**网络安全实训 搭建简单的Web站点**

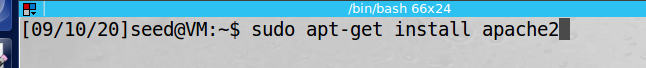
**实验一 HTTP基础**

**57118135**

**许皓钦**

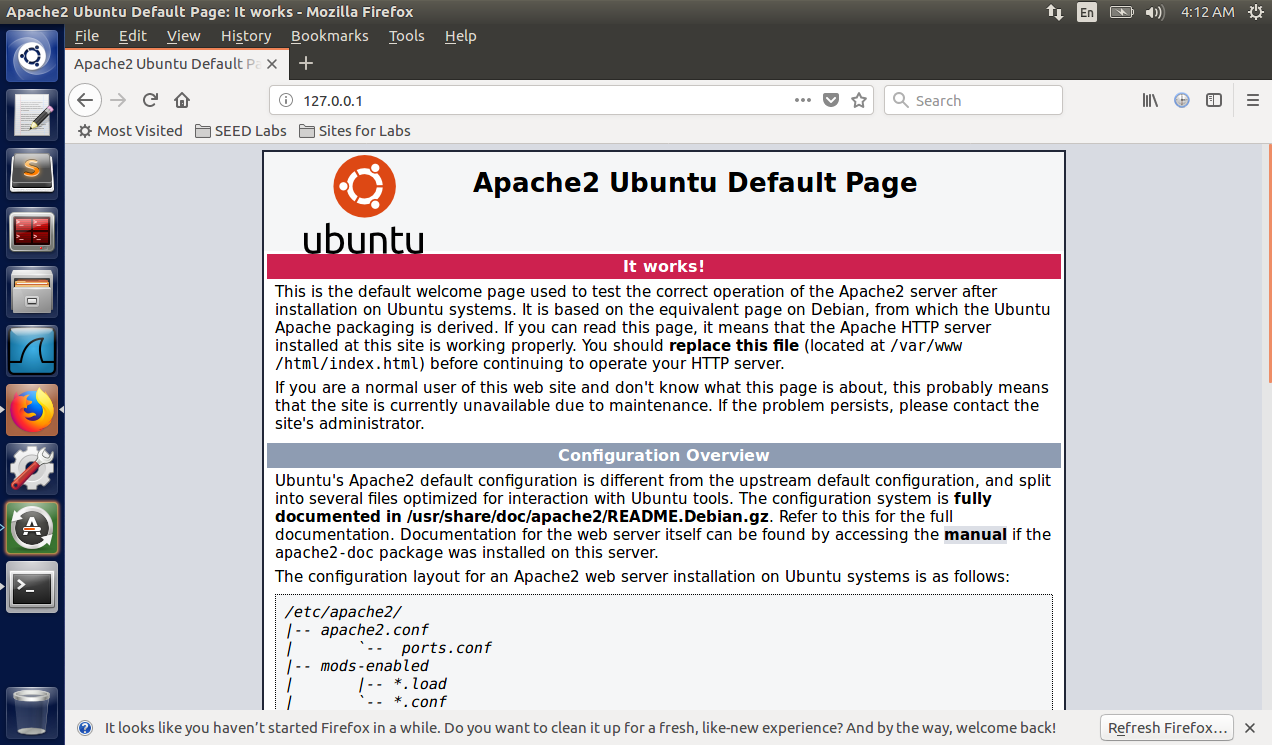
**任务一：安装apache服务器 并用简单页面验证**

步骤 1：在虚拟机中打开terminal终端窗口，输入sudo apt-get install apache2



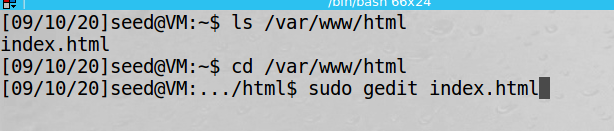
输入root用户密码，即可完成安装，提问到发现新版本是否修改配置文件，选择N

步骤 2：Apache安装完成后，默认的网站根目录是”var/www/html”，在网站根目录路径下有一个index.html文件，在本机或虚拟机浏览器中输入”127.0.0.1”就可以打开该页面。

