**测试流程**

**2019.7**

**目标站点简介**

DVWA（Damn Vulnerable Web Application）是一个用来进行安全脆弱性鉴定的PHP/MySQL Web应用，旨在为安全专业人员测试自己的专业技能和工具提供合法的环境，帮助web开发者更好的理解web应用安全防范的过程。

我们本次的测试，会利用这个平台作为一个检验标准。测试环境已经调试完成，搭建在云服务器上。

测试链接:<http://120.79.174.75/DVWA-master/>

**本次测试内容**

扫描Web安全测试平台(Dvwa)的高阶SQL漏洞，以及软件扩展性展示。

我们会寻找一款同类软件进行对比，对比内容主要包括如下三点。

1. 扫描速度对比
2. 扫描目录完整性对比
3. 扫描漏洞的准确性对比

扩展性展示

扩展自己编写的后门插件

**接下来介绍对本次测试软件**

WebScan，即本作品，是一款跨平台，可拓展的高效Web漏洞扫描工具。通过研究面向 Web 安全漏洞的分析技术，提出相应的修补建议，切实提高网站的自身安全。

对比产品AWVS(v12)

Acunetix Web Vulnerability Scanner（简称AWVS）是一款知名的网络漏洞扫描工具，它通过网络爬虫[测试](http://lib.csdn.net/base/softwaretest)你的网站安全，检测流行安全漏洞。

**软件准备**

WebScan本体(通过setup.py打包)

BackDoor模块组件

其他：  
蚁剑(后门利用演示工具)

