏感信息检测 | 软件组件检测 | 应用组件暴露 | Web组建安全 | SQL注入漏洞 | 目录遍历漏洞 |
| | 指纹信息提取 | 脆弱代码检测 | 系统漏洞检测 | 隐私权限检测 | DNS漏洞检测 | XSS漏洞检测 |
| **技术支撑** | 漏洞扫描引擎 | 信息抽取引擎 | 漏洞分析引擎 | Web发布组件 | 对外服务API | |
| **IaaS层** | **支持多种私有化部署方式** | | | | | |
| | 企业自由IDC | 软硬一体化交付 | 阿里云 | Amazon AWSA | Microsoft zure | |

# 浙江省工业互联网网络安全公共服务平台




## ◆平台运营

**运营模式：**

浙江省工业互联网网络安全公共服务平台通过物SaaS 服务的形式对外提供物联网安全检测服务。平台用户可通过平台直接购买固件检测、云平台/API、APP检测次数，并获得检测结果。

**收费标准：**

浙江省工业互联网网络安全公共服务平台按检测次数分别对三种不同检测服务进行收费，价格如下：

固件检测：2000元/次

云平台/API：2000元/次

APP：3500元/次

# 让安全成为物联网应用的基础设施