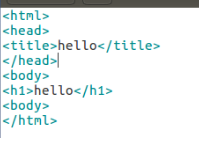


步骤 3：

1.cd /var/www/html

2.使用sudo gedit index.html指令打开index.html并进行编写（可自己进对应文件夹查看文件是否存在，www文件夹被隐藏，图形化界面需要ctrl+H显示被隐藏的文件，而使用terminal界面则默认可查看所有文件，如下图）

编写内容如下，内容随意



<html>

<head>

<title>hello</title>

</head>

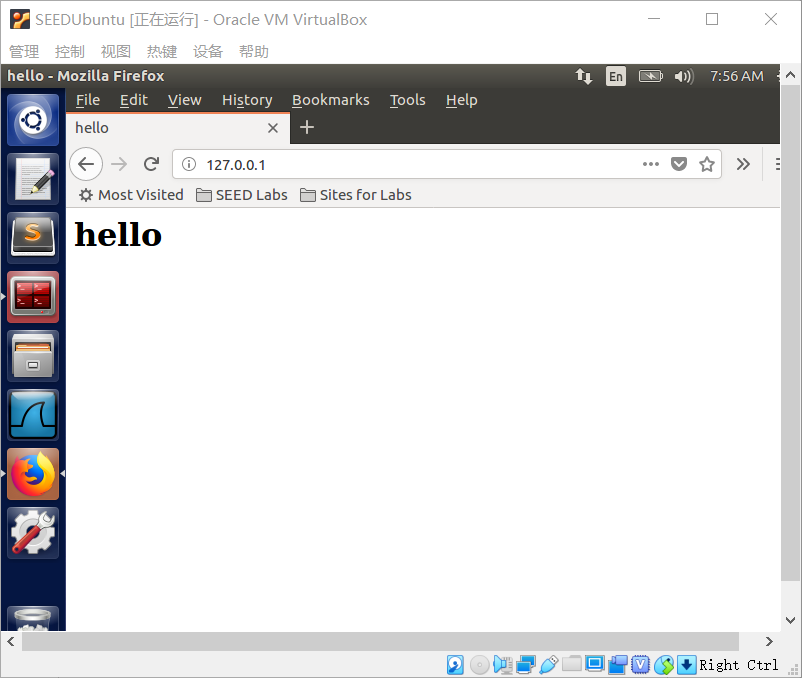
<body>

<h1>hello</h1>

