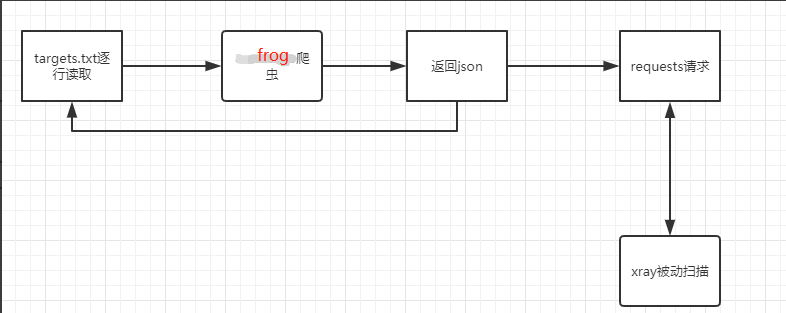
基于Xray+ScreamingFrogSEOspider的漏洞扫描

# 1、原理

基本原理如下图，盗的图，原理基本一样：



看了xray社区教程，发现使用脚本的方式进行调用，使用比较麻烦。

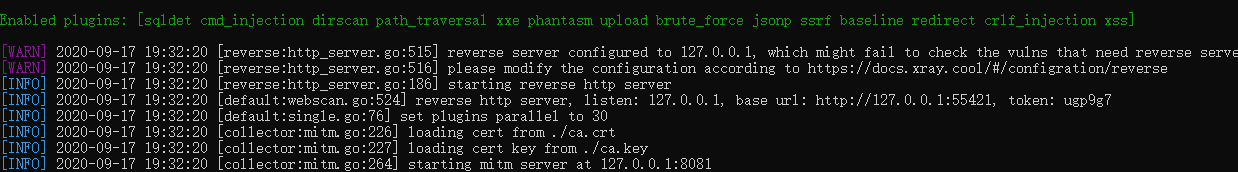
Crawlergo 遇到的问题，启动无反应，可能对Linux兼容性更好一点。并且移植到新环境需要搭建python环境，安装库文件，容易出错，不如直接使用GUI界面的配置比较好，并且crawlergo的模块比较小，爬取性能有限。

# 2、Xray配置

Cmd窗口运行：

xray\_windows\_amd64.exe webscan --listen 127.0.0.1:8081 --html-output xray-testphp1.html