**实操流程**

1. 展示平台登录平台和本产品（<http://120.79.174.75/DVWA-master/> ）

首先我们展示DVWA我们的测试平台

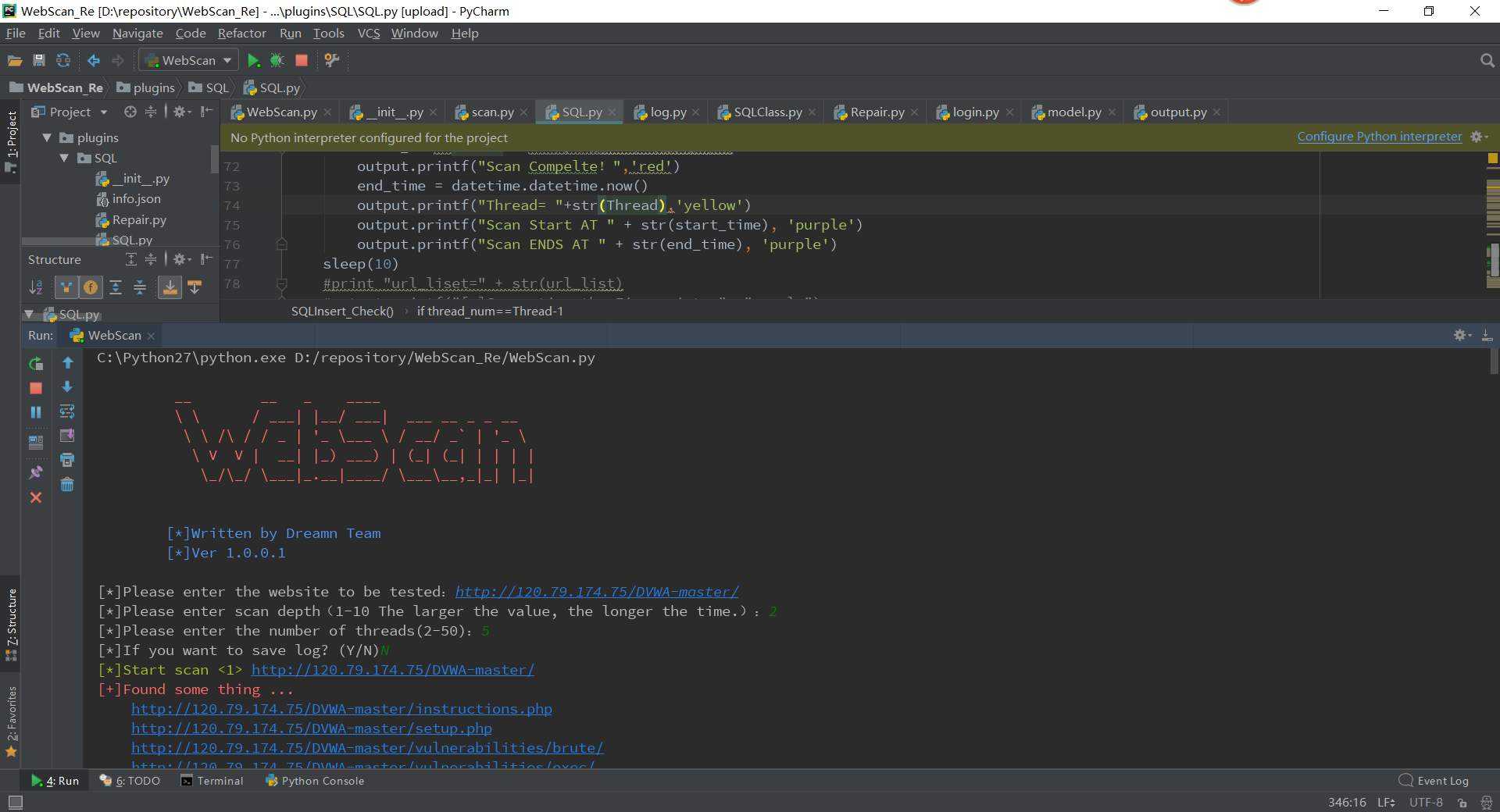
平台内部主要是OWASP排名前十的WEB漏洞环境

我们对比测试环节主要针对的是SQL注入模块。

本产品操作指南