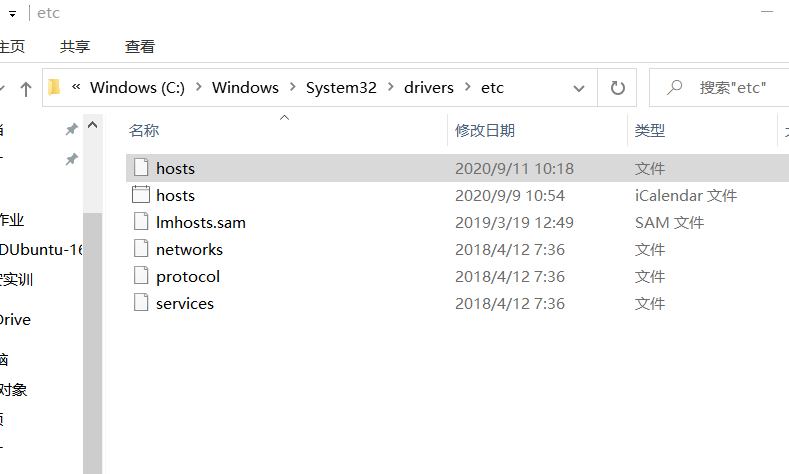
<body>

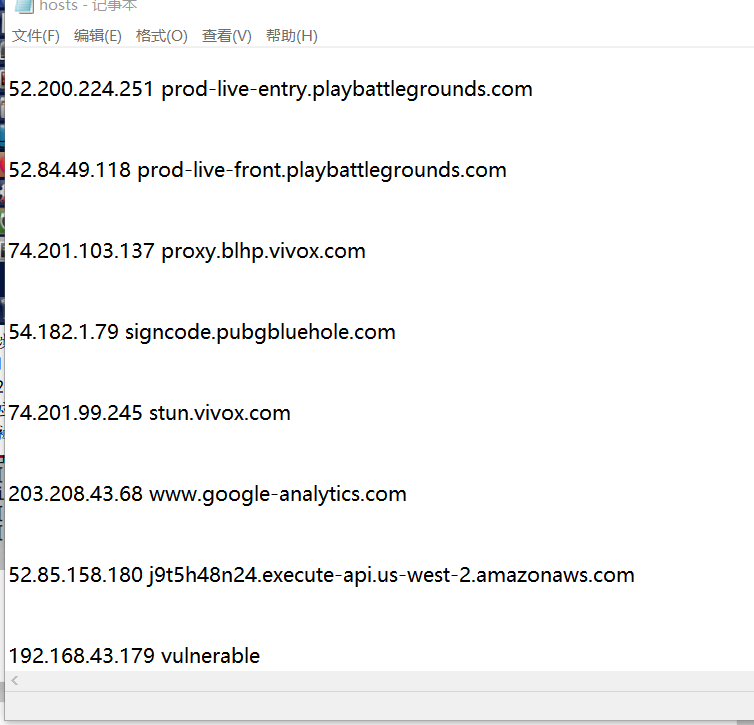
</html>

**步骤 4：修改后使用浏览器登录127.0.0.1，页面更改为新主页。**

**任务二：通过host文件解析名称**

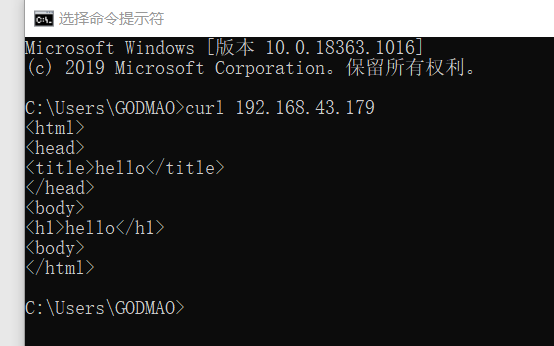
步骤 1： 在windows主机中找到hosts文件记事本打开，**修改hosts文件加入虚拟机ip地址与主机名vulnerable并保存**（C:\Windows\System32\drivers\etc）





