php源代码安全审计使用说明

**—— 安全团队**

目录

[1.1 RIPS 2](#_Toc9429063)

[1.1.1 工具介绍 2](#_Toc9429065)

[1.1.2 工具安装及使用 2](#_Toc9429066)

## RIPS

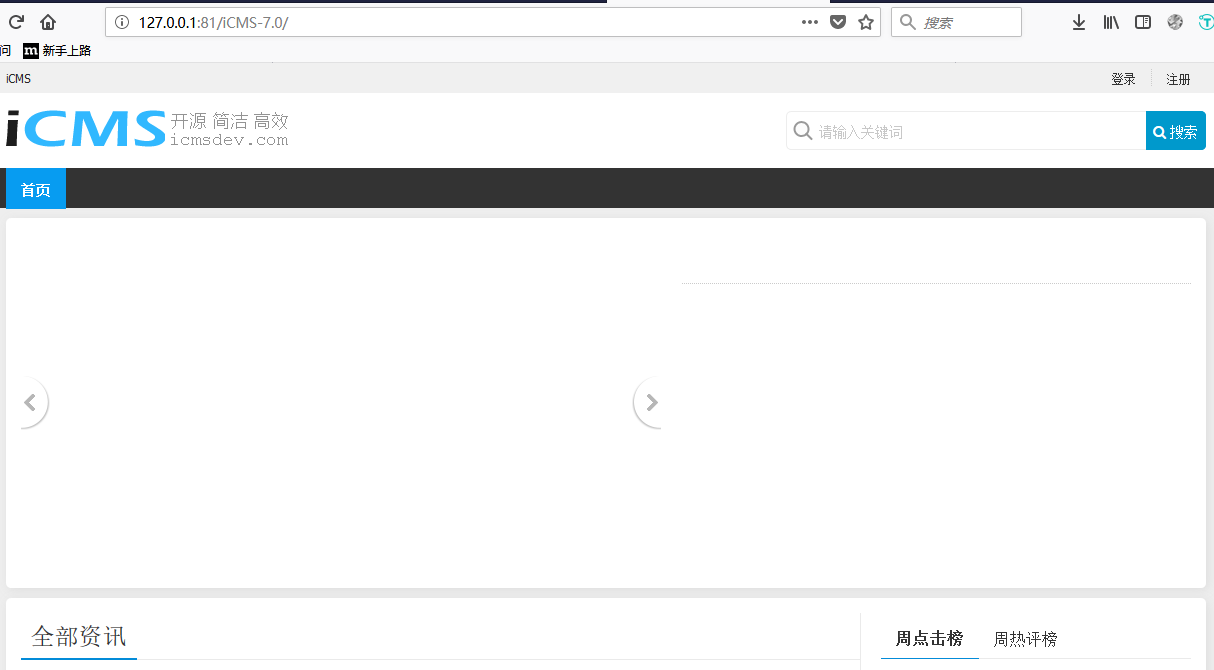
### 工具介绍

RIPS是一个用 PHP 编写的源代码分析工具，它使用了静态分析技术，能够自动化地挖掘 PHP 源代码潜在的安全漏洞。渗透测试人员可以直接容易的审阅分析结果，而不用审阅整个程序代码。由于静态源代码分析的限制，漏洞是否真正存在，仍然需要代码审阅者确认。RIPS 能够检测 XSS, SQL 注入, 文件泄露, Header Injection 漏洞等。

### 工具安装及使用

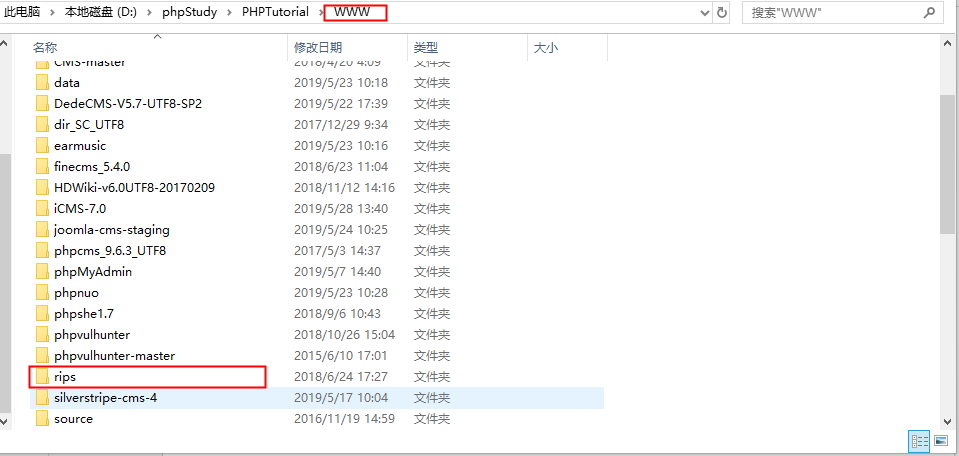
首先需要安装php集成环境比如phpstudy之后需要把项目安装到目录里跑起来，之后才可以进行扫描，以某cms举例；

