



南开大学  
Nankai University

南 开 大 学

网 络 空 间 安 全 学 院

计算机网络实验报告

---

## 上机实验 2: web 服务器的实现与交互分析

---

姓名: 罗功成

学号: 1910487

年级: 2019 级

专业: 信息安全

指导教师: 张建忠 徐敬东

2021 年 11 月 13 日

## 摘要

在 Windows 下搭建一个 web 服务器 (iis)，在其中制作一个简单的页面，并进行交互分析说明。

**关键字：** IIS,html,wireshark

## 目录

一、 实验流程	1
(一) web 服务器搭建和页面制作 . . . . .	1
(二) 实验核心代码 . . . . .	2
(三) wireshark 的交互分析 . . . . .	3
二、 总结和收获	4

## 一、实验流程

## (一) web 服务器搭建和页面制作

- (1) 安装 iis 程序
- (2) 在 IIS 添加网站，然后写好对应的网站名字，物理地址处写好 html 所在文件夹的位置。
- (3) 在 dreamweaver 下编写对应的 html 文件，制作含有学号姓名专业的网页。

设置好服务器:

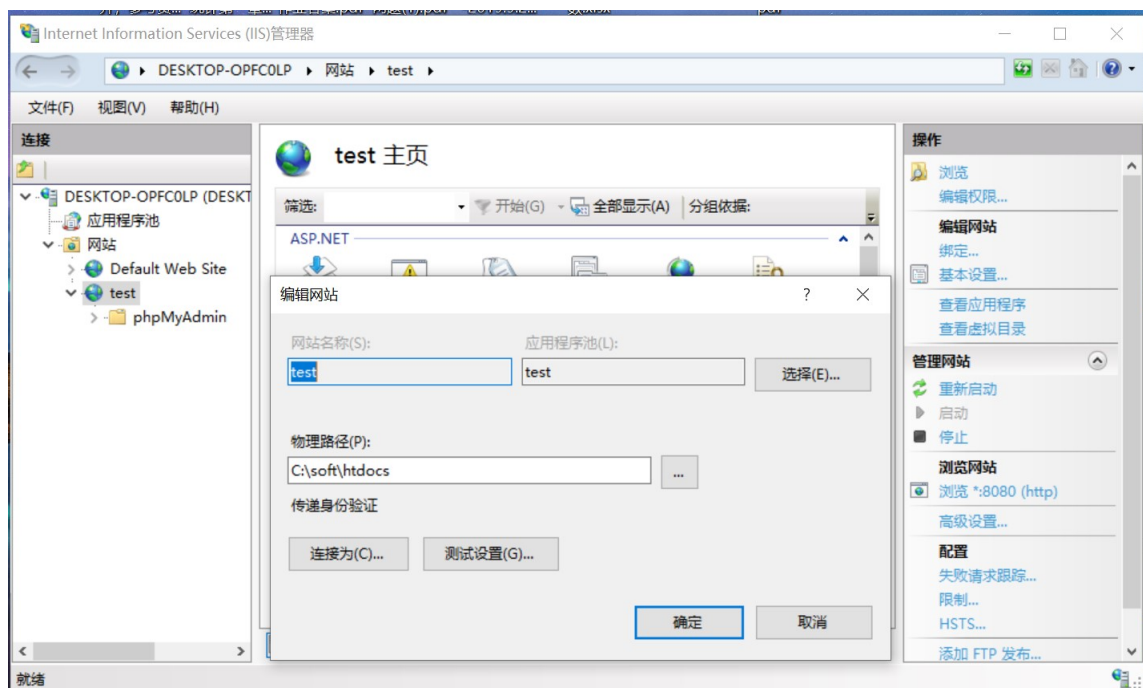


图 1: 服务器实现效果

点击浏览网站，进入目录浏览。

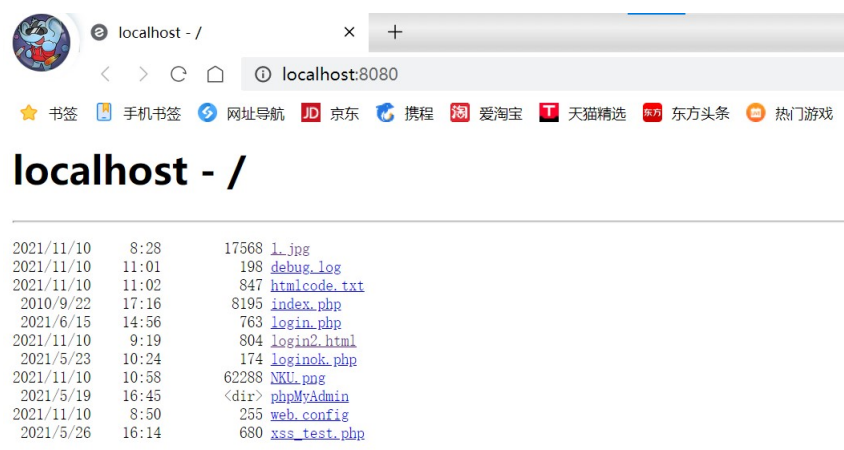


图 2: 目录浏览

点击制作的 HTML 文件处，可以看到制作的网页

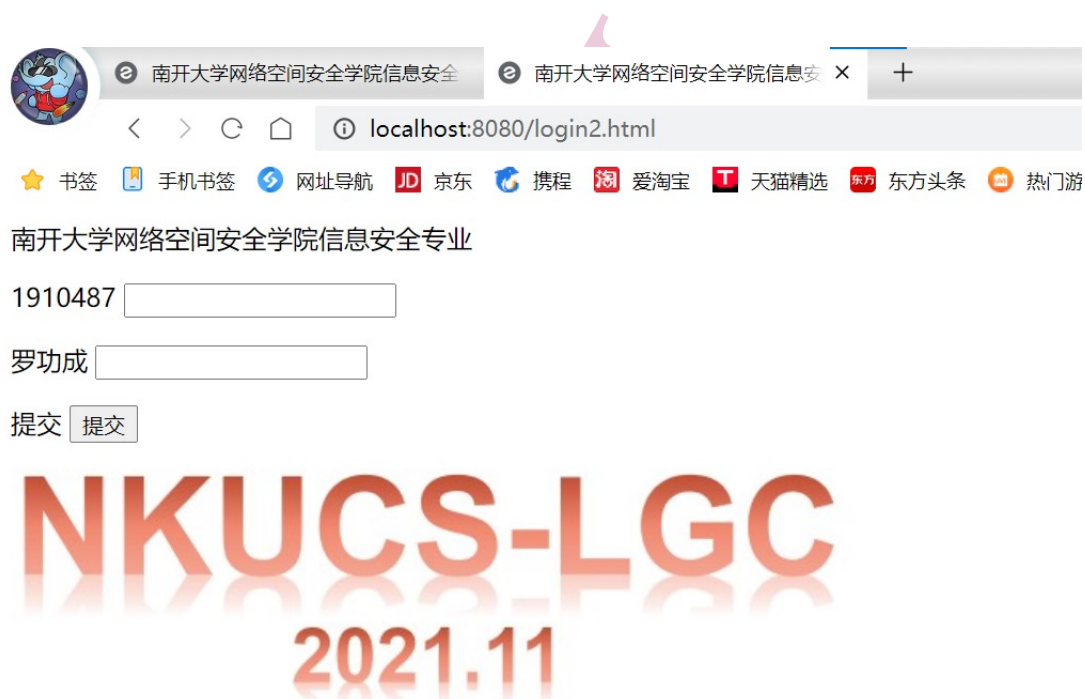


图 3: 页面实现效果

可见，在最后的网页中可以体现学号，姓名，专业，LOGO 等要求的信息。

## (二) 实验核心代码

一个简易的页面制作

```
1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3
   .org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
2 <html xmlns="http://www.w3.org/1999/xhtml">
3 <head>
4 <meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
5 <title>南开大学网络空间安全学院信息安全专业</title>
6 </head>
7
8 <body>
9 <form id="username" name="username" method="get" action="XSS.php">
10   <label>南开大学网络空间安全学院信息安全专业</label><p>
11   <label>1910487
12   <input name="username" type="text" id="username" />
13   </label>
14   <p>
15     <label>罗功成
16     <input name="password" type="password" id="password" />
17     </label>
18   </p>
19
20   <p>
21     <label>提交
22     <input type="submit" name="Submit" value="提交" />
23     </label>
24   </p>
25   
26 </form>
27 </body>
28 </html>
```