**任务三：编写HTTP客户端，使用http库检索站点的主页**

步骤1：windows主机中输入curl+虚拟机ip地址可查看编写的index文件内容

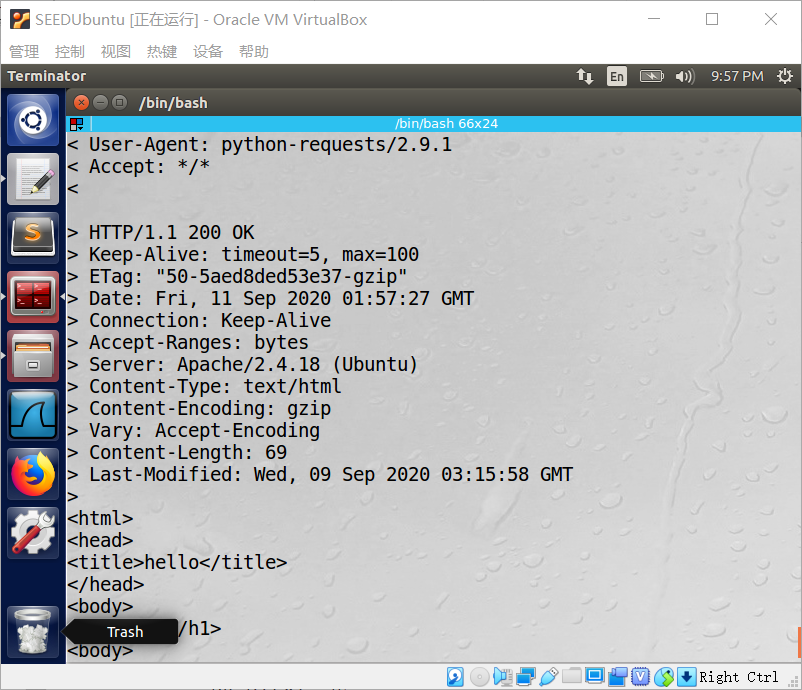


步骤2：虚拟机中输入python3 --version 查看虚拟机是否有python3.5

步骤3：创建.py的python执行文件（新建document，用gedit进行编辑，编辑结束重命名为xxx.py）

步骤4：命令行转到文件所在位置（可以右键properties查看），输入命令

python3 test.py 得到信息如下



**任务四：编写HTTP客户端以使用套接字检索站点的主页，代码如下：**

步骤1：在主机创建c语言程序，写入如下代码

#include <stdio.h>

#include <stdlib.h>

#include <string.h>

#include <iostream>

#include <winsock2.h>

#include<time.h>

#pragma comment(lib,"ws2\_32.lib")

void ReadPage(char\* host)

{

WSADATA data;

//winsock版本2.2

int err = WSAStartup(MAKEWORD(2, 2), &data);

if (err)

return;

//用域名获取对方主机名

struct hostent \*h = gethostbyname(host);

if (h == NULL)

return;

//IPV4

if (h->h\_addrtype != AF\_INET)

return;

struct in\_addr ina;

//解析IP

memmove(&ina, h->h\_addr, 4);

LPSTR ipstr = inet\_ntoa(ina);

//Socket封装

struct sockaddr\_in si;

si.sin\_family = AF\_INET;

si.sin\_port = htons(80);

si.sin\_addr.S\_un.S\_addr = inet\_addr(ipstr);

int sock = socket(AF\_INET, SOCK\_STREAM, IPPROTO\_TCP);

connect(sock, (SOCKADDR\*)&si, sizeof(si));

if (sock == -1 || sock == -2)

return;

//发送请求

char request[1024] = "GET /?st=1 HTTP/1.1\r\nHost:";

strcat(request, host);

strcat(request, "\r\nConnection:Close\r\n\r\n");

int ret = send(sock, request, strlen(request), 0);

//获取网页内容

FILE \*f = fopen("recieved.txt", "w");

int isstart = 0;

while (ret > 0)

{

const int bufsize = 1024;

char\* buf = (char\*)calloc(bufsize, 1);

ret = recv(sock, buf, bufsize - 1, 0);

printf(buf);

fprintf(f, "%s", buf);

free(buf);

}

fclose(f);

closesocket(sock);

WSACleanup();

printf("读取网页内容成功，已保存在recieved.txt中\n");

return;

}

void main() {

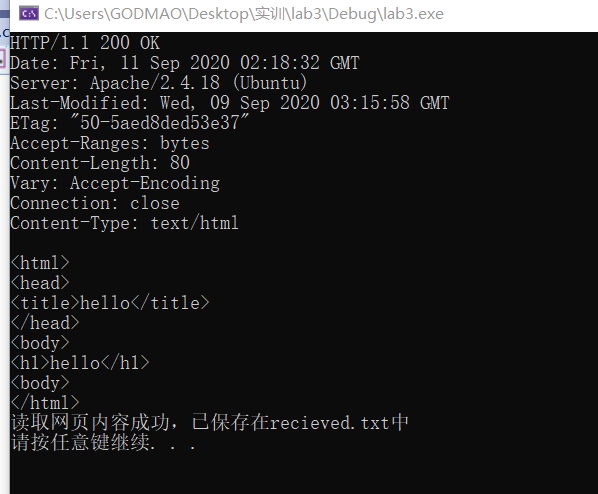
char\* str = "vulnerable";

