硬编码检测工具使用指南

**—— 安全团队**

目录

[1.1 2](#_Toc9429063)

[1.1.1 工具介绍 2](#_Toc9429065)

[1.1.2 工具特点 2](#_Toc9429066)

[1.1.3 工具使用 2](#_Toc9429065)

## detect-secrets

### 工具介绍

detect-secrets硬编码检测工具是美国的「大众点评」公司 Yelp 正式开源其密码检测框架，该框架用于防止代码中的密码等相关敏感信息被提交到代码库中，它可以在保证安全性的同时不会给开发者的生产力带来任何影响。

Yelp 的扫描使用了正则规则，可以检测出如下几种密码：

API 秘钥

AWS 秘钥

OAuth 客户端秘钥

SSH 私钥

其他高熵数字符串（比如使用 Shannon Entropy 计算的字符串）等

### 工具特点

1. 可定制化规则

可根据业务需要制作规则比如白名单的方式。

1. 编程语言无关性

可支持不同的语言比如Python，PHP，Java，JavaScript等，无需编译即可扫描。

### 工具使用

github地址: <https://github.com/Yelp/detect-secrets>

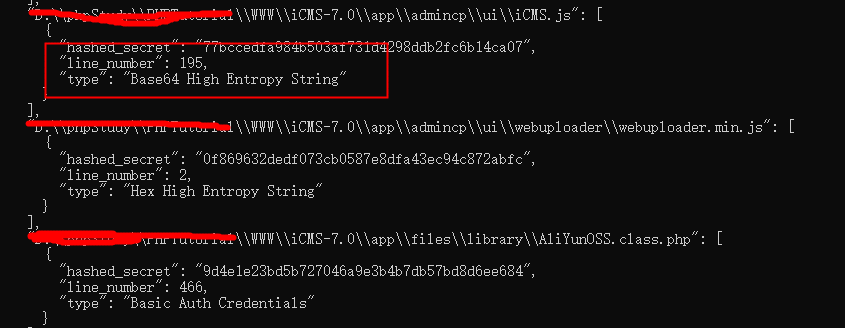
支持WINDOWS,LINUX等平台使用；

首先进行下载之后进入detect-secrets目录，执行命令为；

detect-secrets scan --all-files 项目路径

我们可以自定义要使用的plugins插件进行扫描；

扫描结果如下；



可以扫描到哪个文件下的第几行存在硬编码。