漏洞扫描工具使用实验

一【实验目标】

- 了解 Burp Suite 的概念及工作原理
- 掌握 Burp Suite 的攻击过程。

二【实验环境】

- Windows 10 操作系统
- Burp Suite

三【实验原理】

Burp Suite 是用于攻击 web 应用程序的集成平台。它包含了许多工具，并为这些工具设计了许多接口，以促进加快攻击应用程序的过程。所有的工具都共享一个能处理并显示 HTTP 消息，持久性，认证，代理，日志，警报的一个强大的可扩展的框架。

工作原理：当 Burp Suite 运行后，Burp Proxy 开启默认的 8080 端口作为本地代理接口。通过置一个 web 浏览器使用其代理服务器，所有的网站流量可以被拦截，查看和修改。默认情况下，对非媒体资源的请求将被拦截并显示。

对所有通过 Burp Proxy 网站流量使用预设的方案进行分析，然后纳入到目标站点地图中，来勾勒出一张包含访问的应用程序的内容和功能的画面。

四【实验步骤】

实验具体操作步骤如下：

1. 进入 win10 系统，输入密码“123456”。如图 1 所示。

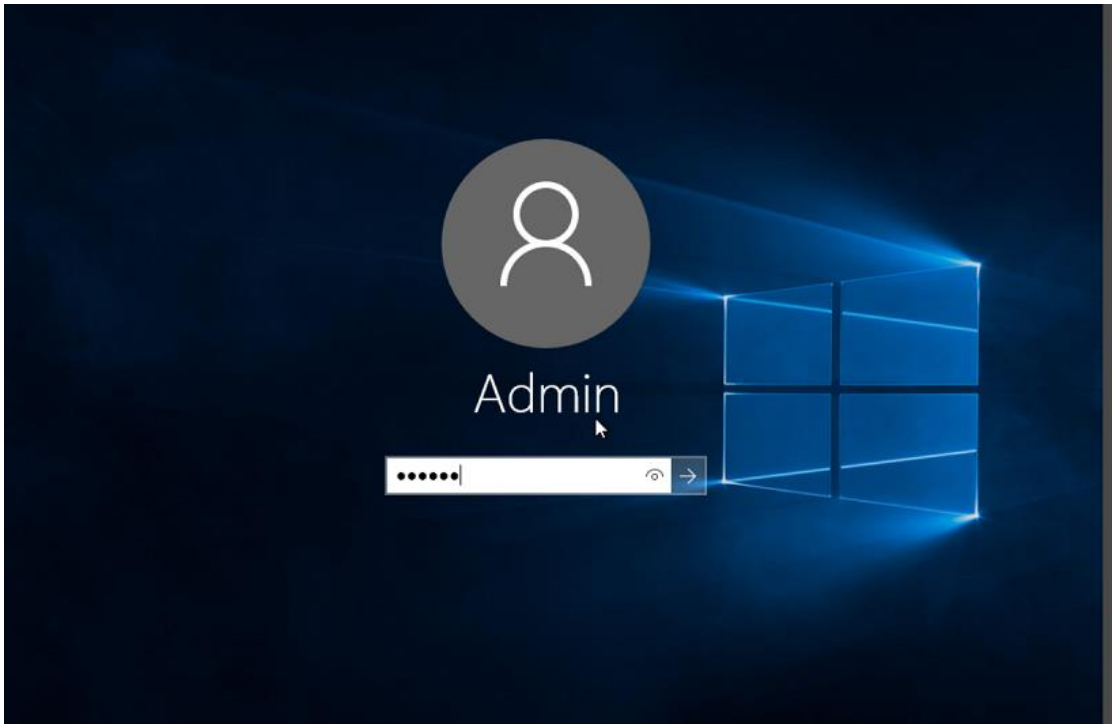

图 1

2. 进入系统后点击开始在菜单搜索栏中输入“IIS”。如图 2 所示

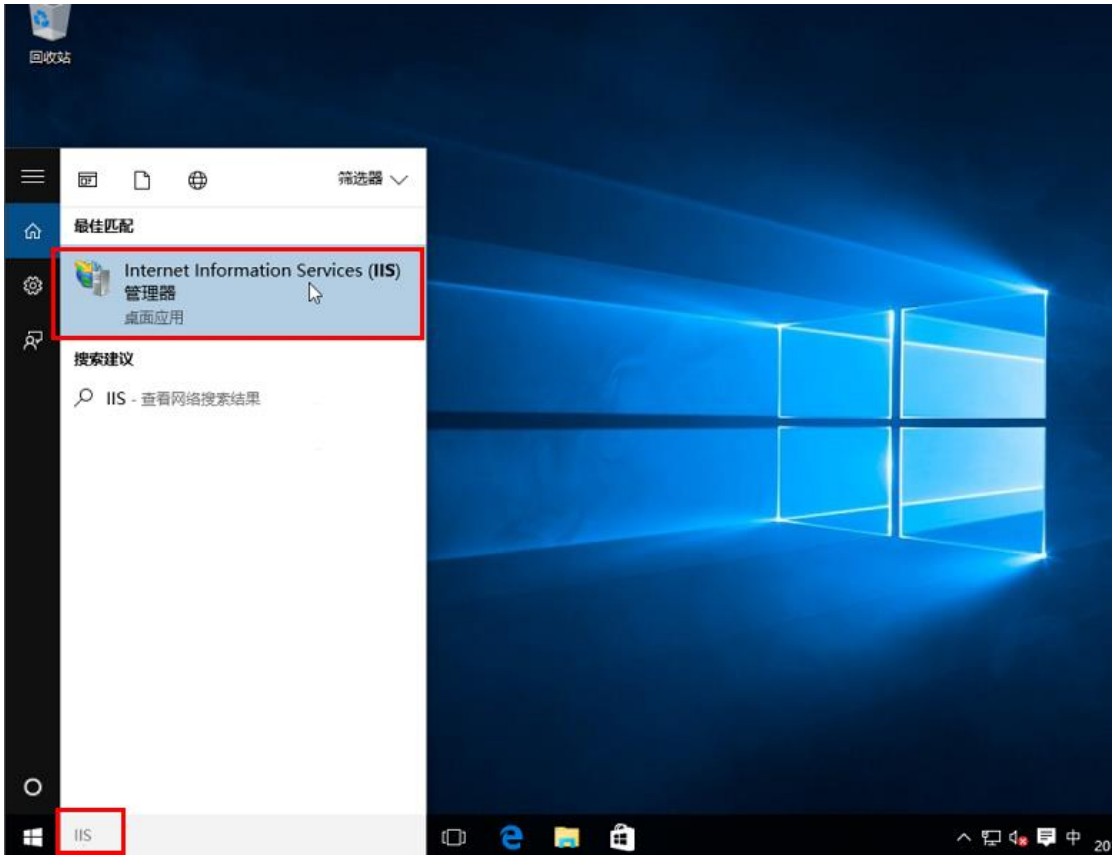

图 2

3. 打开 IIS 后只有一个默认网站，右击【网站】，选择【添加网站】。如图 3 所示。

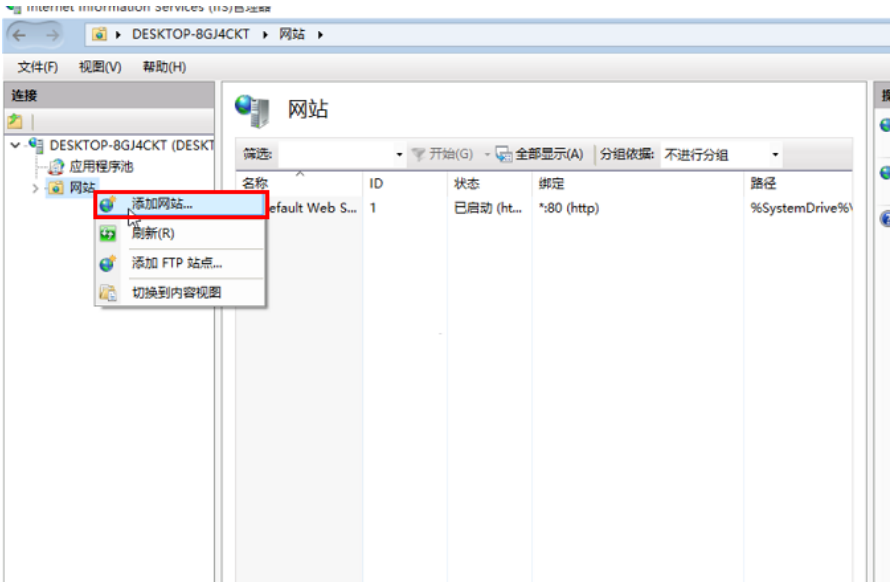

图 3

4. 设置网站名称为【Article】，连接池为【DefaultAppPool】物理路径为【C:/tools/Article】,【IP 地址】选择下拉框中的默认地址。如图 4 所示