下图是我们软件操作的指示图

**这是我们的LOGO**



线程数

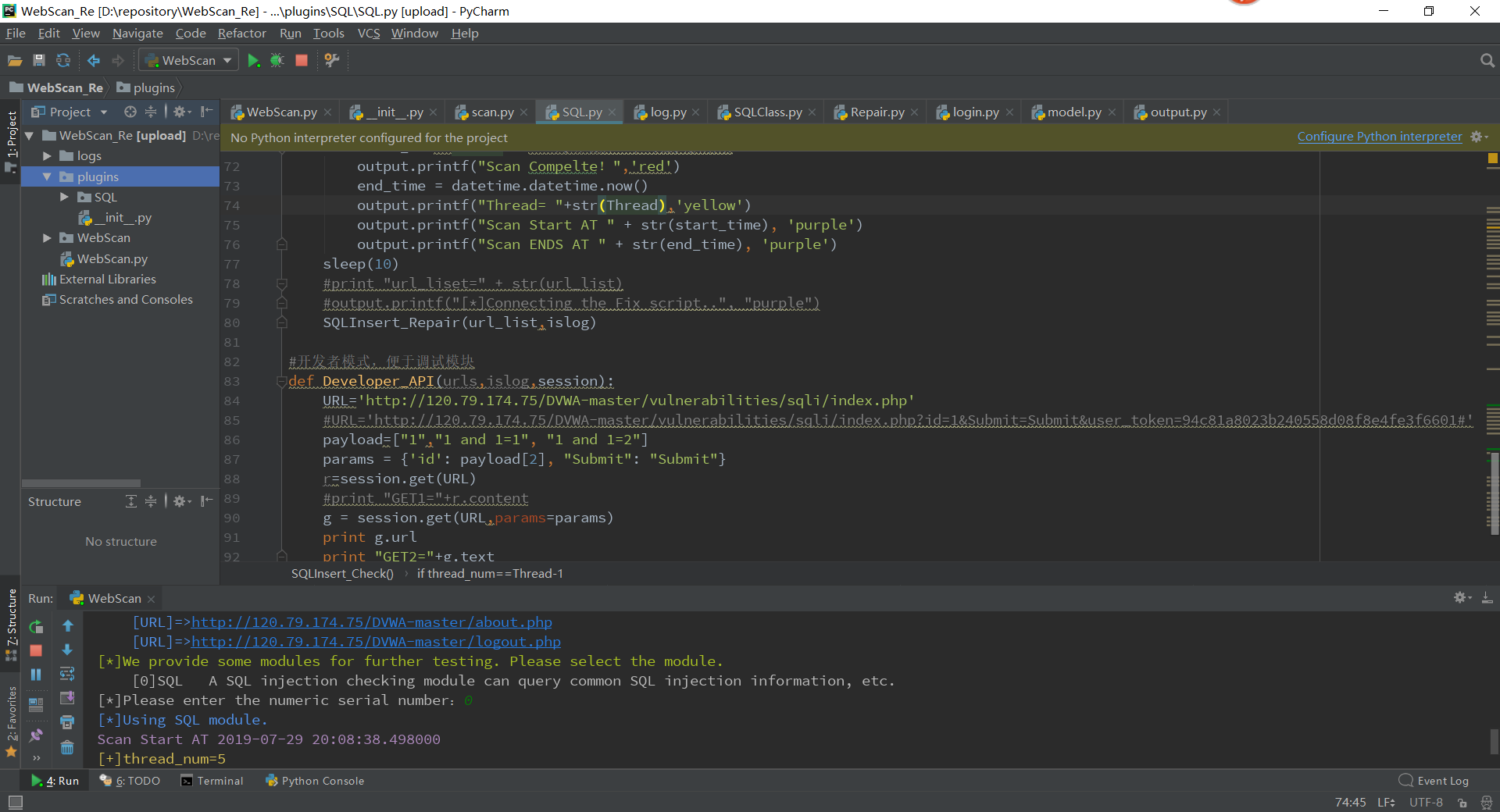
设置扫描深度

这里是我们测试的站点

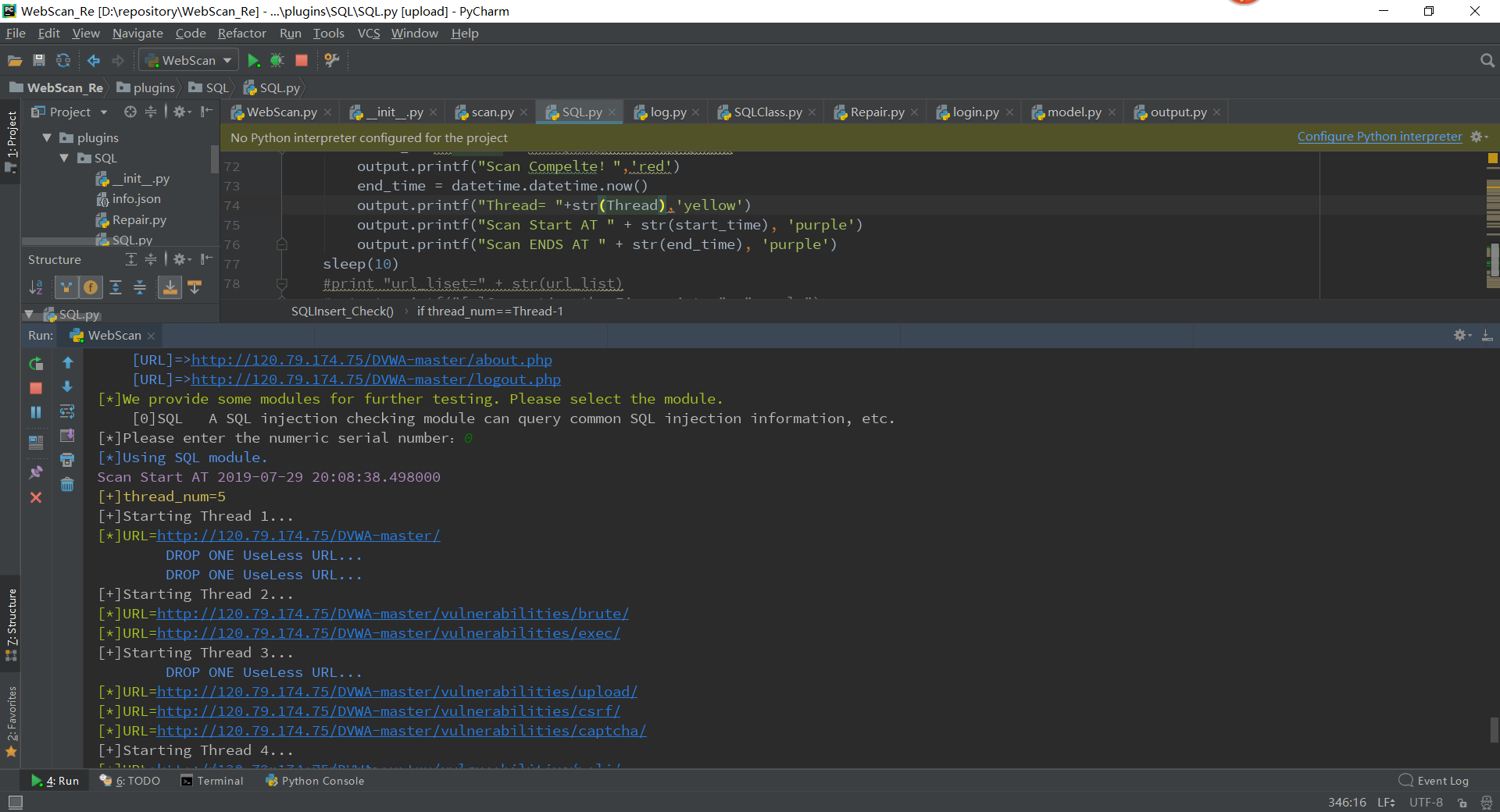
调用模块部分

程序会自动读取plugins目录下存放的插件(按照我们指定的标准和接口编写)

