Web 系统测试

4.7 渗透测试—Spider

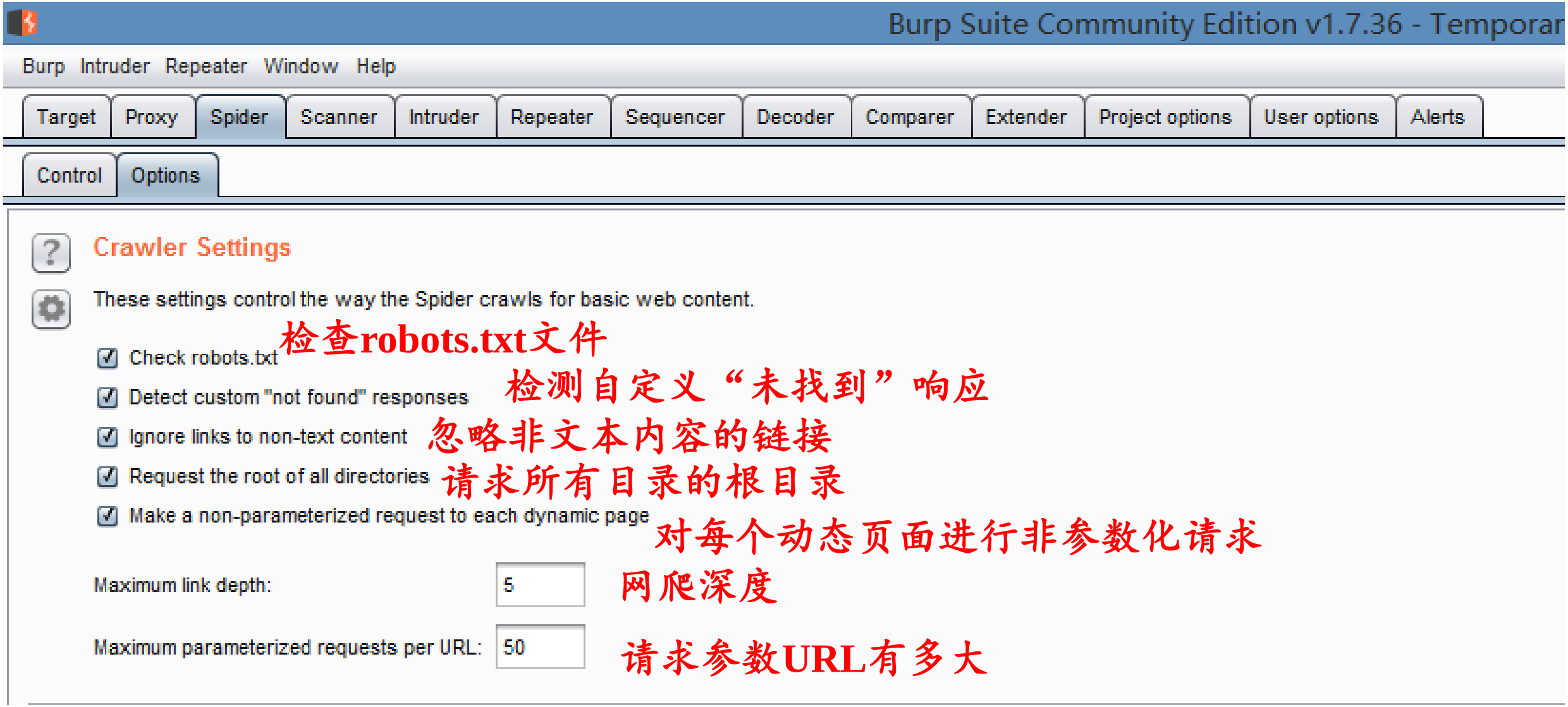
河北师范大学软件学院
Software College of Hebei Normal University

目 录

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**

Spider使用


Burp Suite Community Edition v1.7.36 - Temporar
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Control Options
Crawler Settings
These settings control the way the Spider crawls for basic web content.
Check robots.txt
检查robots.txt文件
Detect custom "not found" responses
检测自定义“未找到”响应
Ignore links to non-text content
忽略非文本内容的链接
Request the root of all directories
请求所有目录的根目录
Make a non-parameterized request to each dynamic page
对每个动态页面进行非参数化请求
Maximum link depth: 5
网爬深度
Maximum parameterized requests per URL: 50
请求参数URL有多大