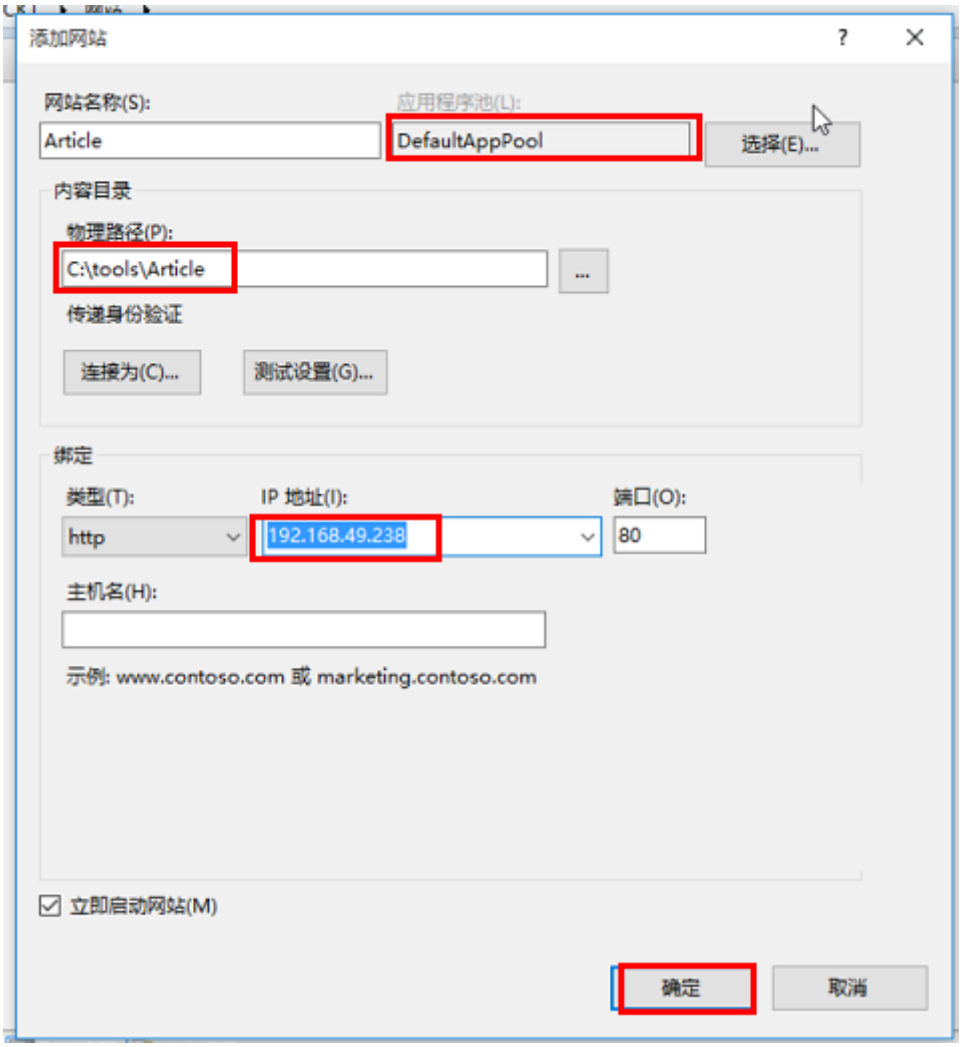

图 4

5. 点击左侧栏的【应用程序池】，选择【设置应用程序池默认设置】。如图 5 所示。

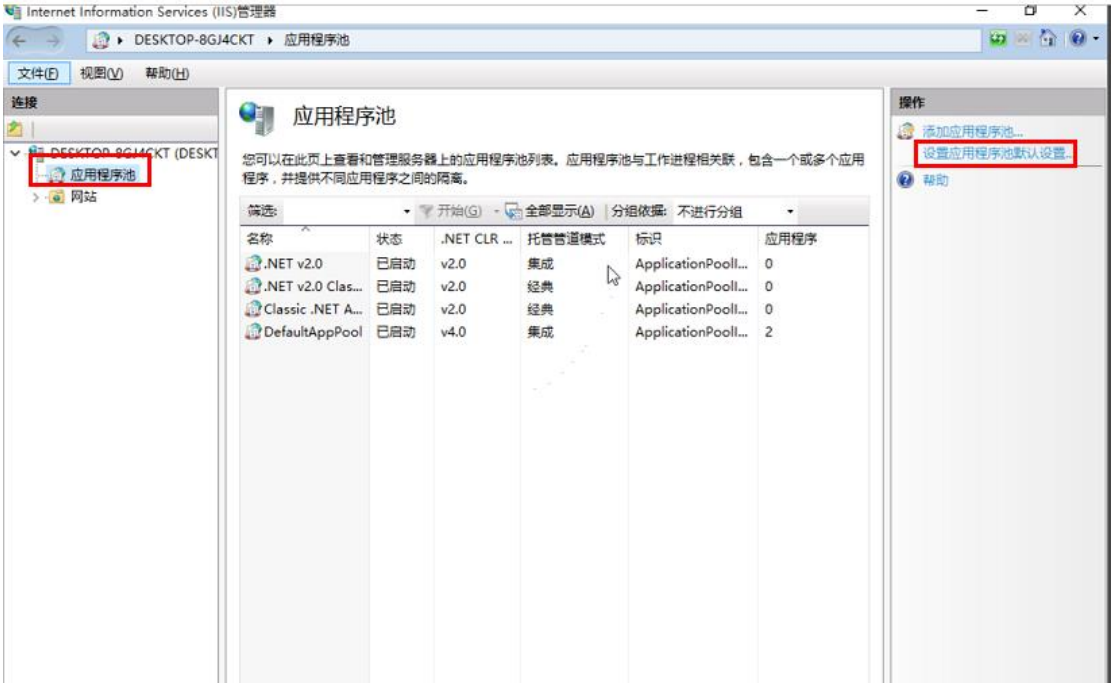

图 5

6. 将【启用 32 位应用程序】的属性设置为【true】，如图 6 所示。

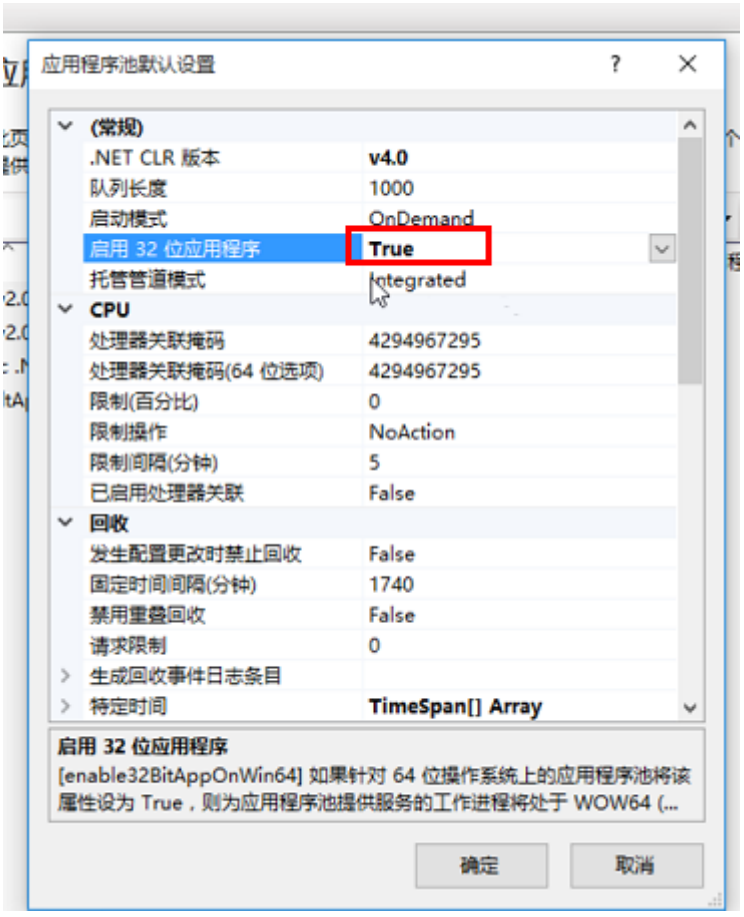

图 6

7. 右击【Article】网站，选择【管理网站】中的【浏览】。如图 7 所示。

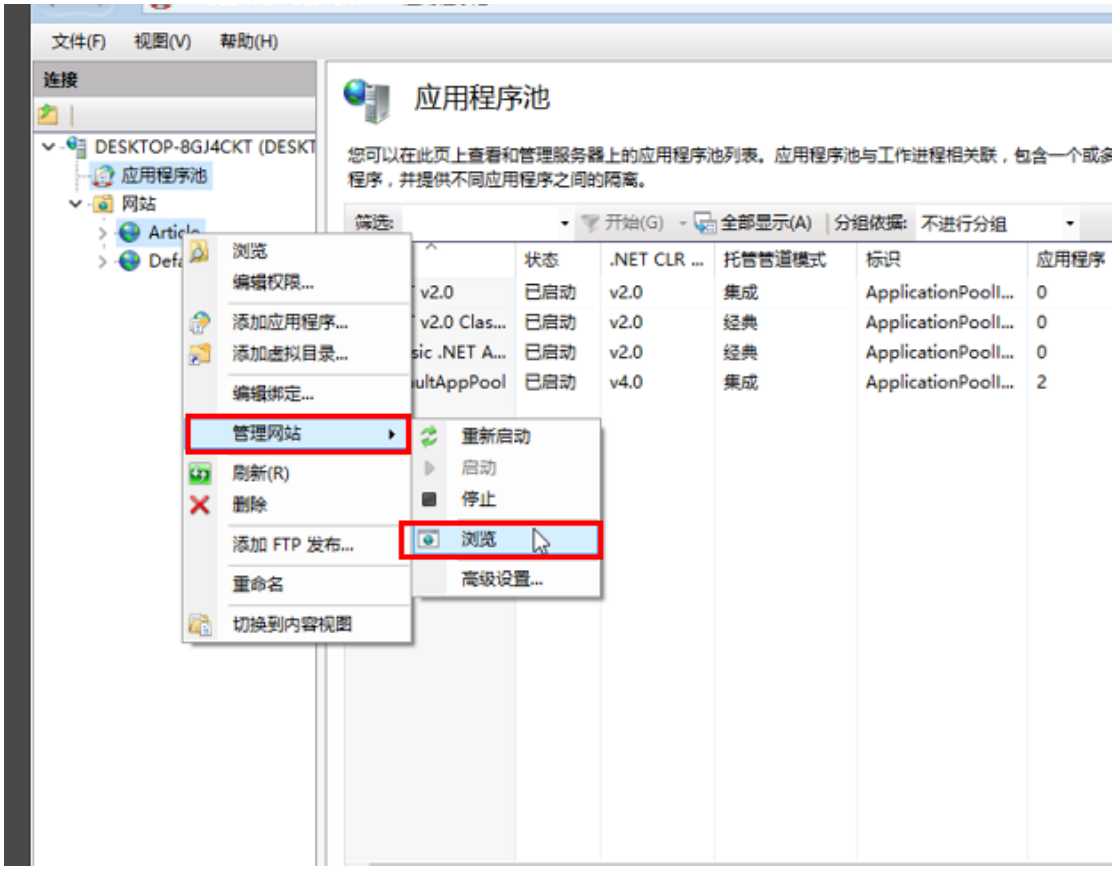

图 7

8. 浏览器打开 Article 网站，可以看到网站中的内容。如图 8 所示。

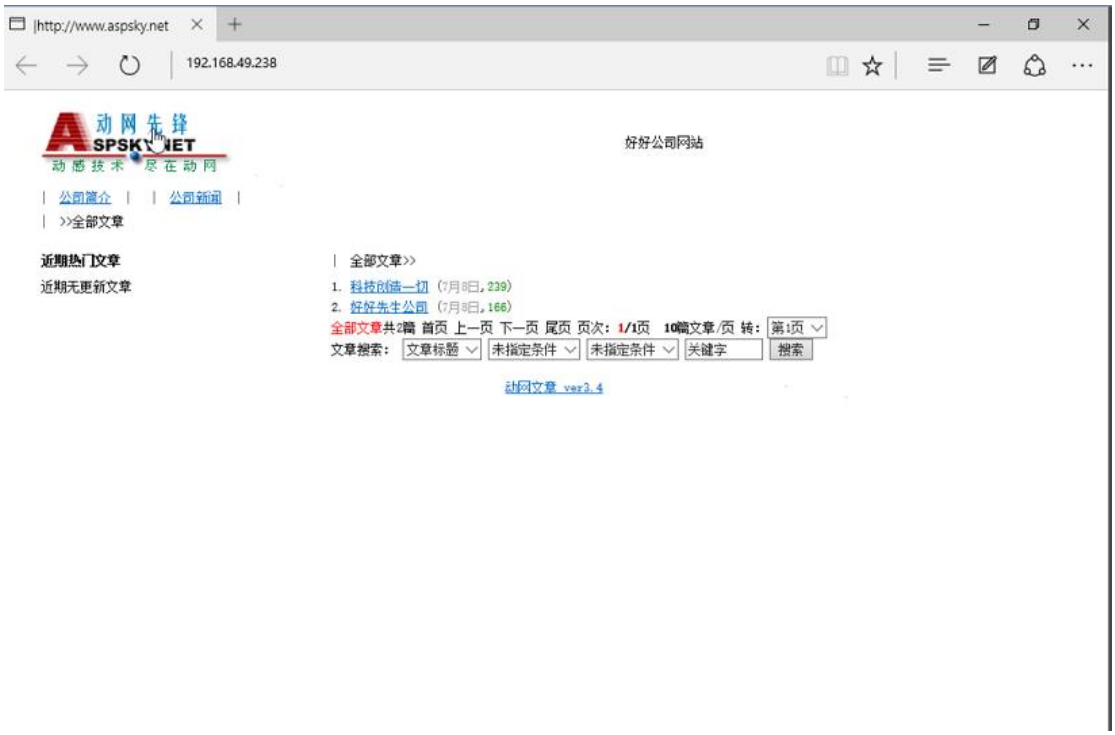