只需要输入序号即可调用模块



读取的插件



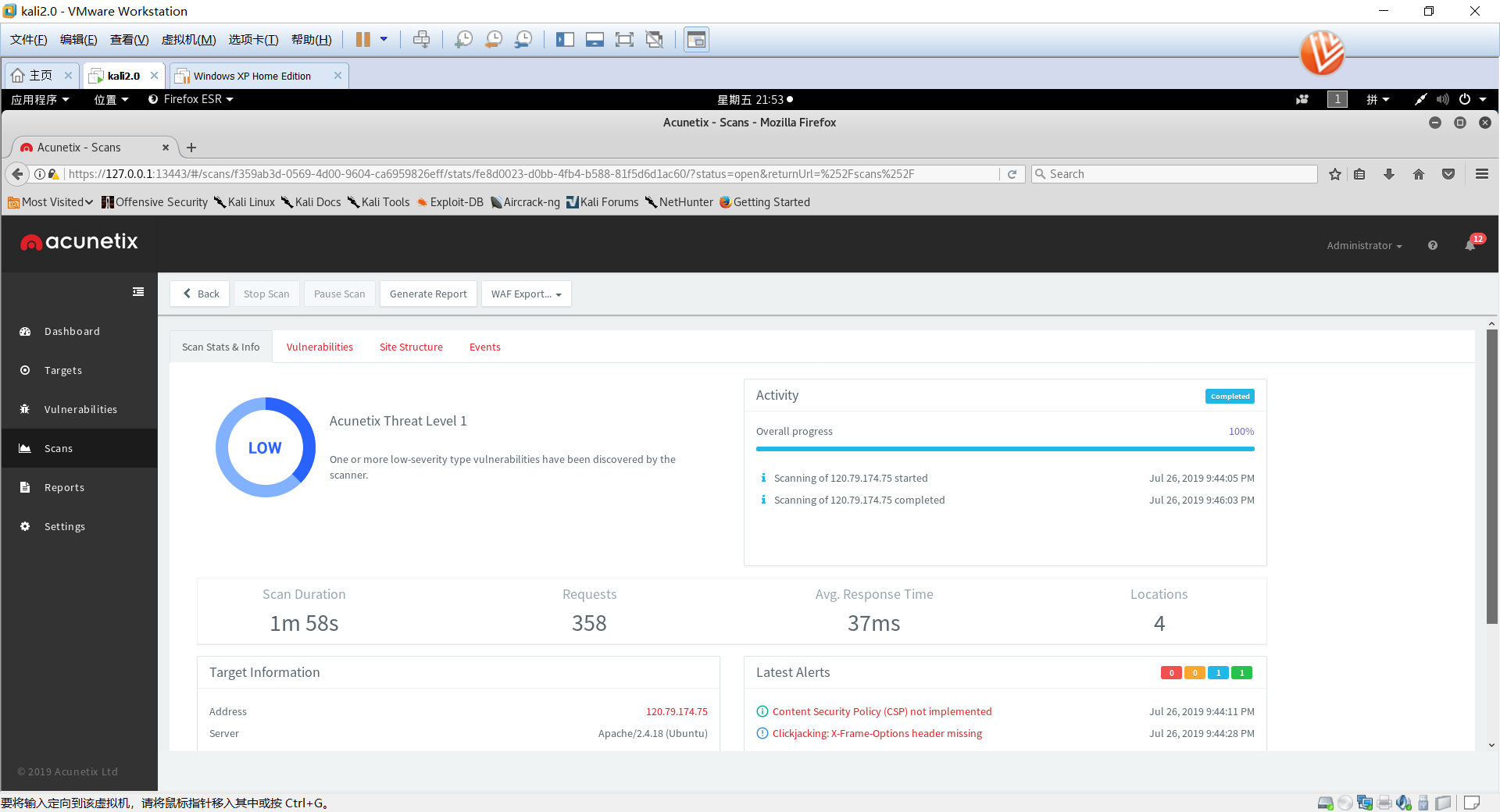
1. 站点扫描

（本软件和awvs分别测试) - 枚举该站点所有可能的目录或者敏感文件

2.1时间对比测试

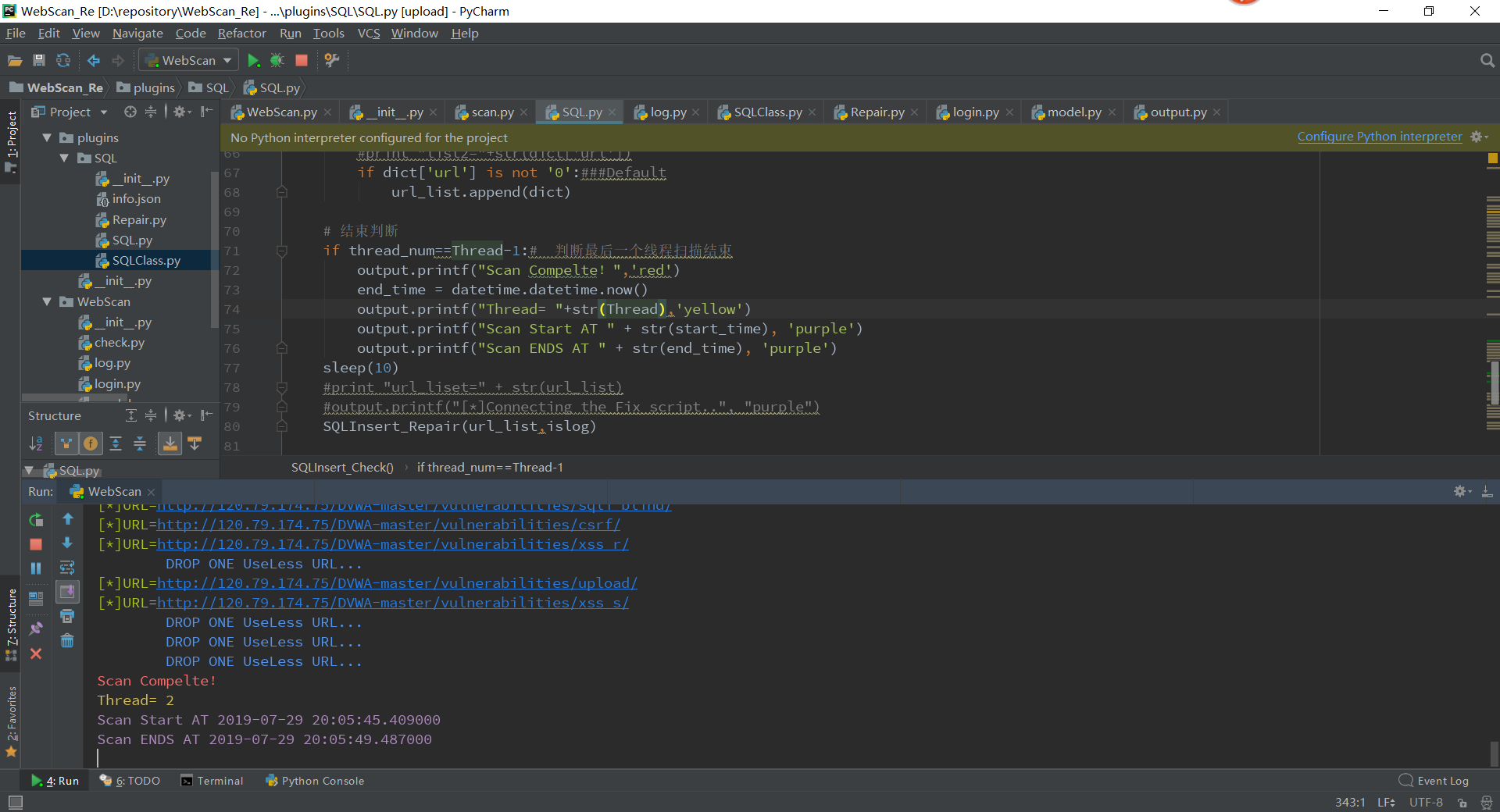
扫描速度对比

首先看对比软件AWVS扫描时间，总共花费xxx(1:58min）