Spider使用

Passive Spidering

被动爬网

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

Spider使用

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

Spider使用

Add

Edit

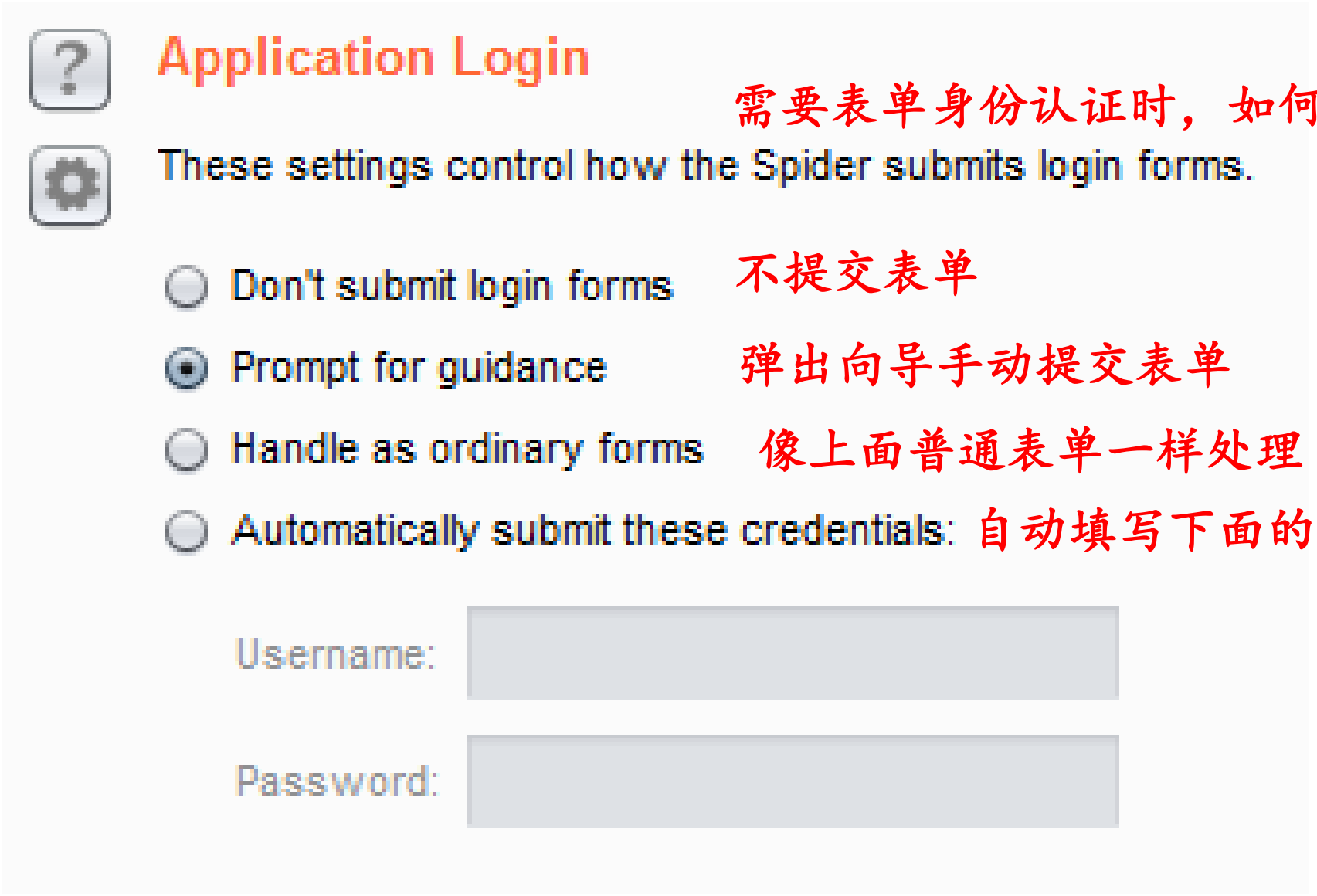
Remove

Up