图 8

9. 打开【控制面板】选择【系统和安全】中的【Windows Defender 防火墙】。如图 9 所示

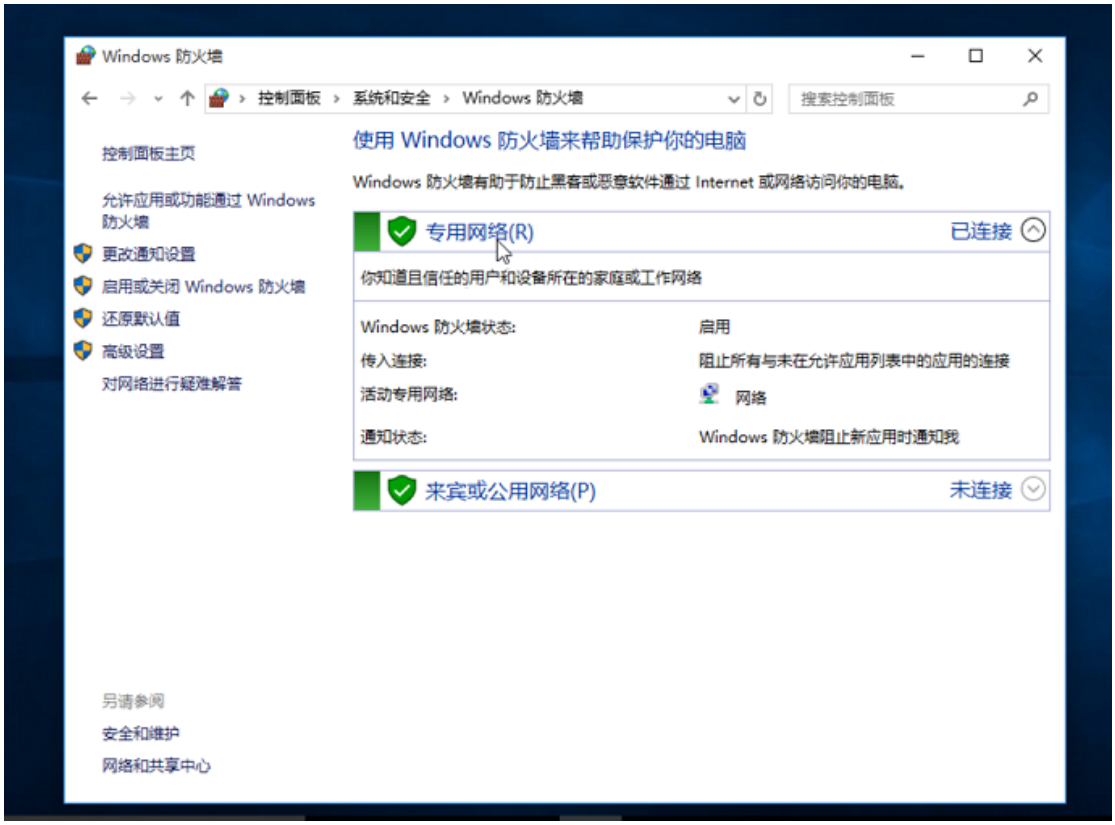

图 9

10. 点击左侧【启用或关闭 Windows Defender 防火墙】，关闭防火墙，点击【确定】。如图 10 所示。

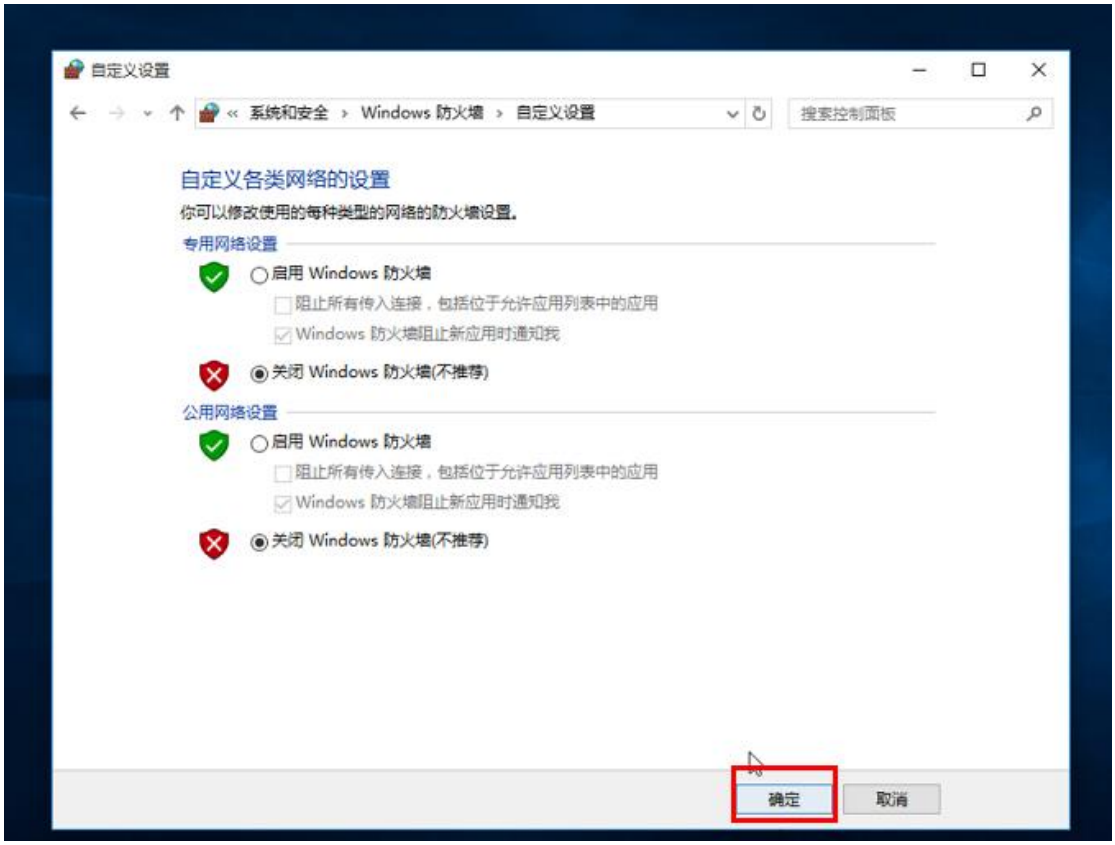

图 10

11.在 IIS 中，右击 Article 网站，绑定域名【www.test.com】。进入【C:/windows/system32/drivers/etc】文件夹，双击 host 文件，以记事本形式打开。在最后一行加入本机 IP 地址与域名的映射【192.168.49.238　　www.test.com】。如图 11 所示。