安装完成cms页面如下；

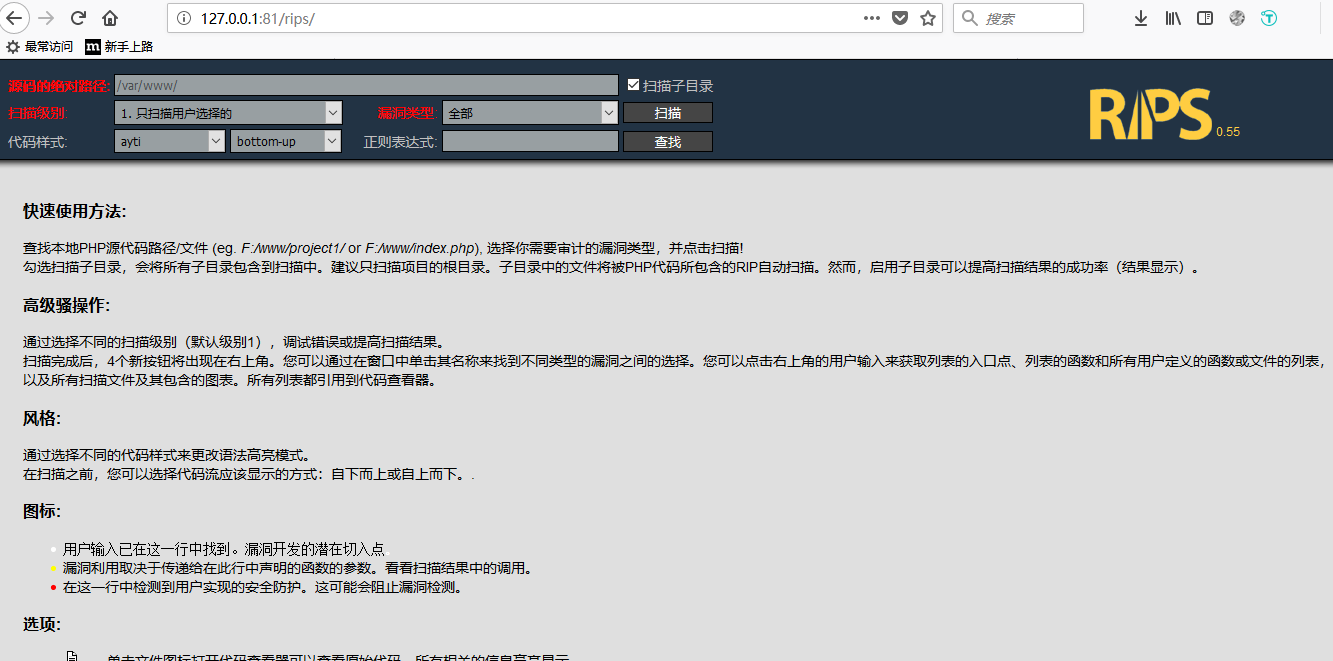


之后我们安装RIPS，下载地址如为<http://rips-scanner.sourceforge.net/>

之后同样安装到WWW目录里（就是我们cms安装的目录）；



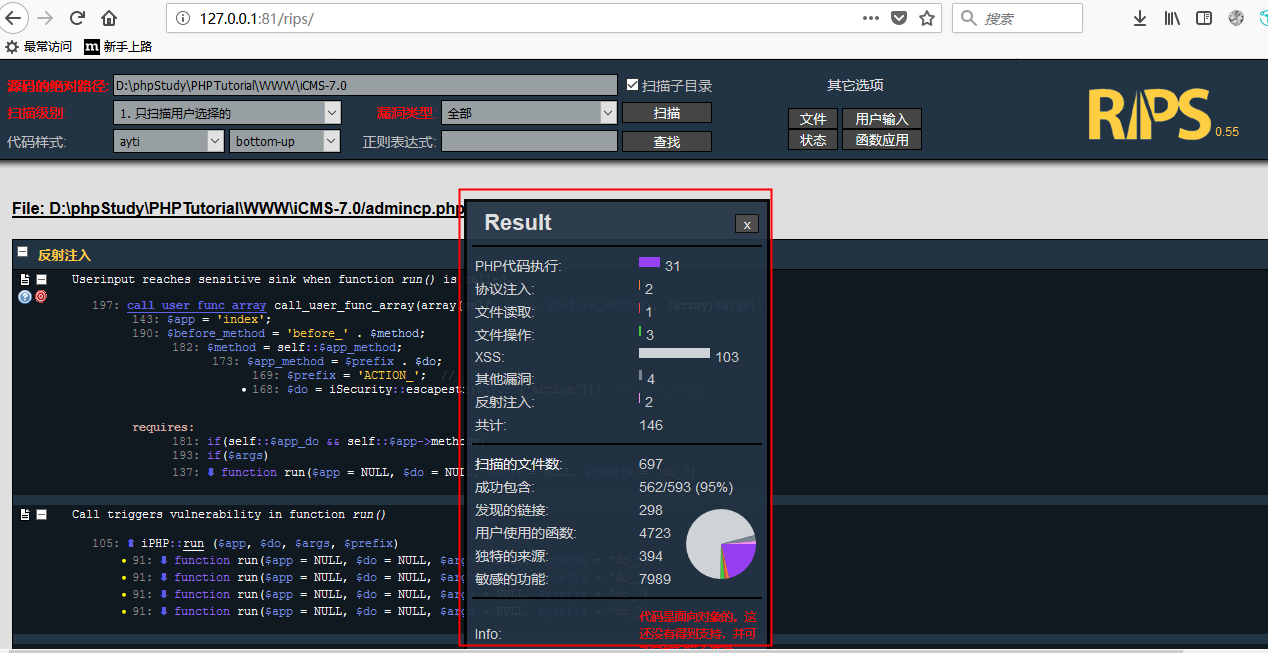
之后访问；



