# Web系统测试

3.7 Web安全测试—Spider



### 目录

>什么是Spider

>Spider怎样使用



#### Spider



》Spider:爬虫

》作用:用来抓取Web应用程序的链接和内容等,它会自动提交登录表单(通过用户自定义输入)的情况下,Burp Suite的蜘蛛可以爬行扫描出网站上所有的链接,通过对这些链接的详细扫描来发现Web应用程序的漏洞









#### Passive Spidering \*\*





Passive spidering monitors traffic through Burp Proxy to update the site map without making any new requests.

Passively spider as you browse

Link depth to associate with Proxy requests:

0





#### Form Submission 表单提交



These settings control whether and how the Spider submits HTML forms.
对于爬网的时候遇到HTML表单如何操作

Individuate forms by:

Action URL, method and fields



- Don't submit forms 不发送表单
- Prompt for guidance 弹出向导,手动输入表单后发送
- Automatically submit using the following rules to assign text field values: 如有下面匹配规则对应表名就自动填写对应的值



Add	Enabled	Match type	Field name	Field value	
Edit	✓	Regex	mail	winter@example.com	<b>A</b>
	✓	Regex	first	Peter	
Remove	✓	Regex	last	Winter	
	✓	Regex	surname	Winter	
Up	✓	Regex	name	Peter Winter	
	✓	Regex	comp	Winter Consulting	
Down	✓	Regex	addr	1 Main Street	¥
		_			*





#### Application Login

需要表单身份认证时, 如何操作



These settings control how the Spider submits login forms.

- Don't submit login forms 不提交表单
- Prompt for guidance 弹出向导手动提交表单
- Handle as ordinary forms 像上面普通表单一样处理
- Automatically submit these credentials: 自动填写下面的表单

Username:	
Password:	





#### Spider Engine



These settings control the engine used for making HTTP requests when spidering.

Number of threads: 10 线程数

Number of retries on network failure: 3 失败后重新尝试的数目

Pause before retry (milliseconds): 2000 等待时间

Throttle between requests (milliseconds): 0

Add random variations to throttle





#### Request Headers 请求头



These settings control the request headers used in HTTP requests made by the Spider.

Add A
Edit U
Remove

Accept: \*/\*

Accept-Language: en

User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)

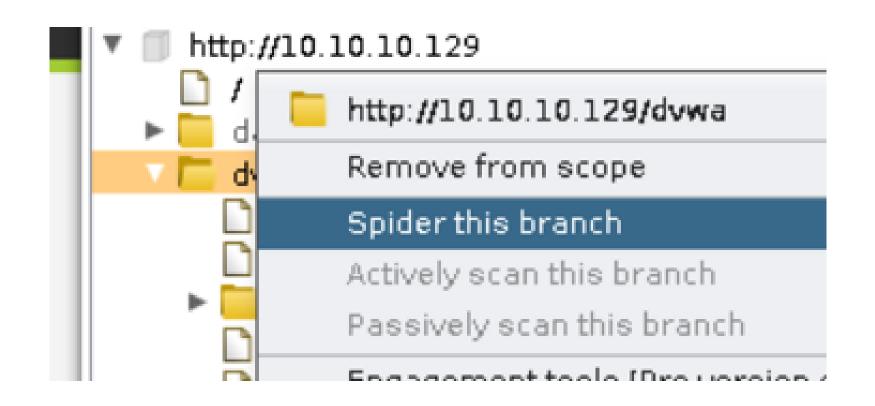
Connection: close

Up

Down



)通常对一个站点先进行手动爬网在进行被动爬网 在Target界面对目标右键,选择Spider进行爬网







## Question