ReadPage(str);

system("pause");

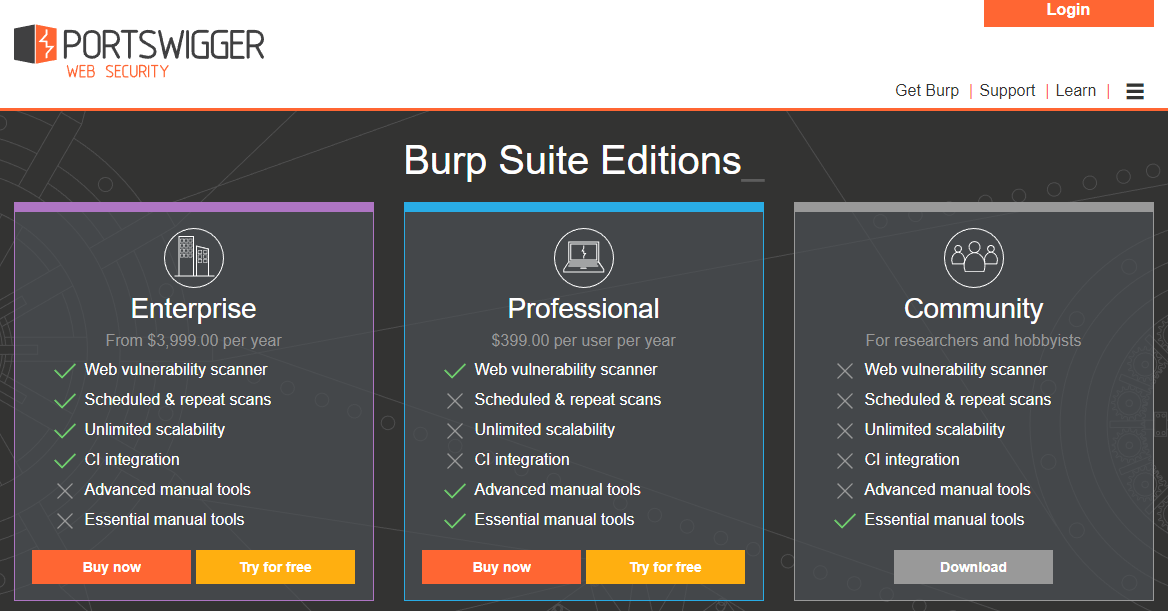
}

步骤2：执行该文件，查看网页定向是否正确



**任务五：下载软件Burp Suite并访问网站查看请求与响应的信息**