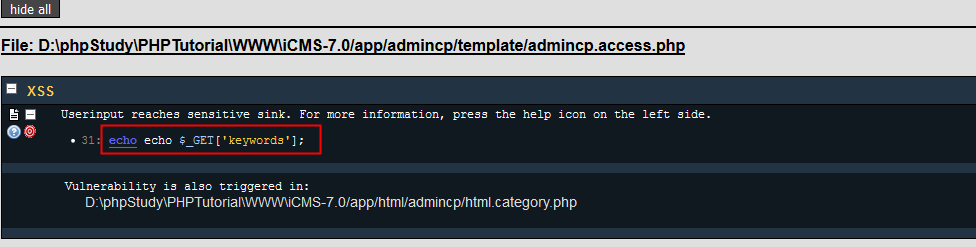
我这里使用的是汉化版，可以自行下载语言包；

之后只需要把cms安装目录放上去扫描就可以了

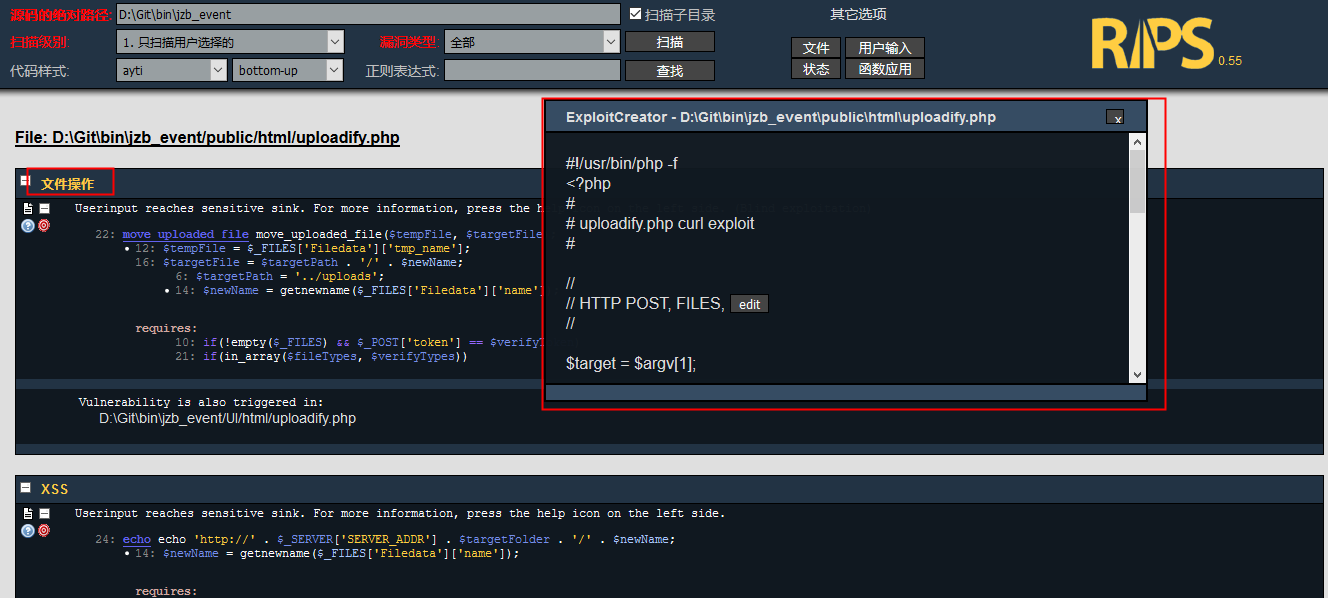
扫描完成页面如下；



可以看到自动导出报告，包括漏洞类型，来源等；



除了报告之外，还可以自动生成相关漏洞利用代码，比如；



文件操作相关的漏洞利用代码，我们可以去参考进行分析。