图 4: LOGO 设计

### (三) wireshark 的交互分析

再进入 wireshark 中，设置好 http 的过滤器后，可以看到下面的抓包结果。

488	41.086472	10.136.16.109	182.254.116.116	TCP	66 1837 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PE
489	41.096251	182.254.116.116	10.136.16.109	TCP	66 80 → 1837 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=
490	41.096379	10.136.16.109	182.254.116.116	TCP	54 1837 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
491	41.096835	10.136.16.109	182.254.116.116	HTTP	182 GET /d?dn=806810eb3f3c79c09fb6185772dad974&id=2046&ttl=1 HTTP
492	41.103575	182.254.116.116	10.136.16.109	HTTP	206 HTTP/1.1 200 OK (text/html)
493	41.103576	182.254.116.116	10.136.16.109	TCP	60 80 → 1837 [FIN, ACK] Seq=153 Ack=129 Win=65664 Len=0
494	41.103707	10.136.16.109	182.254.116.116	TCP	54 1837 → 80 [ACK] Seq=129 Ack=154 Win=131072 Len=0
495	41.104193	10.136.16.109	182.254.116.116	TCP	54 1837 → 80 [FIN, ACK] Seq=129 Ack=154 Win=131072 Len=0
499	41.114512	182.254.116.116	10.136.16.109	TCP	60 80 → 1837 [ACK] Seq=154 Ack=130 Win=65664 Len=0

图 5: wireshark 抓包 (1)

简要分析:

(1) 三次握手: 首先由客户端发送连接请求【SYN】, 当服务器接收到来自客户端的 SYN 时, 将会发出 SYN 来请求客户端连接, 并且发出确认接受到了 SYN 的 ACK 指令; 最后客户端收到服务器的 SYN 后再向服务器发送 ACK 确认, 最后完成三次握手, 实现了客户端和服务器的连接。

(2) 信息传送: 建立连接后, 以 HTTP1.1 协议下 get 方式向对应的网页请求获取页面包含信息, 由于文件中包含文本, 所以显示出 text 表明接收到了文本消息, 同理, get 1.png 也表明接收到了设计的 logo 图片。

在 HTTP1.1 下, 用 get 的方式获取页面中 logo 图片。

10645	91.315920	120.220.173.52	10.130.112.170	TCP	66 80 → 11454 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SA
10646	91.315987	10.130.112.170	120.220.173.52	TCP	54 11454 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
10647	91.316262	10.130.112.170	120.220.173.52	HTTP	225 GET /zlj/k/one.png HTTP/1.1
10648	91.322114	10.130.112.170	111.30.159.178	TCP	234 [TCP segment of a reassembled PDU]

图 6: wireshark 抓包 (2)

(3) 四次挥手: 从客户端发出希望断开连接的 FIN 请求, 并开始等待服务器的响应; 当服务器接收到对应的 FIN 后, 将发出 ACK 确认收到, 此时, 客户端继续等待, 等到服务器再次发送服务器回传数据结束后发出 FIN 断开连接请求, 以及第二次的 ACK 确认后, 客户端将会结束等待状态, 随后向服务器发送 ACK 确认收到了 FIN, 之后客户端断开连接, 服务器在接收到客户端的 ACK 后也将会断开连接。至此完成了四次挥手, 实现了客户端和服务器的连接断开。

## 二、 总结和收获

1. 熟悉和回顾了页面制作 (HTML 等), web 服务器 (IIS) 搭建, wireshark 等相关知识。
2. 用户端和服务端之间的交互过程有了更深入的了解。
3. 对于 TCP 的三次握手和四次挥手部分知识得到了学习和提高, 同时通过抓包分析, 得到了文本信息和图片信息的传输方式。