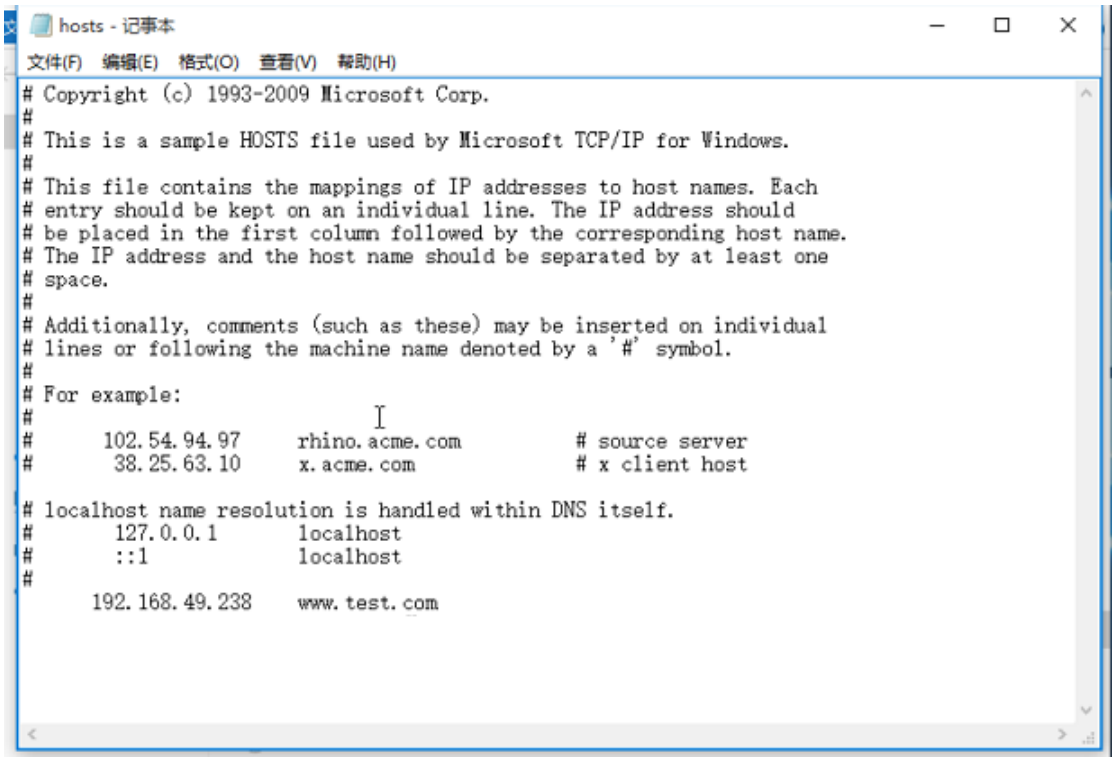

图 11

12. 打开浏览器，在地址栏中输入【www.test.com】，回车。出现网站主页面，说明 IP 地址与域名之间已经建立起映射。如图 12 所示。

图 12

13. 打开 win10_2。输入密码“123456”，首先进入到【C:\tools\Burpsuite】目录下，双击【BurpUnlimit】文件。如图 13 所示.