运行之后会卡到如下界面：



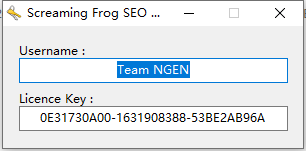
# 3、Forg配置

一路点击安装即可。

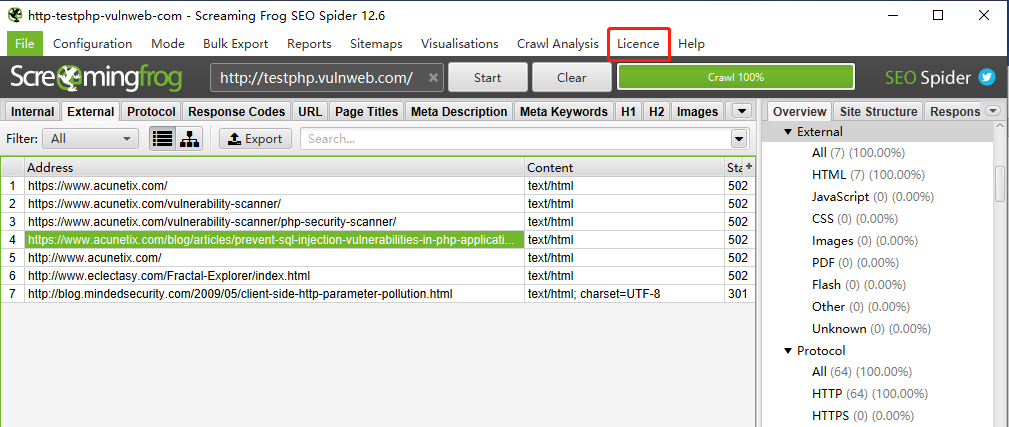
## 激活



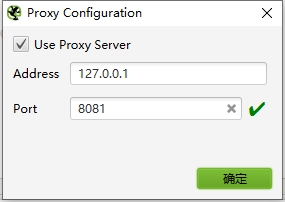
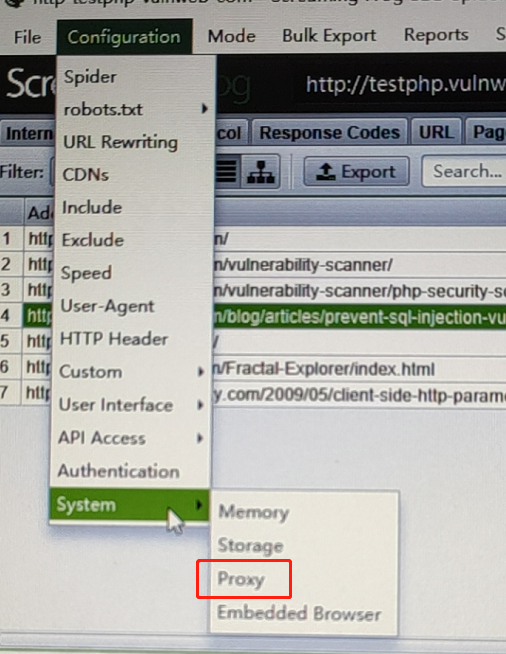
运行激活器



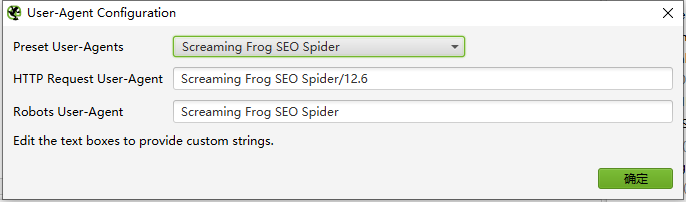
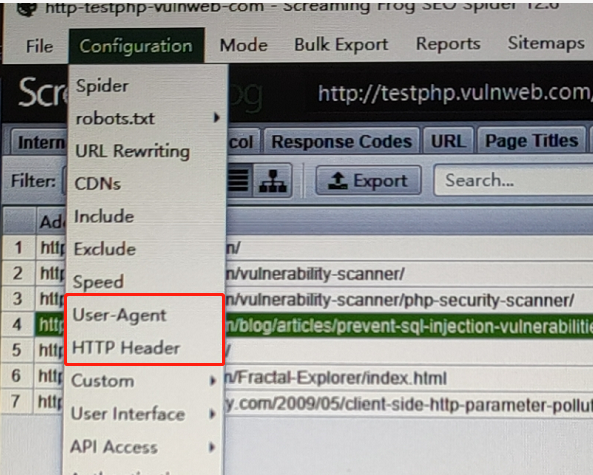
在界面license处导入重启即可。



## 代理配置

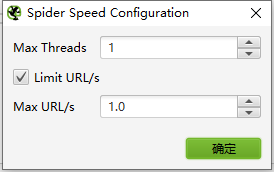
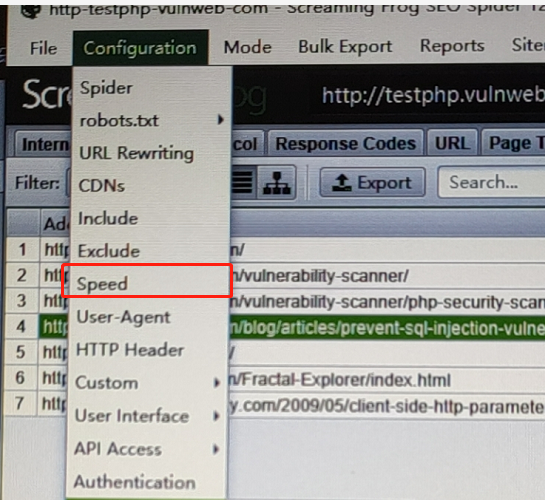