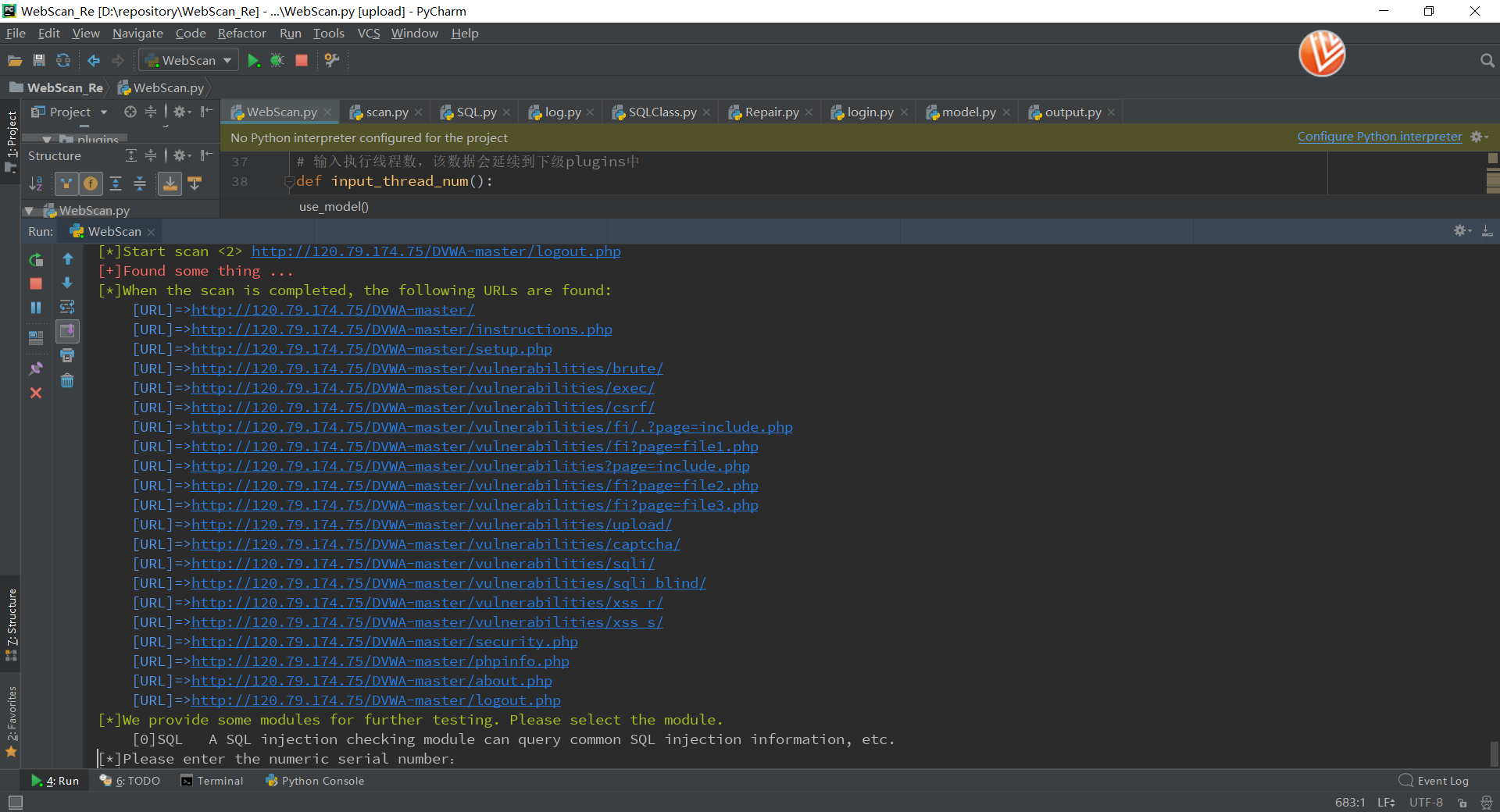
本软件测试结果

SQL模块花费时间4s左右（不算上scan模块）总体速度占优势

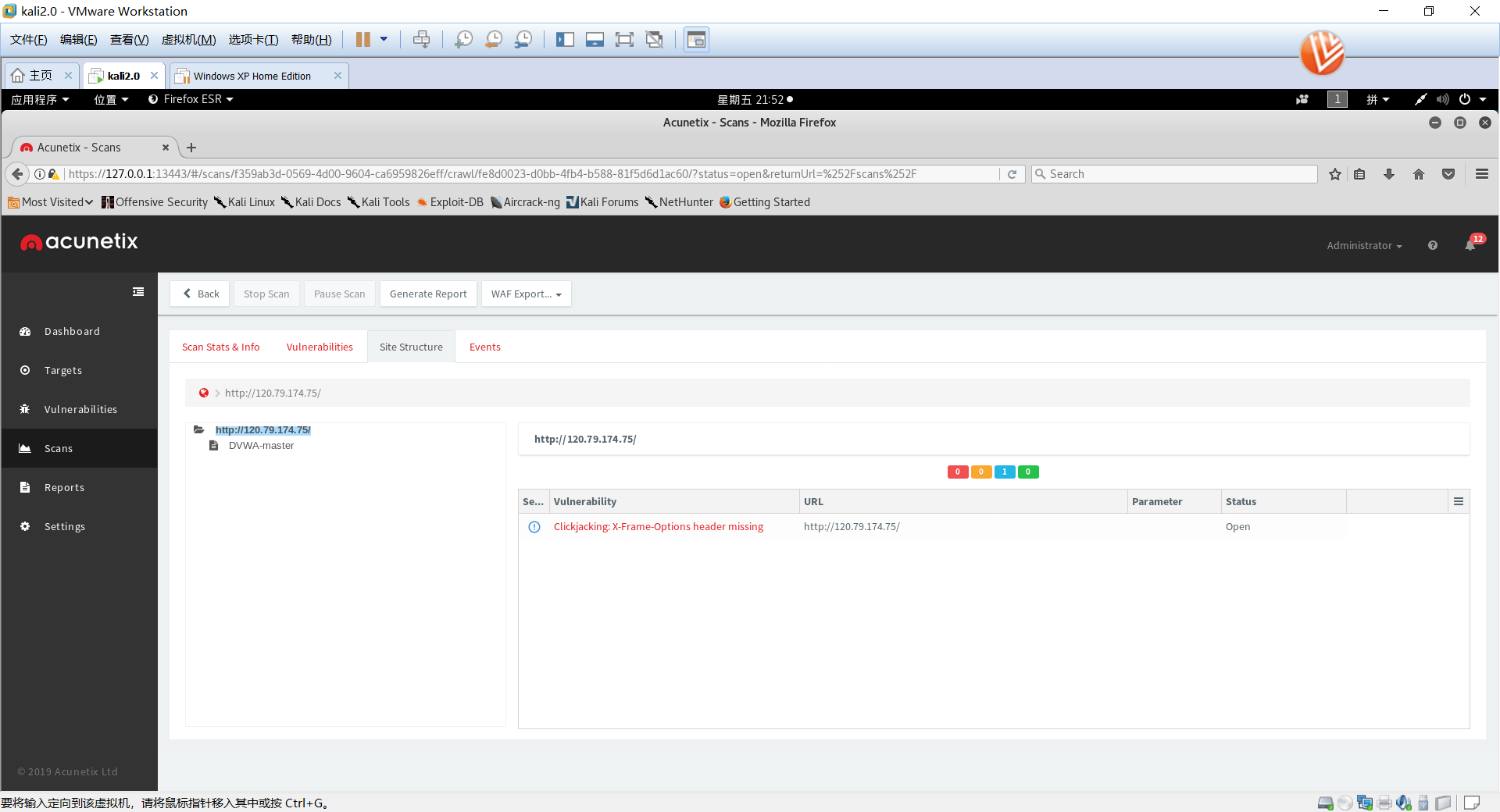


2.2扫描目录完整性对比

本产品扫描结果,扫描出了大量敏感目录。

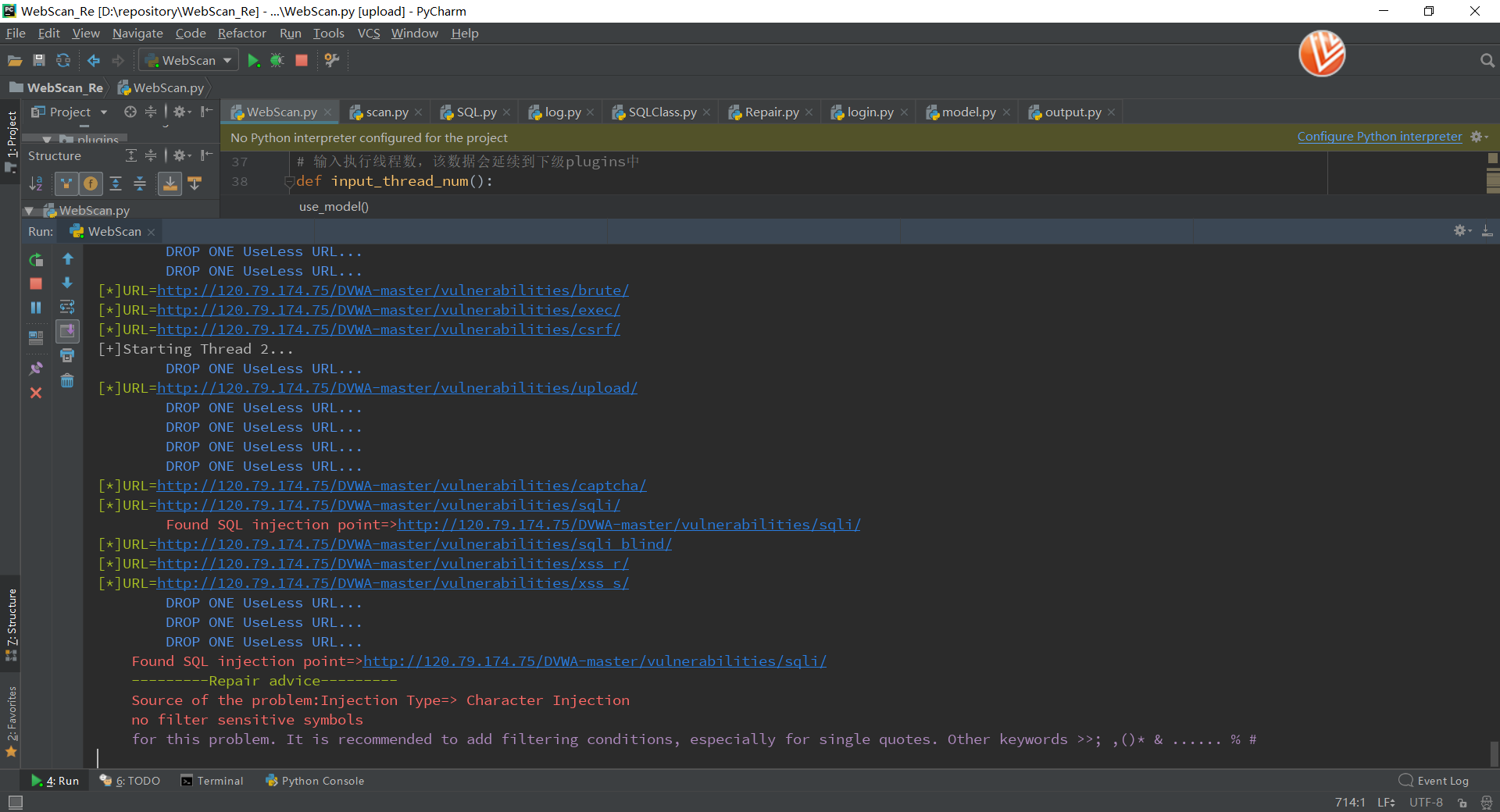