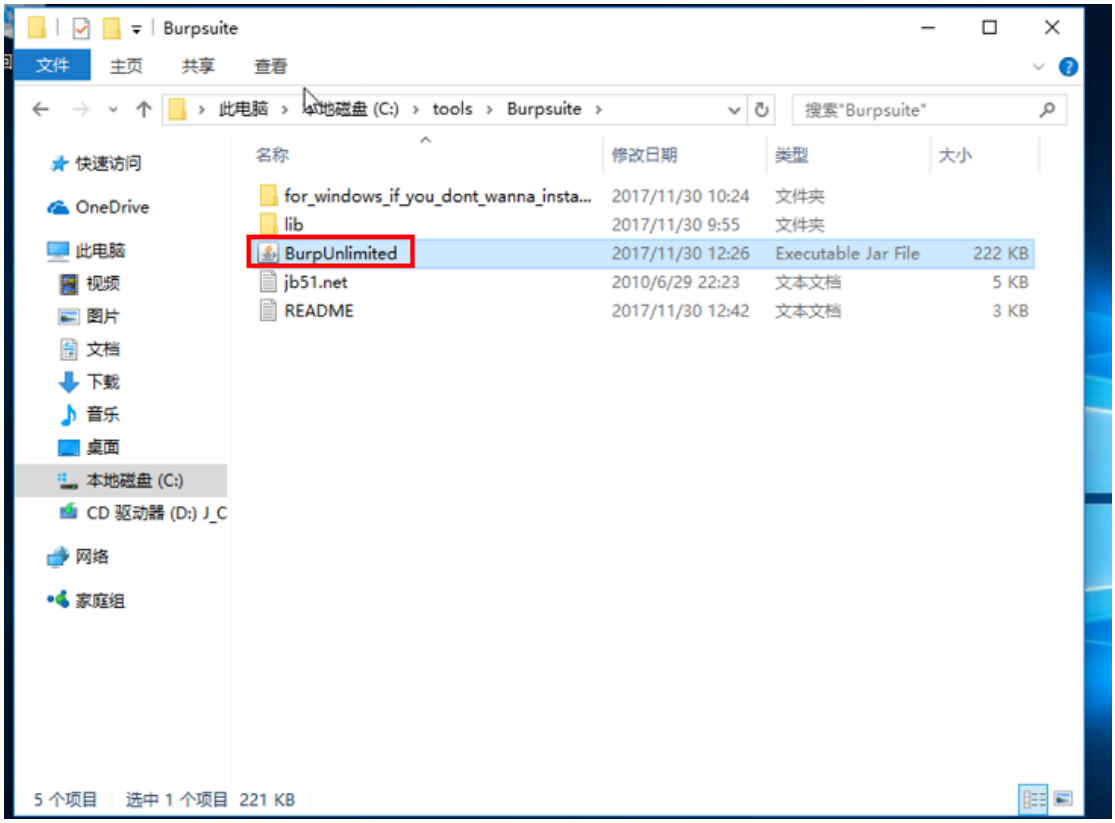

图 13

14. 选择【Temporary project】，点击【next】。如图 14 所示

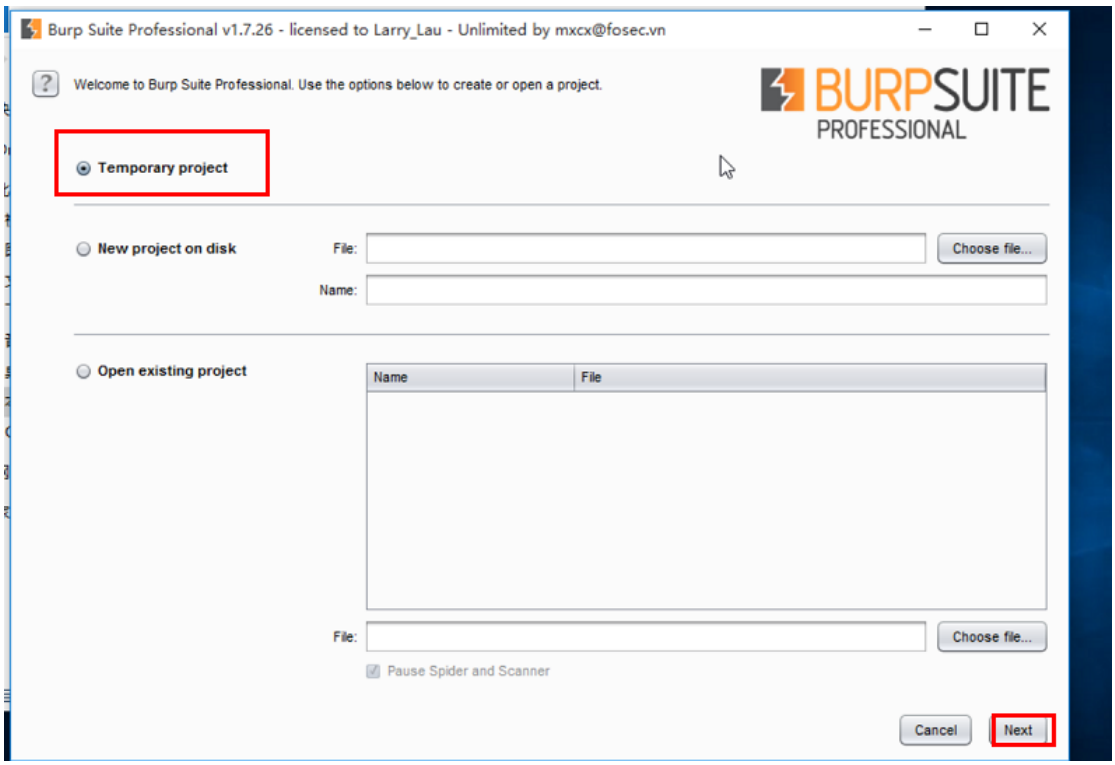

图 14

15. 选择【use Burp defaults】，点击【Start Burp】。如图 15 所示。

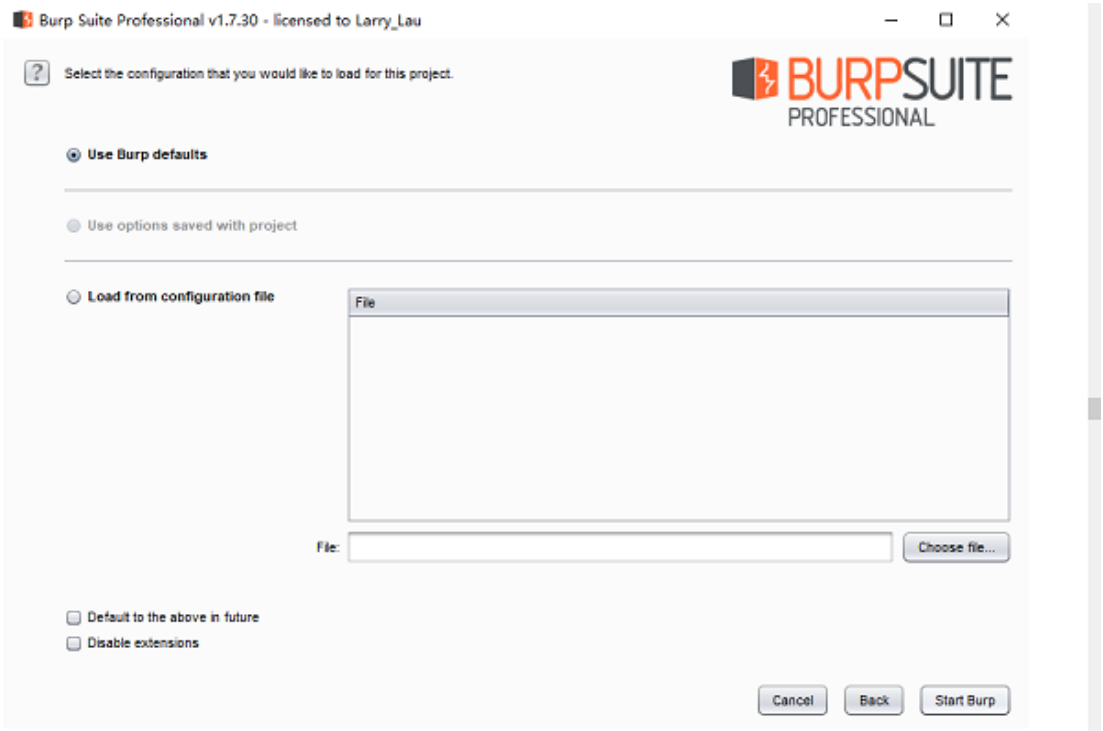

图 15

16. 进入主页面。如如图 16 所示。

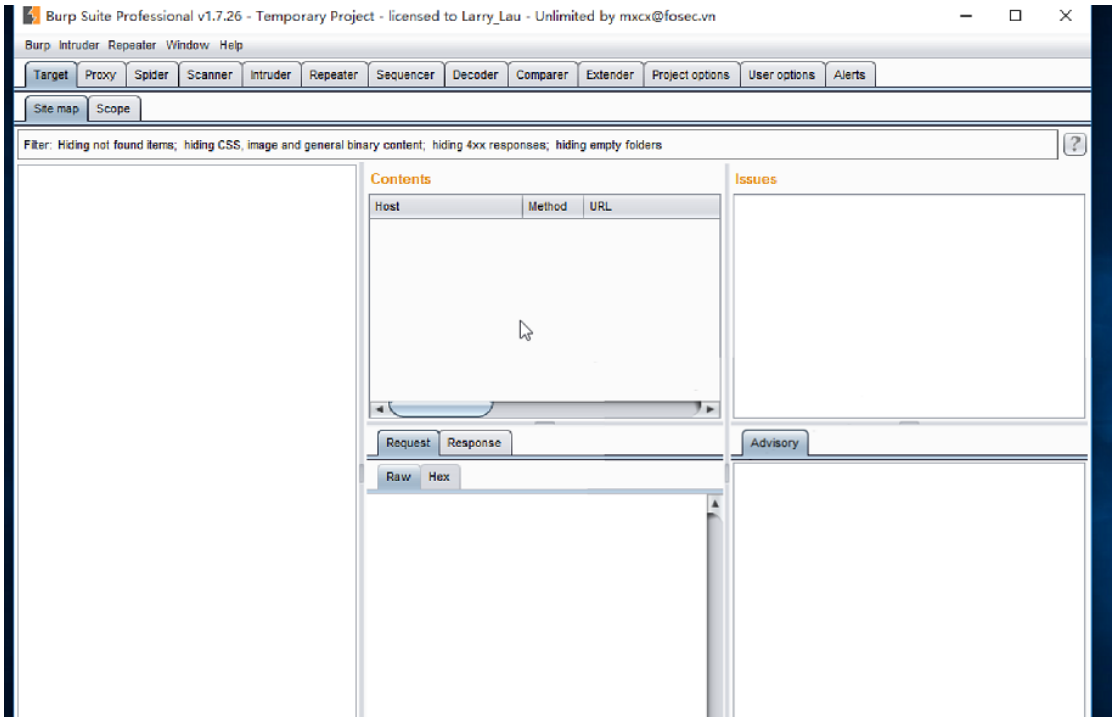

图 16

17. 进入路径【C:/windows/system32/drivers/etc】文件夹，双击 host 文件，以记事本形式打开。在最后一行加入网站 IP 地址与域名的映射【192.168.49.238　　www.test.com】。如图 17 所示。

