全部课程 (/courses/) / Python打造漏洞扫描器 (/courses/761) / 扫描器测试以及未来展望

在线实验,请到PC端体验

扫描器测试以及未来展望

一、实验简介

这是扫描器的最后一章,主要说说扫描器的使用方式以及对未来的展望。

二、扫描器测试

这个扫描器是python 2.7写的,开发在windows平台上,测试在linux上(实验楼的实验平台),经过测试,在这两个系统上都能够运行。

另外,只需要python安装两个库就可以。 在PIP上的安装指令

pip install requests
pip install beautifulsoup4

代码下载

```
#用下面的代码安装
wget http://labfile.oss.aliyuncs.com/courses/761/shiyanlouscan9.zip
#解压缩
unzip shiyanlouscan9.zip
```

```
shiyanlou:~/ $ wget http://labfile.oss.aliyuncs.com/courses/761/shiyanlouscan9.z
iр
--2017-03-18 22:07:36-- http://labfile.oss.aliyuncs.com/courses/761/shiyanlousc
an9.zip
正在解析主机 labfile.oss.aliyuncs.com (labfile.oss.aliyuncs.com)... 118.178.62.1
正在连接 labfile.oss.aliyuncs.com (labfile.oss.aliyuncs.com)|118.178.62.133|:80.
  已连接。
.. 已连接。
已发出 HTTP 请求,正在等待回应... 200 OK
长度: 79158 (77K) [application/zip]
正在保存至: "shiyanlouscan9.zip"
100%[========] 79,158
                                                           --.-K/s
                                                                     用时 0.001s
2017-03-18 22:07:36 (88.4 MB/s) - 已保存 "shiyanlouscan9.zip" [79158/79158])
shiyanlou:~/ $ unzip shiyanlouscan9.zip
                                                                      [22:07:36]
Archive: shiyanlouscan9.zip
replace shiyanlouscan/.vscode/settings.json? [y]es, [n]o, [A]ll, [N]one, [r]enam
e: A
extracting: shiyanlouscan/.vscode/settings.json
  inflating: shiyanlouscan/data/data.json
  inflating: shiyanlouscan/data/dir.txt
  inflating: shiyanlouscan/data/web_shell.dic
```

然后进入到 shiyanlou 目录,查看下目录。

```
shiyanlou:~/ $ cd shiyanlouscan

shiyanlou:shiyanlouscan/ $ ls

data lib script test.py w8ay.py
shiyanlou:shiyanlouscan/ $ [22:09:29]

[22:09:29]

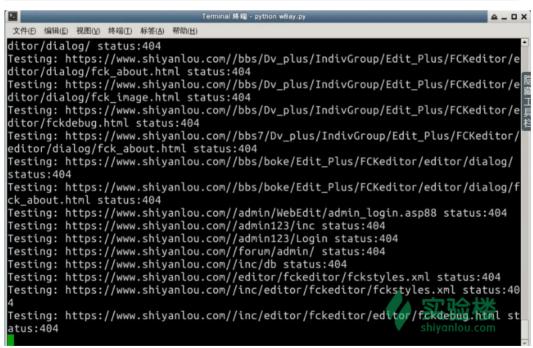
[22:09:30]
```

目录下就两个文件,test.py是写代码时候的测试脚本,我们直接运行w8ay.py,然后就开始扫描了,我们程序默认扫描的是 实验楼 www.shiyanlou.com。

```
shiyanlou:~/ $ cd shiyanlouscan
shiyanlou:shiyanlouscan/ $ ls
data lib script test.py w8ay.py
shiyanlou:shiyanlouscan/ $ python w8ay.py
CDN check....
```

运行截图:

```
115.29.233.149:9999 Close
115.29.233.149:21 Close
115.29.233.149:22 Close
115.29.233.149:23 Close
115.29.233.149:25 Close
115.29.233.149:2082 Close
115.29.233.149:2083 Close
115.29.233.149:5672 Close
115.29.233.149:2601 Close
115.29.233.149:2604 Close
115.29.233.149:53 Close
115.29.233.149:1080 Close
115.29.233.149:3389 Close
115.29.233.149:10050 Close
115.29.233.149:50000 Close
115.29.233.149:3128 Close
115.29.233.149:9300 Close
115.29.233.149:4440 Close
115.29.233.149:7001 Close
115.29.233.149:80 OPEN [web]
115.29.233.149:873 Close
115.29.233.149:1900 Close
115.29.233.149:28017 Close
```