## Header和agent配置



默认是Frog自带的，防护设备会识别到，所以爬取会阻断，要设置为常见的Google或者火狐的。

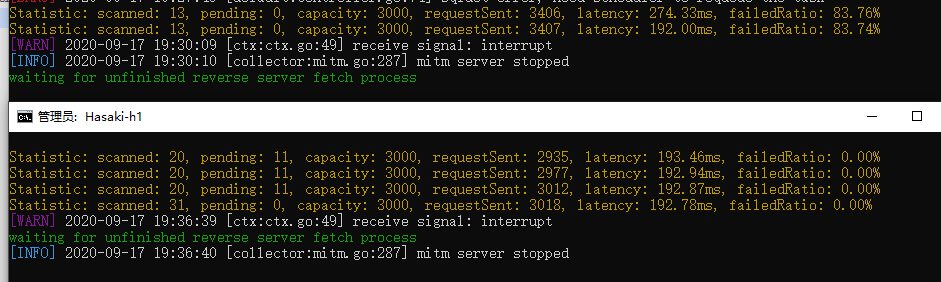
## 爬取速度配置



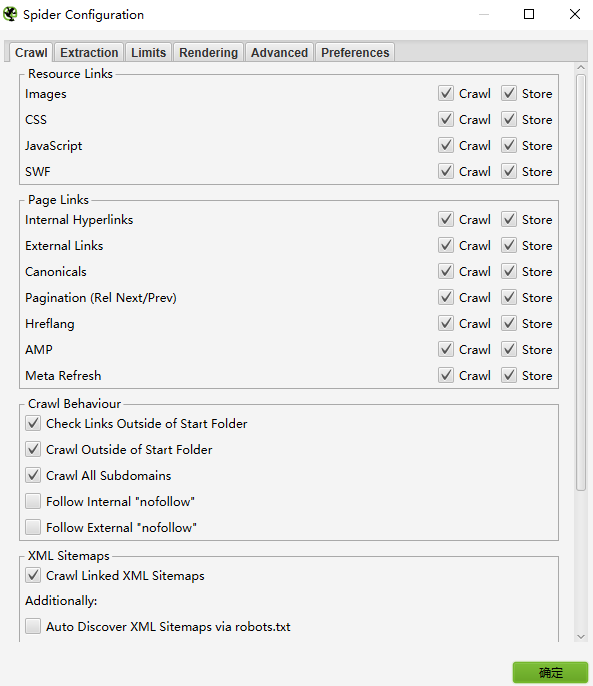
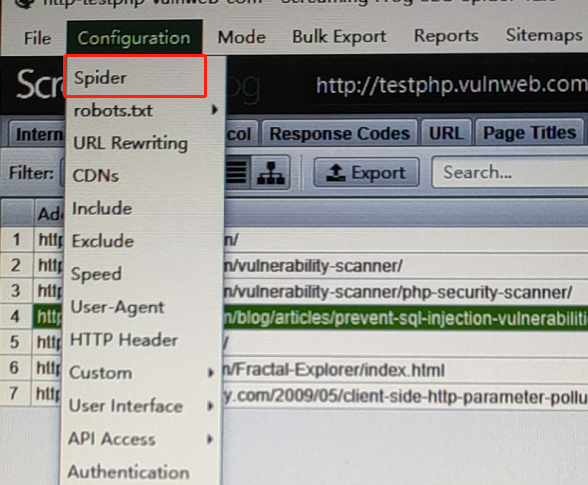
不赶时间尽量调低为1，xray接受不过来要丢包。