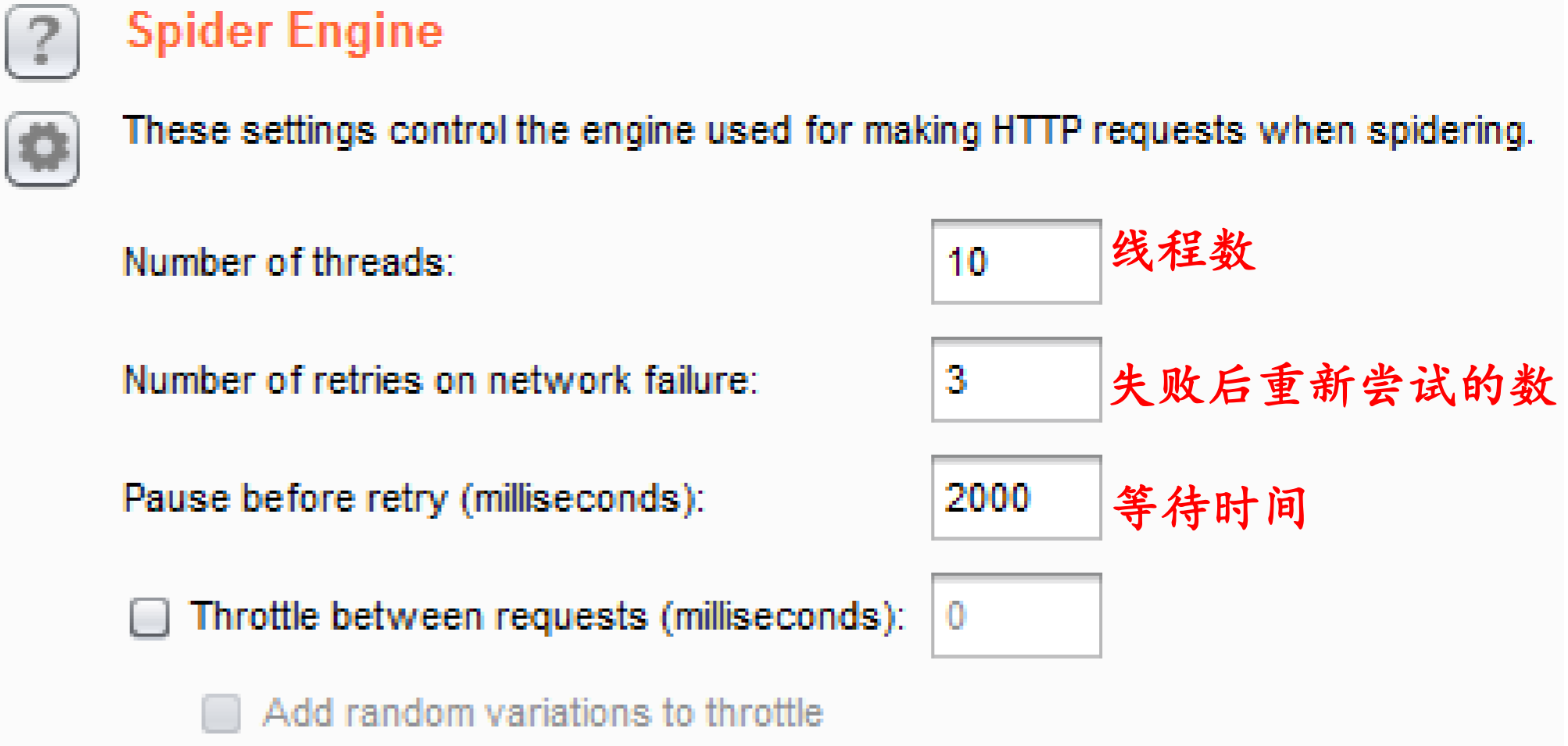
Down

Enabled	Match type	Field name	Field value
☑	Regex	mail	winter@example.com
☑	Regex	first	Peter
☑	Regex	last	Winter
☑	Regex	surname	Winter
☑	Regex	name	Peter Winter
☑	Regex	comp	Winter Consulting
☑	Regex	addr	1 Main Street