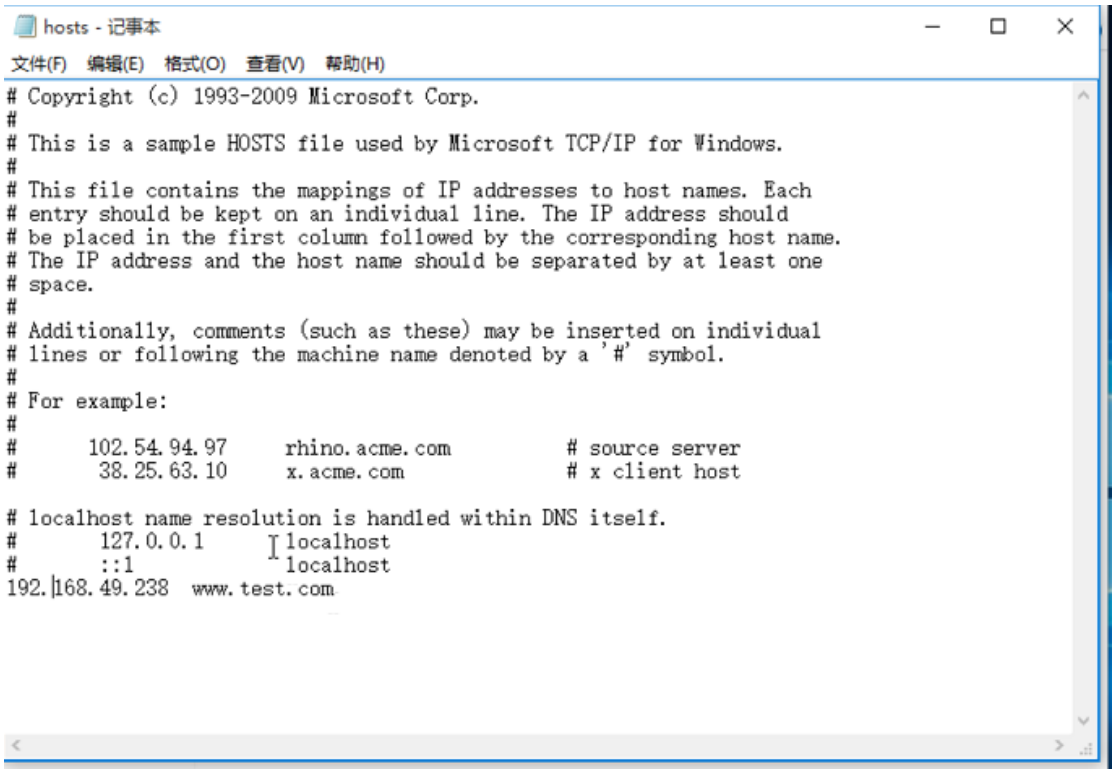

图 17

18. 设置代理，选择开始，点击桌面浏览器，在右上角选择【设置】，选择【Internet 选项】，如图 18 所示。

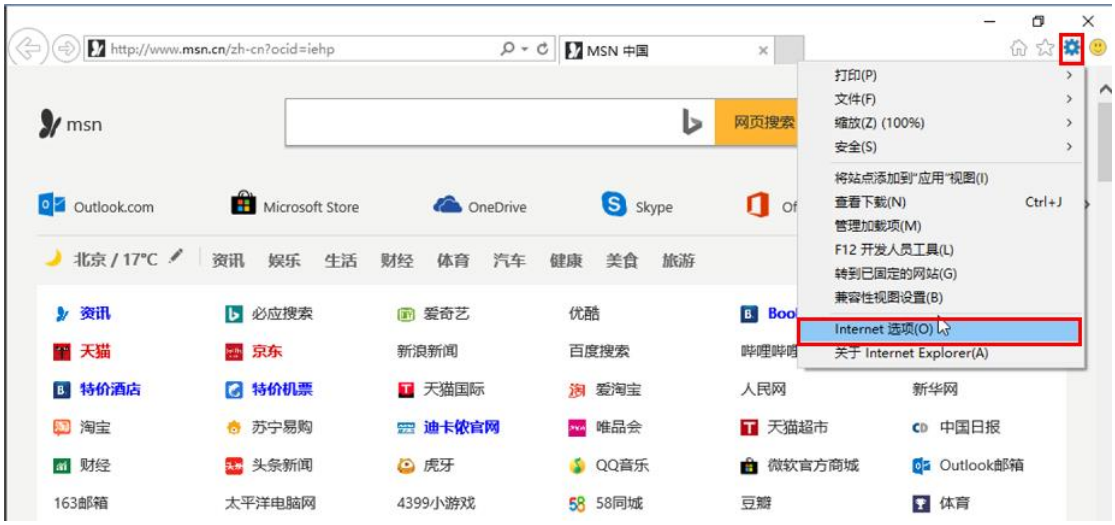

图 18

19. 打开【连接】选项卡，点击【局域网设置】。如图 19 所示。

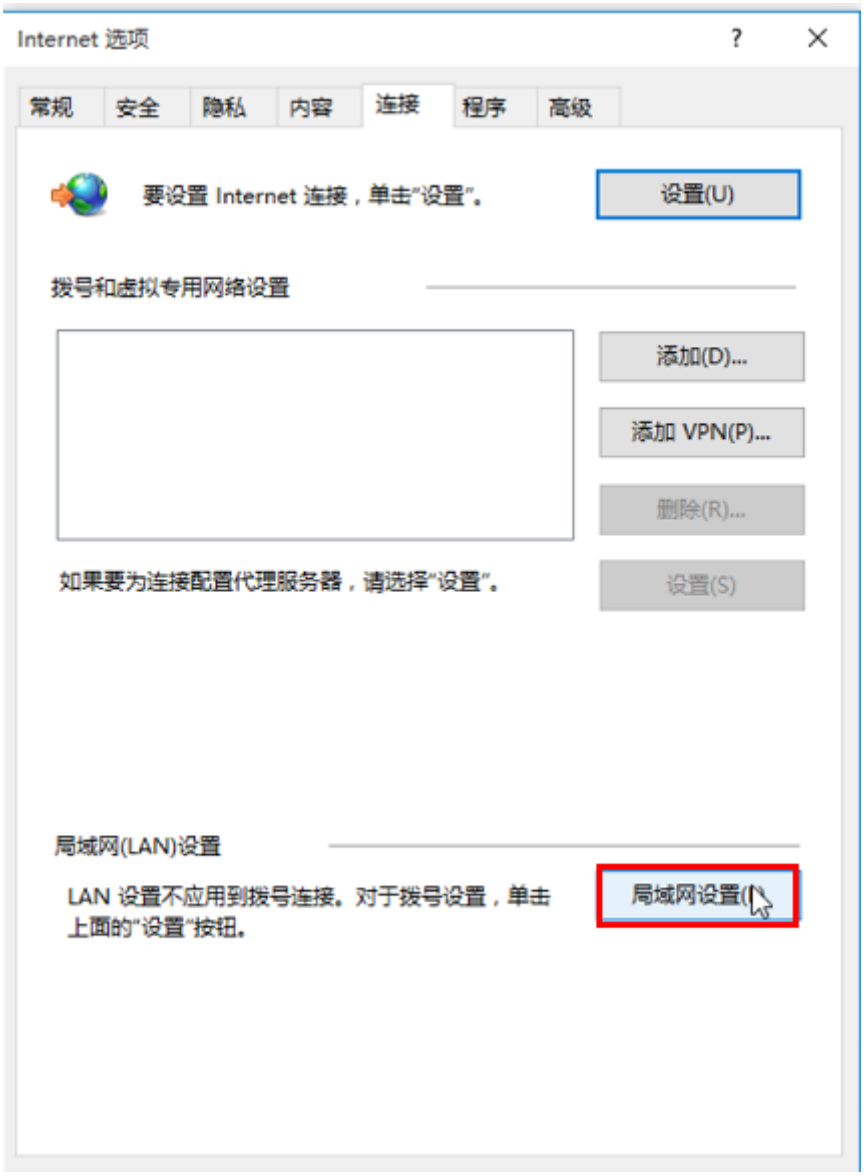

图 19

20. 配置代理服务器，勾选【为 LAN 使用代理服务器】，地址【127.0.0.1】，端口为【8080】。如图 20 所示。

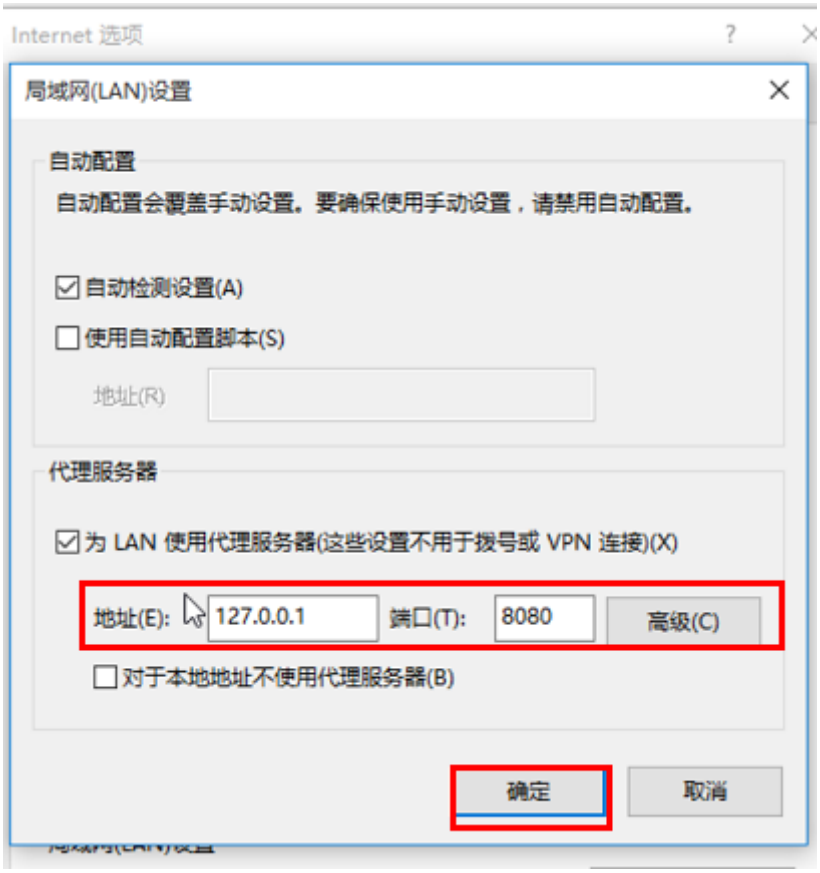

图 20

21. 打开 IE 浏览器，在地址栏中输入【www.test.com】远程访问网站主页面。如图 21 所示。

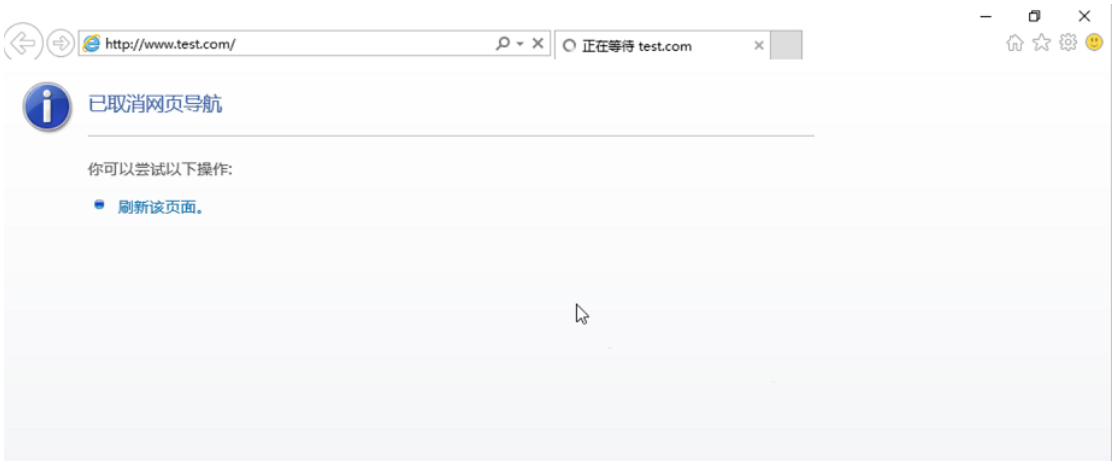

图 21

22. 在 Burp Suite 中，打开【Proxy】中的【Intercept】，出现如下界面（如果无内容则先点 intercept off，然后 intercept on，再次刷新 www.test.com），说明 Burp Suite 已经正常运行。(点击 Drop 可以找到“www.test.com”对应数据包)如图 22 所示。