AWVS则没有扫出敏感目录



2.3扫描漏洞的能力对比

本产品扫描出了正确的结果，存在SQL注入。



而AWVS扫描出了一些低危漏洞和中危漏洞。扫描全面却较慢，并且没有扫描出DVWA平台上的SQL注入漏洞。

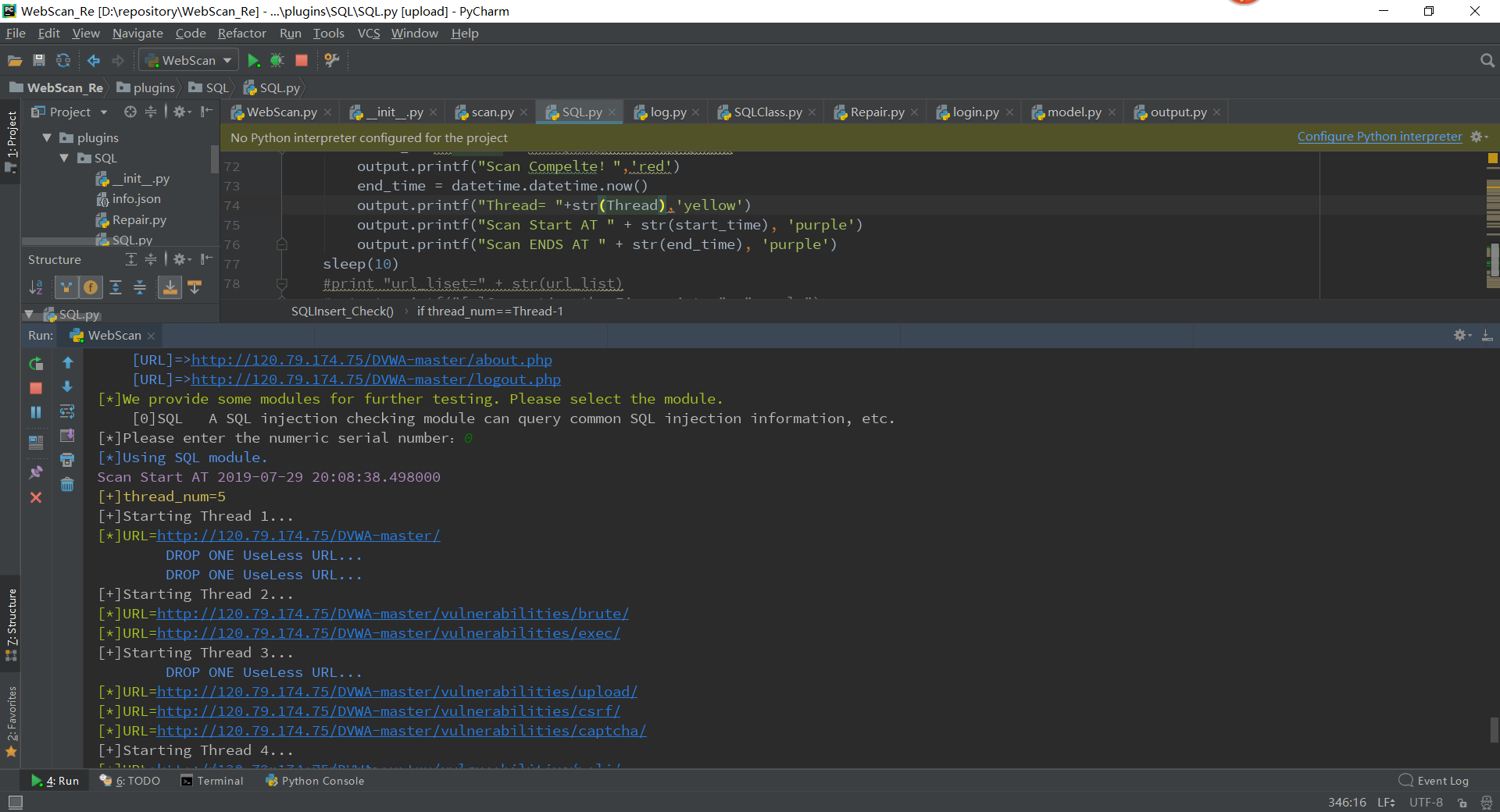
综上可见，全面性目前还并不是本产品的优势，但是针对性和扫描效率本产品的实力还是有目共睹的。