Spider使用


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使用


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

Spider使用

Request Headers 请求头

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

Add

Edit

Remove

Up

Down

Accept: */*

Accept-Language: en

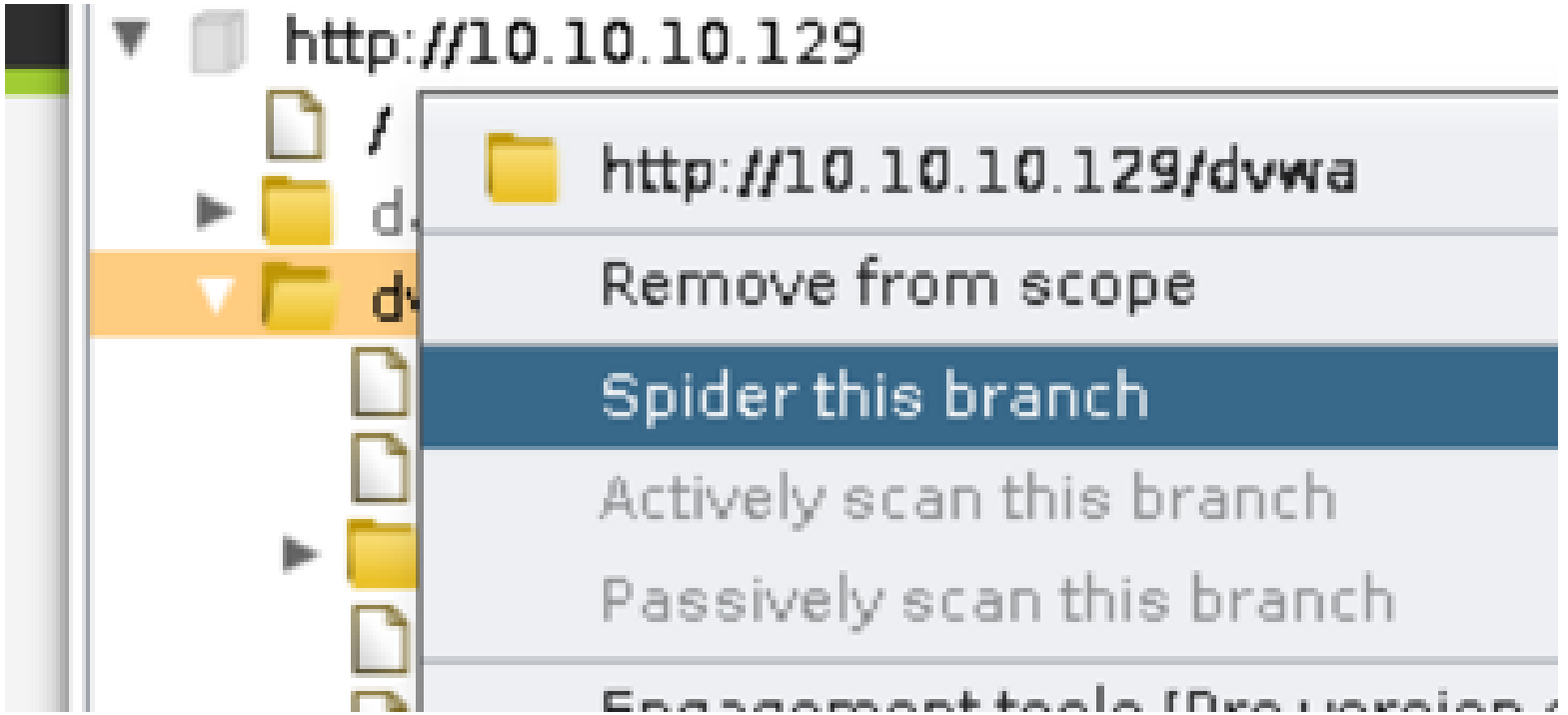
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)

Connection: close

Spider使用

➢通常对一个站点先进行手动爬网，再进行被动爬网

在Target界面对目标右键，选择Spider进行爬网



Spider使用


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Control
Options
Spider Status
Use these settings to monitor and control Burp Spider. To begin spidering, browse to the target application, then right-click one or more nodes in the target site map, and choose "Spider this host / branch".
停止爬网
清除未爬网的队列
Spider is paused
Clear queues
Requests made: 0
Bytes transferred: 0
Requests queued: 0
显示队列中未爬完的数目
Forms queued: 0

Question