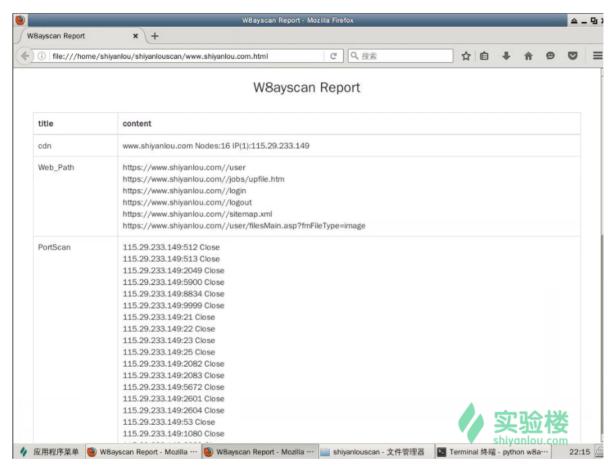
另外发现在实验楼的测试平台上扫描速度真是快的惊人啊。。

打开扫描器目录看到自动生成了报告



我们生成的报告是实时更新的,每个功能模块工作完毕后就会生成报告一次。在扫描器扫描完毕之前,我们可以随时打开,因为报告里面的数据是最新的。

我们已经生成一个报告。打开看看



扫描到一半后,再次打开

	https://www.shiyumou.com/oouises/100	
	https://www.shiyanlou.com/courses/615	
	https://www.shiyanlou.com/courses/614	
	https://www.shiyanlou.com/courses/750	
	https://www.shiyanlou.com/courses/751	
	https://www.shiyanlou.com/courses/756	
cdn	www.shiyanlou.com Nodes:16 IP(1):115.29.233.149	
Web_Path	https://www.shiyanlou.com//user	
	https://www.shiyanlou.com//jobs/upfile.htm	
	https://www.shiyanlou.com//login	
	https://www.shiyanlou.com//logout	
	https://www.shiyanlou.com//sitemap.xml	
	https://www.shiyanlou.com//user/filesMain.asp?fmFileType=image	
Webcms	[webcms]:https://www.shiyanlou.com/ cms NOTFound!	
email	bc3878b7ed0a4468a65390bd79e6e73f@sentry.shiyanlou	
	service@shiyanlou.com	
	bc3878b7ed0a4468a65390bd79e6e73f@sentry.shiyanlou	A
	bc3878b7ed0a4468a65390bd79e6e73f@sentry.shiyanlou	★ 다 하스 144
	bc3878b7ed0a4468a65390bd79e6e73f@sentry.shiyanlou	7 头 须 役
	bc3878b7ed0a4468a65390bd79e6e73f@sentry.shiyanlou	shiyanlou com
	bc3878b7ed0a4468a65390bd79e6e73f@sentrv.shivanlou	+ Sillyulliou.com

发现已经更新了不少东西。

三、实验总结

首先还是要提醒大家一下,本系列的教程只为技术分享,请勿用于非法用途。

然后

我们的扫描器已经完成了,各项功能已经基本具备的雏形。但只是雏形,基本能够满足一般的一些任务。

接下来大家可以对其进行升级,修改一些算法,加快一些速度和准确率。大家可以学习下商业扫描器,看看我们的扫描器和商业扫描器比较差在哪里,也可以看看各种开源的扫描器,看看别人的代码。推荐一下 安全从业人员仓库:https://github.com/We5ter/Scanners-Box/blob/master/README_CN.md (https://github.com/We5ter/Scanners-Box/blob/master/README_CN.md) 这里有很多优秀的代码值得我们学习。

如果大家学习python,学习了一些网页框架的话,也可以把扫描器嵌入到网页框架中玩,实现在浏览器上进行可视化的扫描器操作,结果也可视化的输出。

↓ 上一节 (/courses/761/labs/2673/document)

课程教师



new4

共发布过1门课程

查看老师的所有课程 > (/teacher/102428)



动手做实验,轻松学IT



් (http://weibo.com/shiyanlou2013)

关于我们 (/aboutus)

联系我们 (/contact)

加入我们 (http://www.simplecloud.cn/jobs.html)

技术博客 (https://blog.shiyanlou.com)

服务

公司

企业版 (/saas)

实战训练营 (/bootcamp/)

会员服务 (/vip)

实验报告 (/courses/reports)

合作

我要投稿 (/contribute) 教师合作 (/labs) 高校合作 (/edu/) 友情链接 (/friends) 开发者 (/developer)

学习路径

Python学习路径 (/paths/python) Linux学习路径 (/paths/linuxdev)

动手实践是学习 IT 技术最有效的方式 新聞学习路径 (/paths/giva/) Java学习路径 (/paths/giva/)