加之可扩展性，本产品可以在今后继续吸收大量开发者提供的插件，变得更加完善。

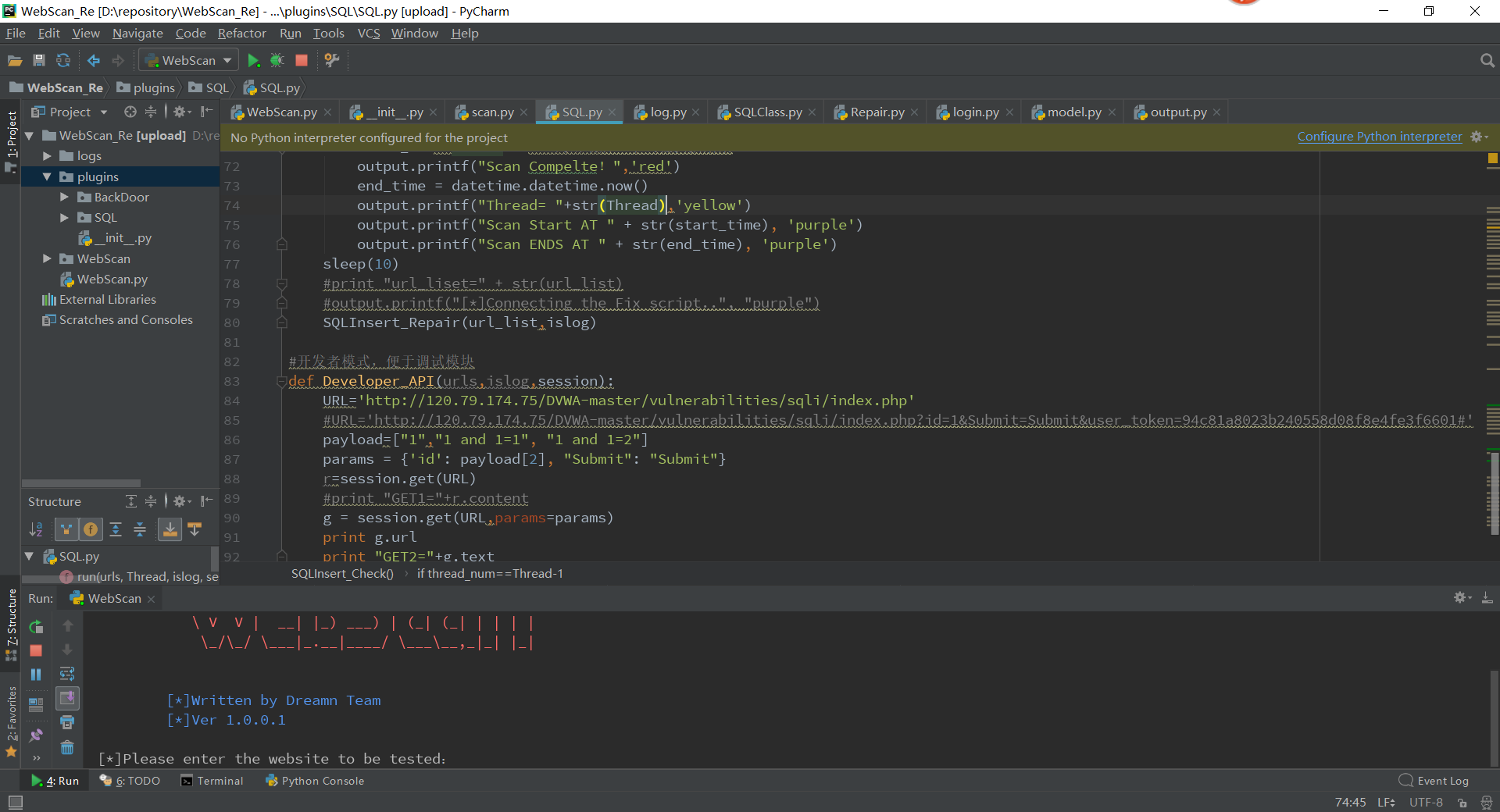
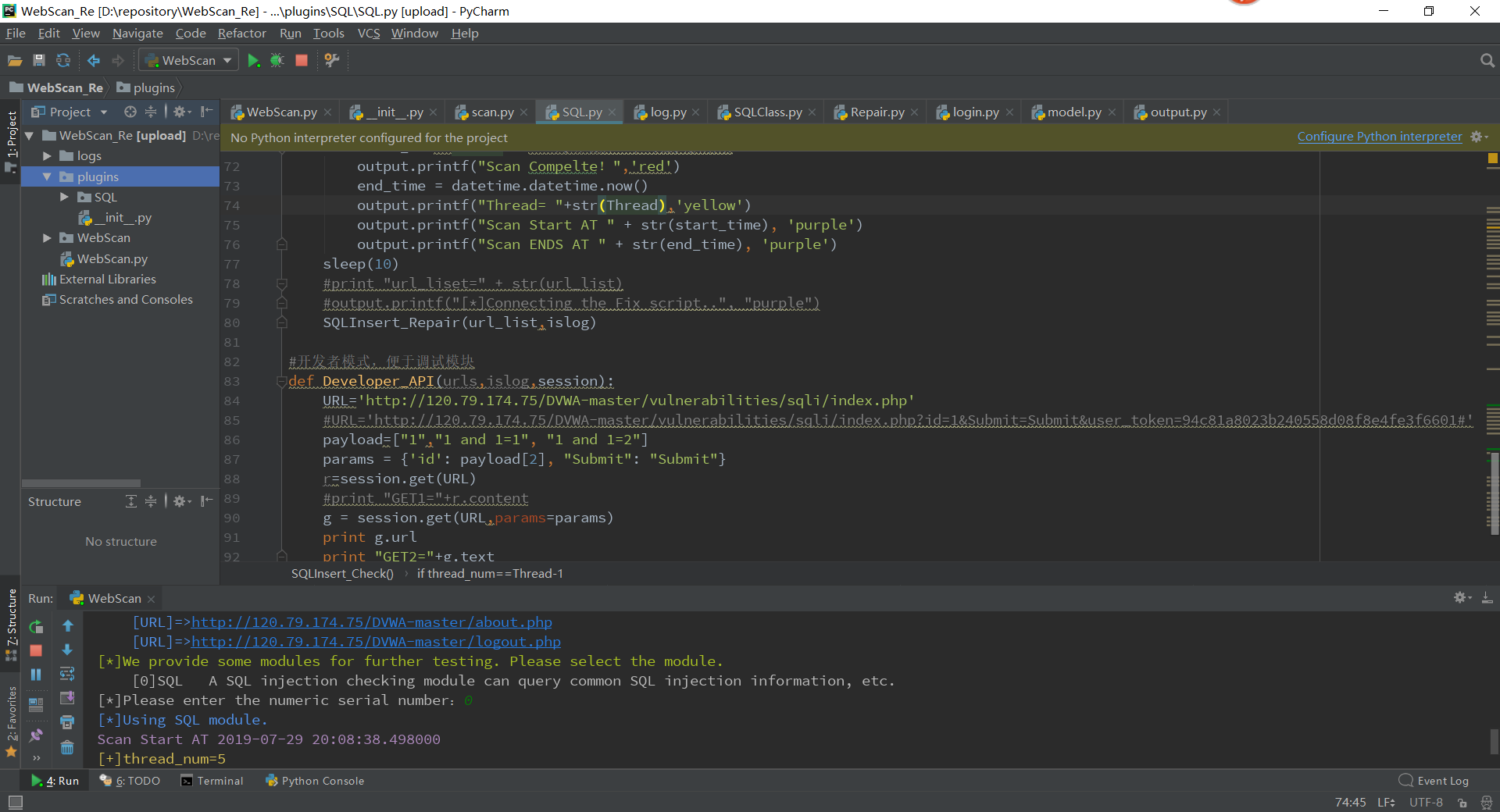
3.模块选择 - 动态加载各种模块