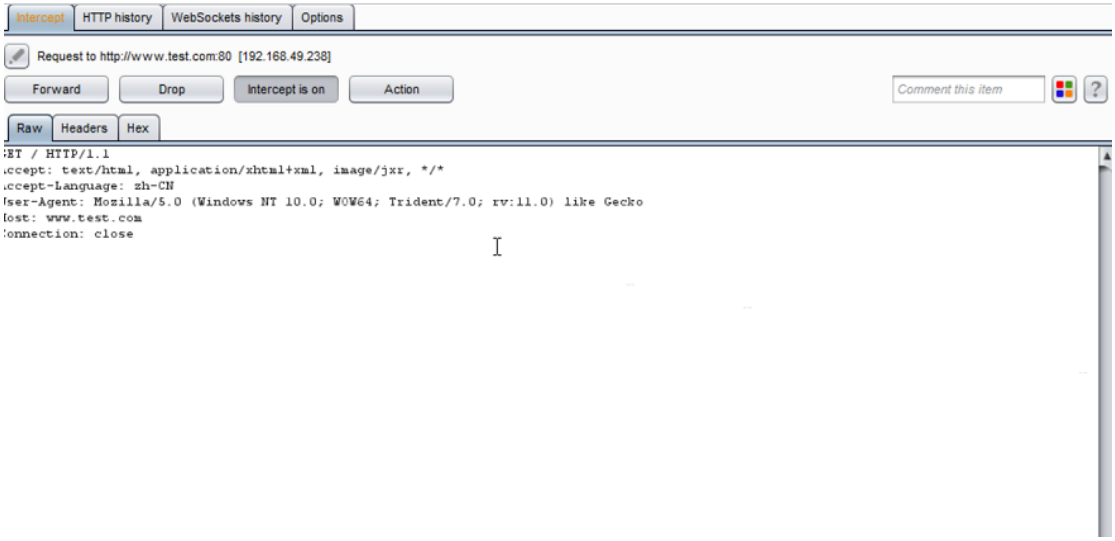

图 22

23. 在【Target】下的【Scope】选项可以设置具体的扫描范围。如图 23 所示

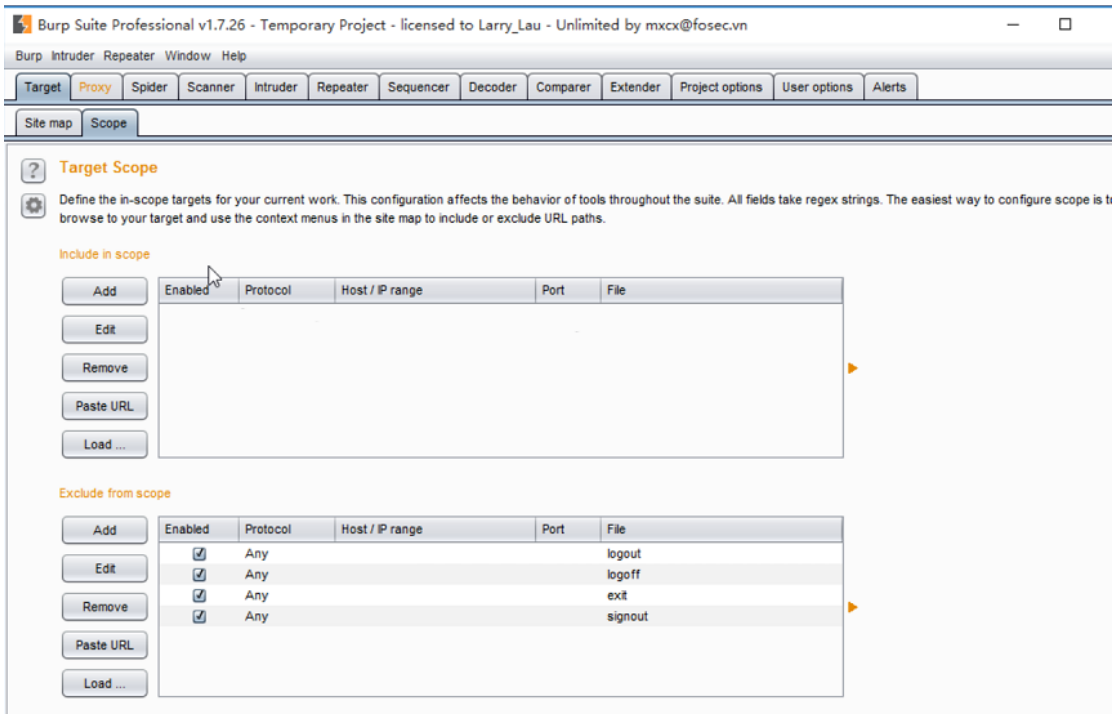

图 23

24. 右键单击【www.test.com】，选择【Spider this host】，作为蜘蛛爬取网页。（如果 site map 页面看不到域名则点击 proxy->HTTP history->找到 www.test.com，右键“add to scope”，如果还看不到请刷新网页）如图 24 所示。