我调5的时候，xray故障率84%：

调1时候故障率为0：

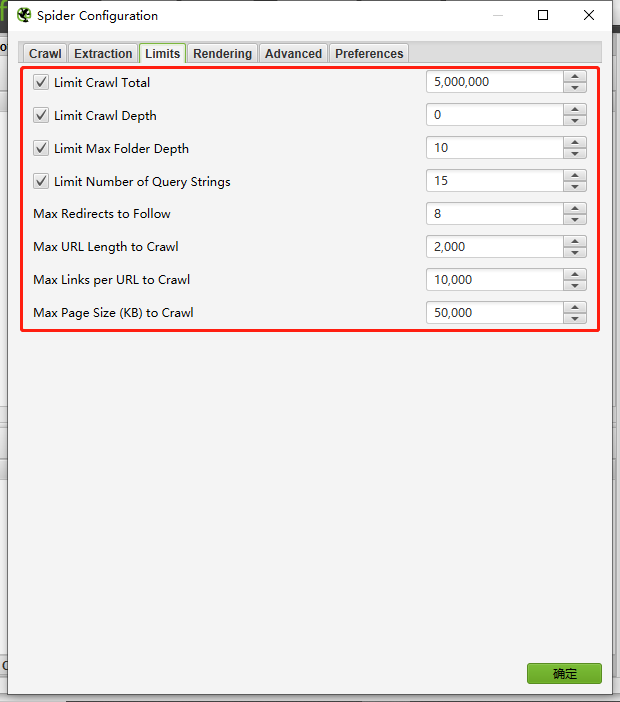


## Spider配置



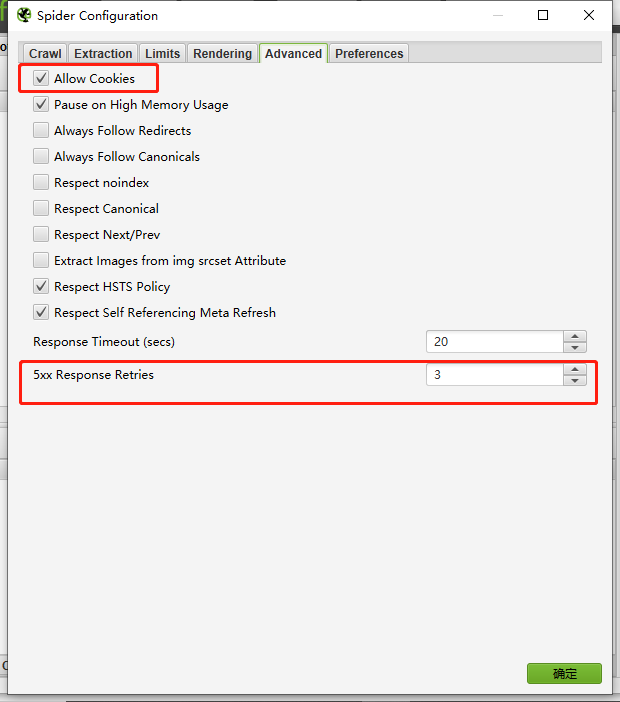
都是一些爬取配置，如果不知道该项的作用，鼠标放上自动会给出描述。

我只配置了比较重要的两条，其余配置各位老铁可以自行摸索。

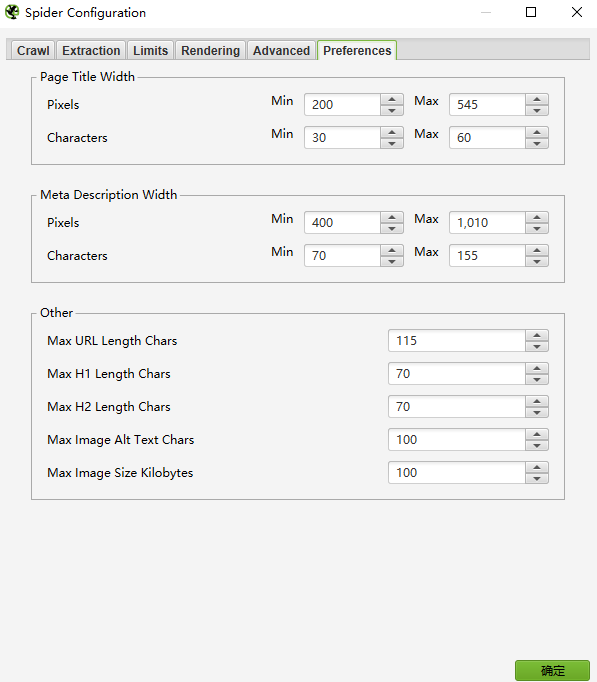


第一条、爬虫爬取深度，文件夹深度尽量调高，指不定有些智障管理员文件夹路径贼深，具体如上图所示，我只是截个图，别抄这个配置，自己估计就好。

第二条如下图所示，某些网站访问会设置cookie，还有500重传次数设置。

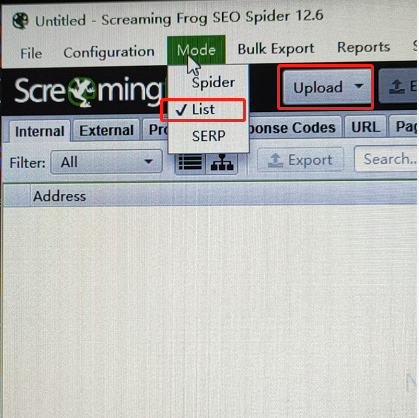


其实还有一个，作用不大，爬取外观上的一些限制，url之类的，还是往大的写。

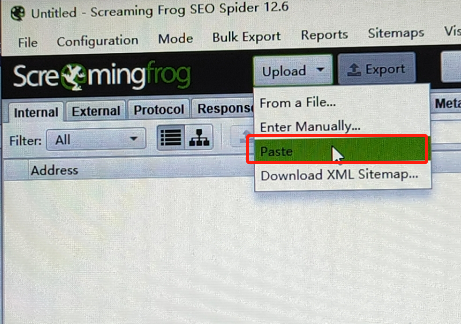


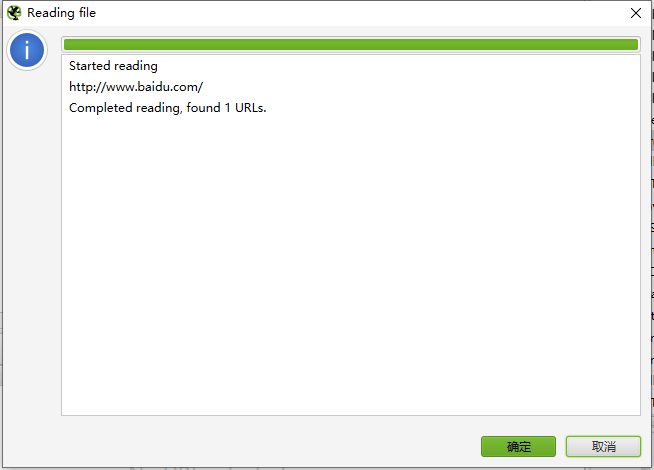
# 4、批量扫描

默认模式是spider爬虫模式，调节为list点击upload即可批量爬取。



直接选paste，此时你得先复制批量扫描的资产。





# 5、开始整活

扫了下测试站，http://testphp.vulnweb.com/，AWVS扫出漏洞比较全面一点。Xray漏洞单一，但优点是速度快。

自行对比