展示可扩展性(产品特色和创新点)

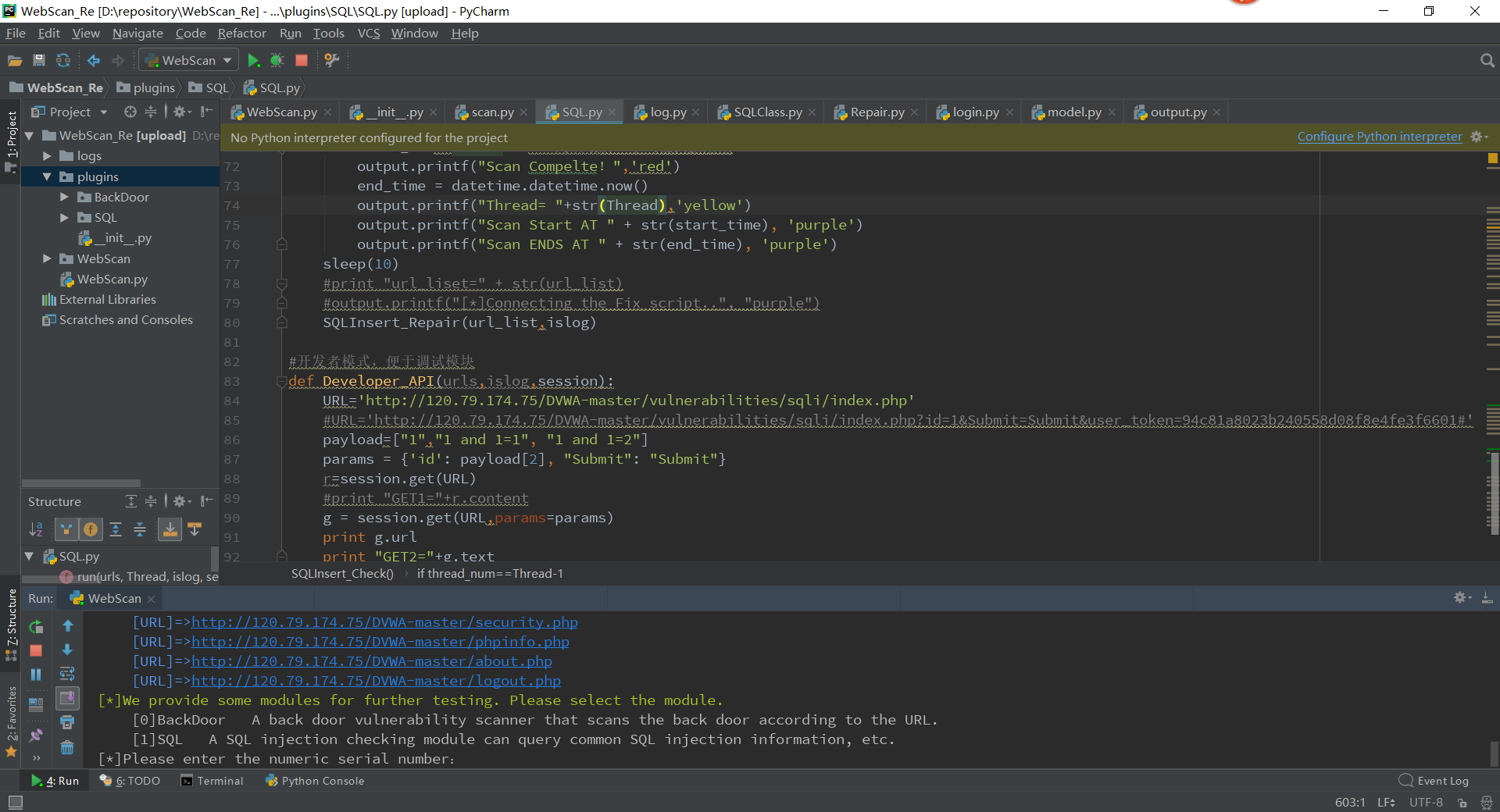
例如本来只拥有SQL注入模块



将其他模块(本次实测后门模块)放入plugins文件夹中



证明本产品扩展极为方便



后门模块测试

#如果有时间#可以展示一下远程连接后门，使用蚁剑连接一下后门，展示危害。

结论

扫描结果符合预期

扩展模块工作正常