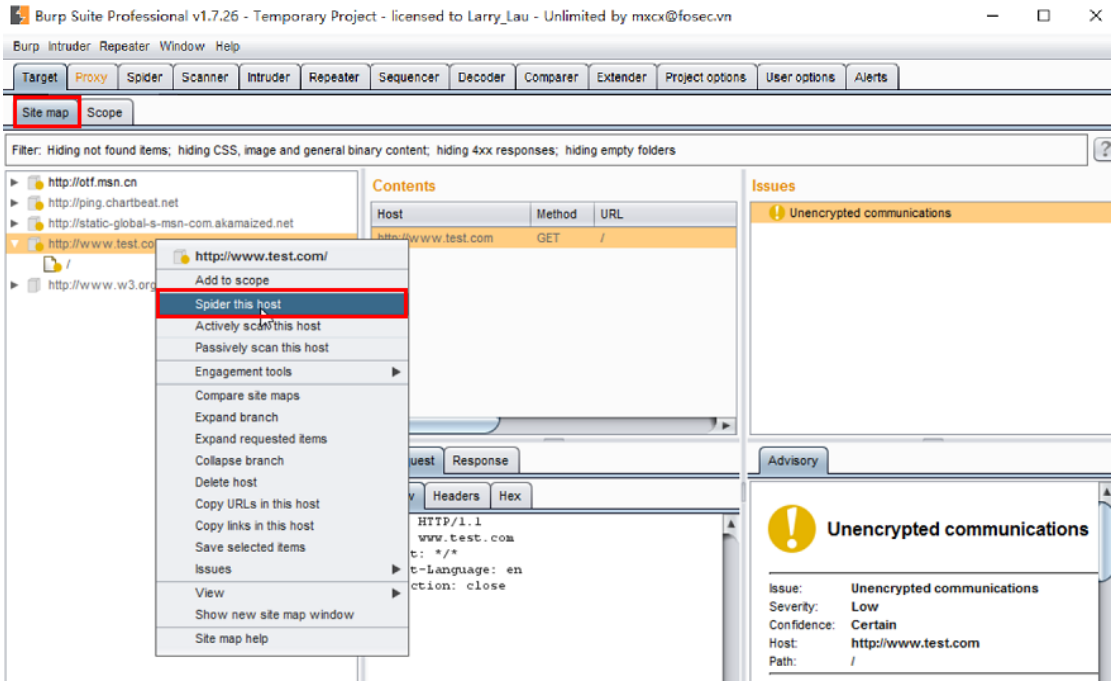

图 24

25. 打开【Spider】下的【Control】选项卡，页面中显示正在爬取的网页，已经请求数量，字节传输量，爬虫范围等信息。如图 25 所示。

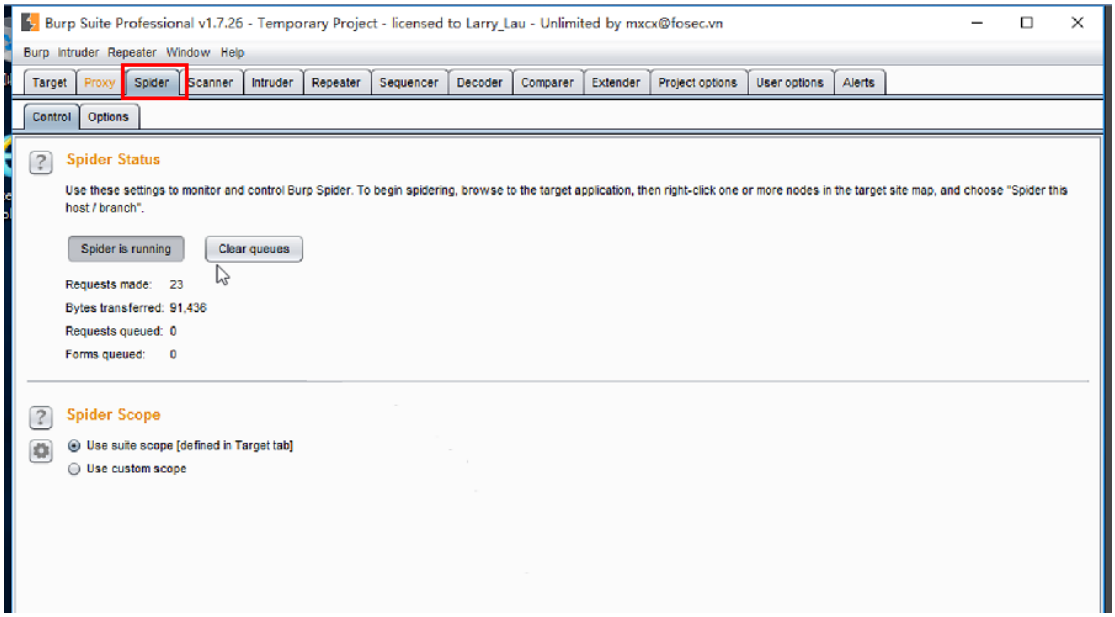

图 25

26. 右键单击【www.test.com】，选择【actively scan this host】，主动扫描网站。如图 26 所示。

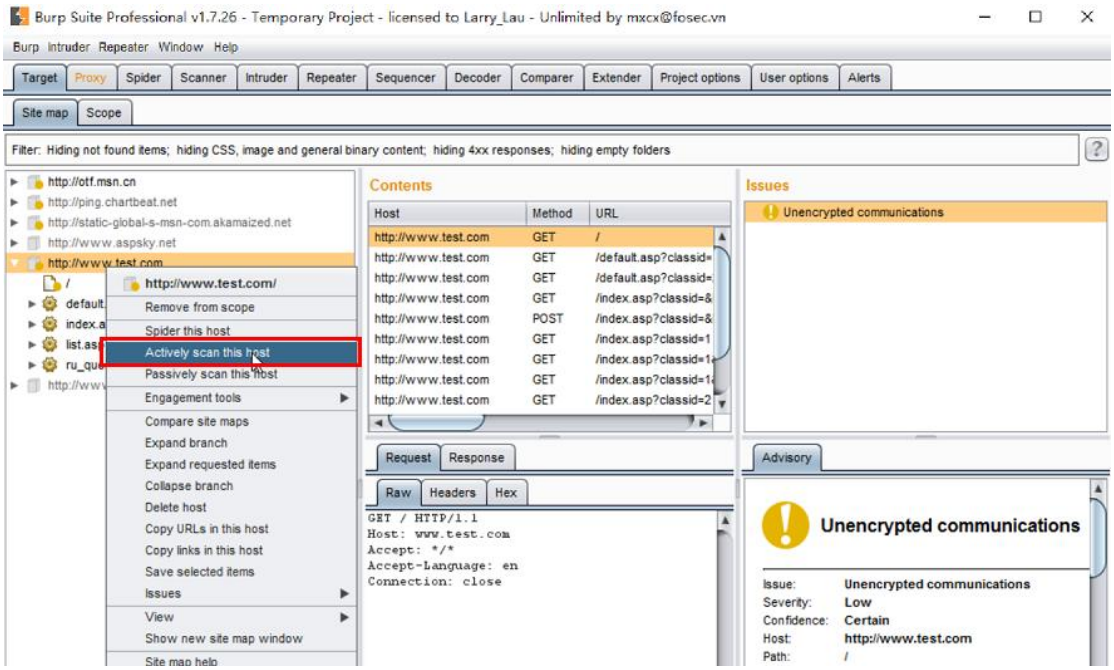

图 26

27. 页面中弹出主动扫描向导，会提示用户已经选择了一些项目来扫描，为了更有效的扫描，可以勾选上要去掉的项目，一般选择默认即可。如图 27 所示。

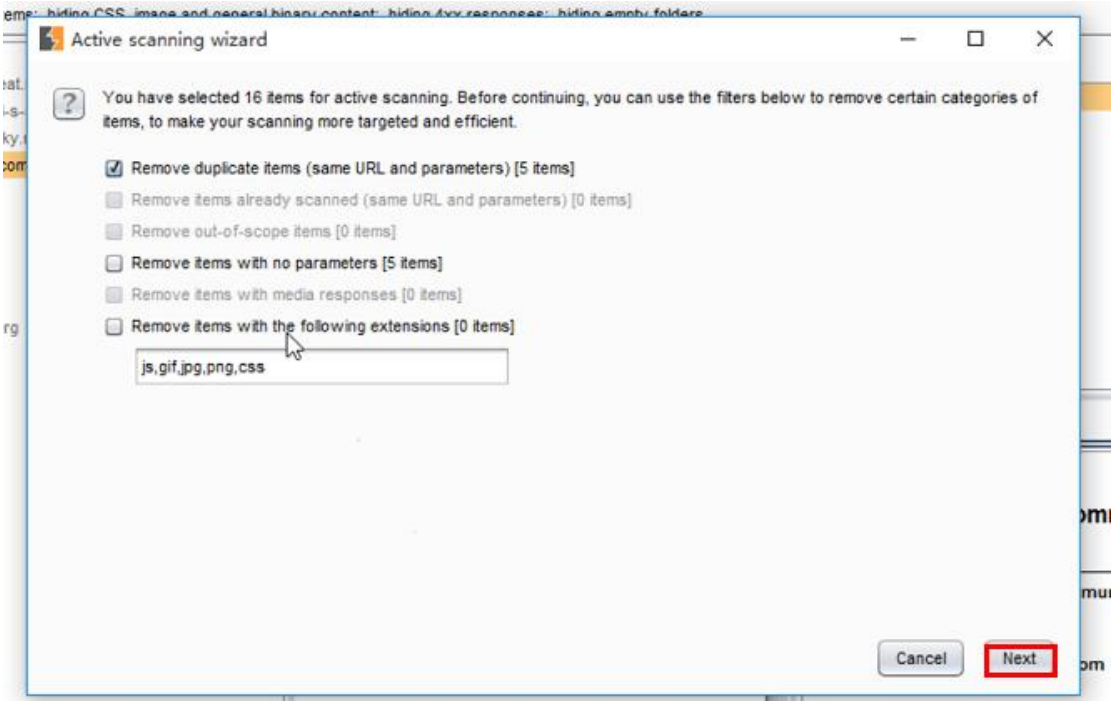

图 27

28. 选择【ok】，如图 28 所示。

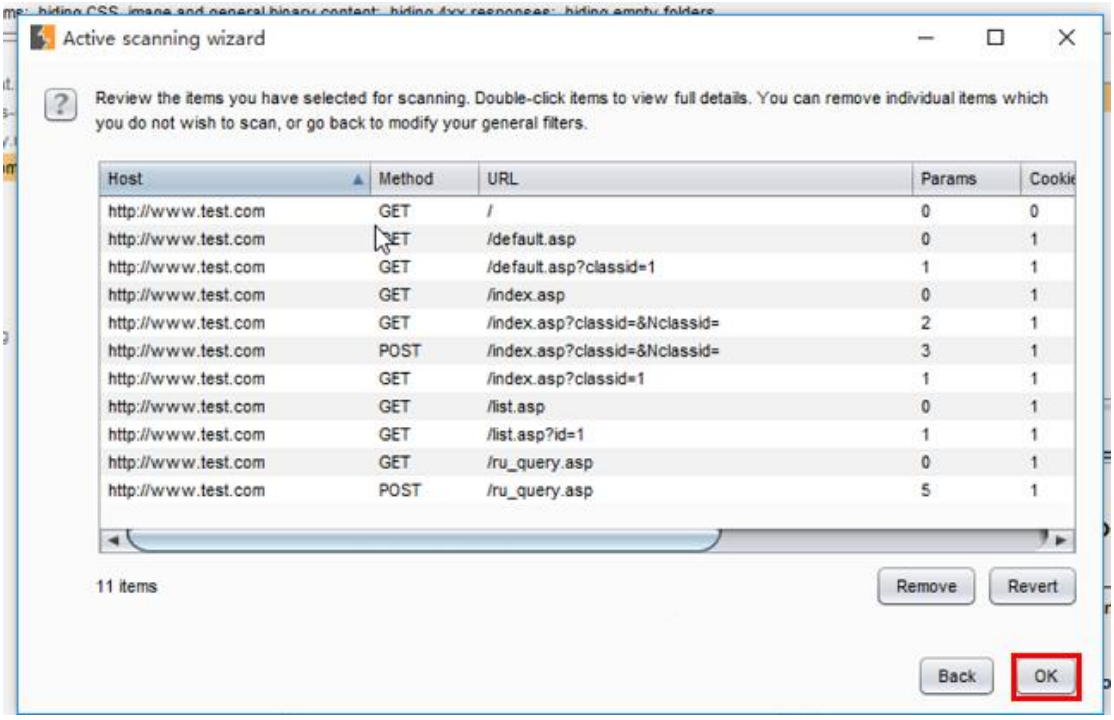

图 28

29. 在【Target】中的【site map】选项卡。就会看到当前网站正在扫描，网站注入，漏洞都会显示出来。如图 29 所示。

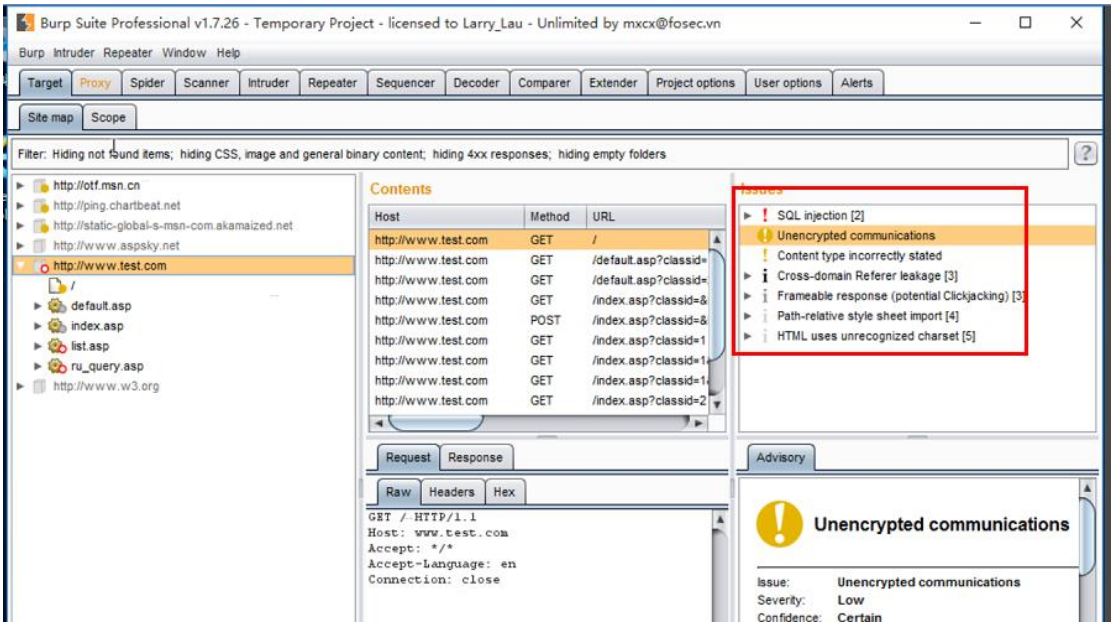

图 29

30. 扫描完成后，需要对漏洞进行详细的分析，可以选择相应的漏洞，然后在右下角的【advisory】里看到，可以看到漏洞名字、严重程度、确信程度、路径地址等信息。如图 30 所示。

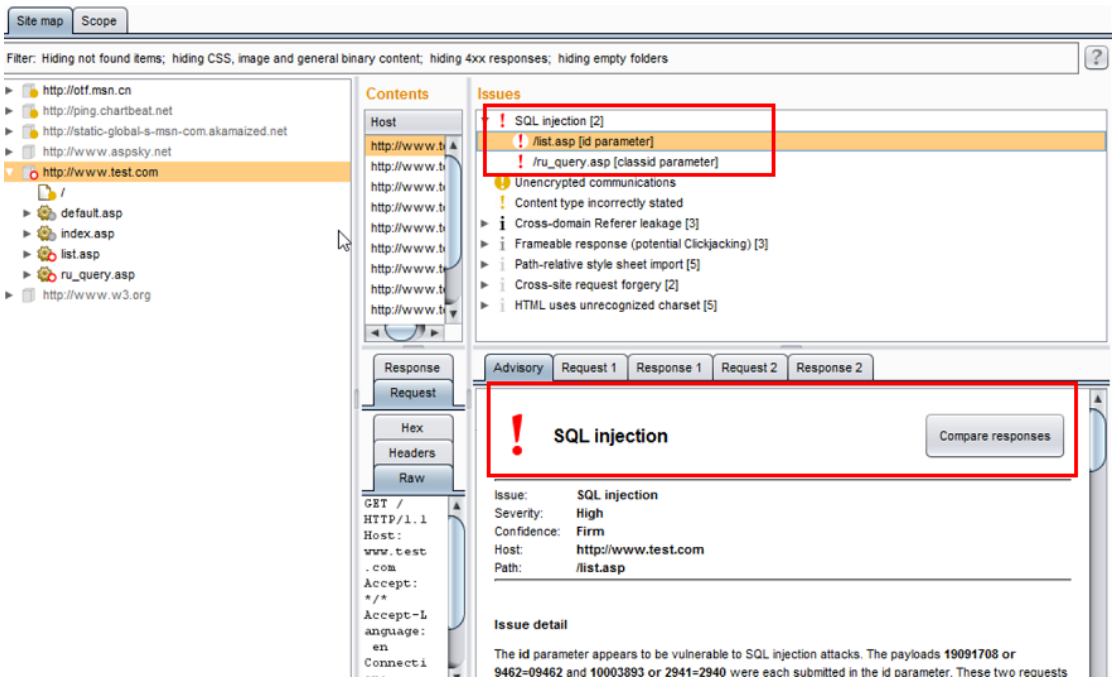

图 30

31. 可以通过这些信息详细了解被扫描网站的信息。

五【实验思考】

● 如何针对漏洞信息给出相应的解决措施？