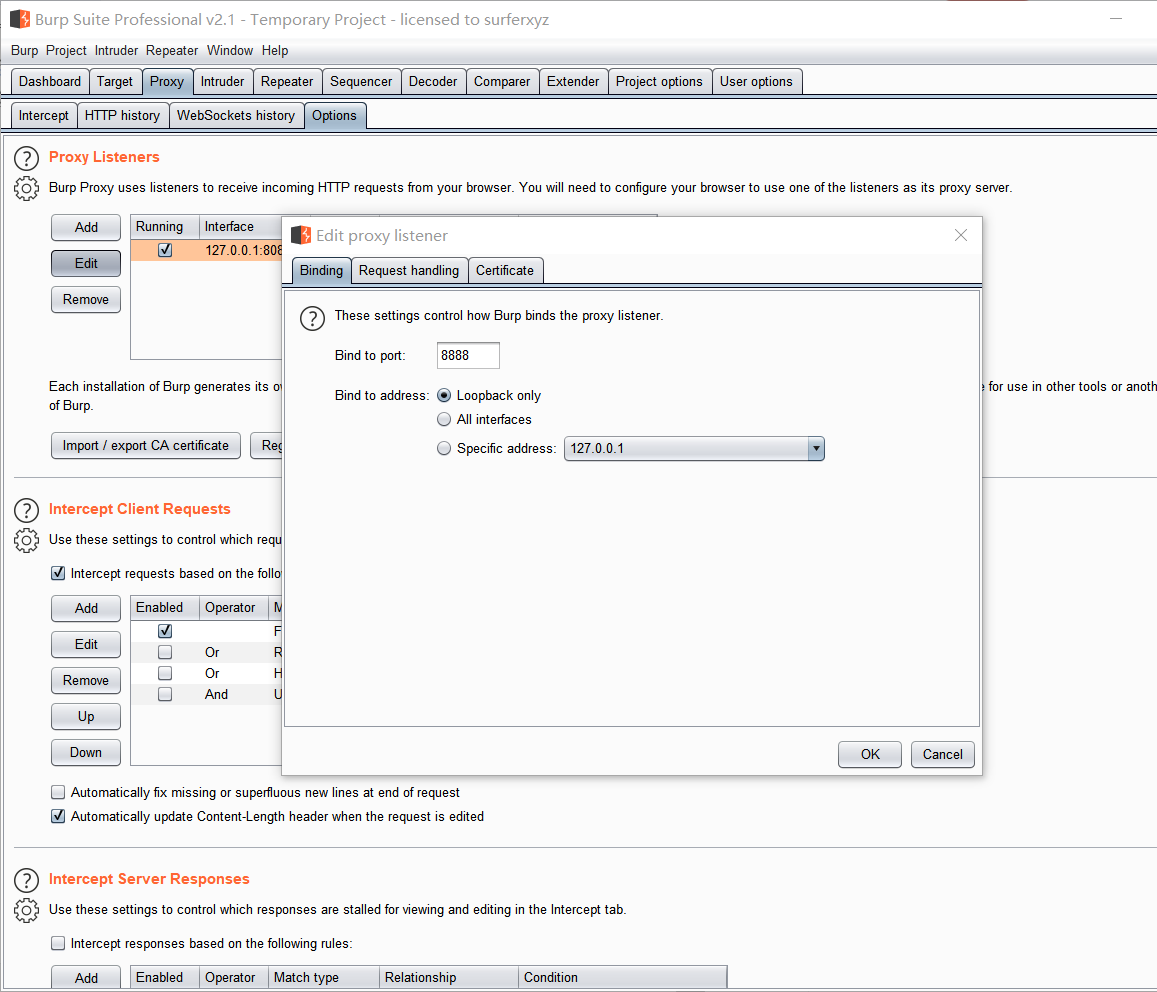
步骤 1：从<https://portswigger.net/burp>网站中下载Comuunity版本



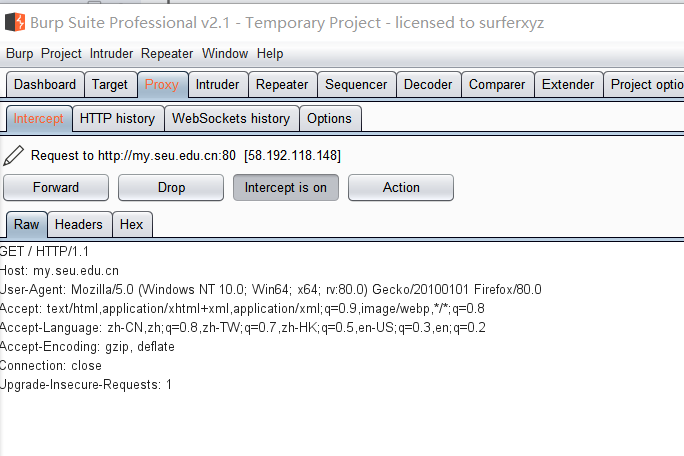
步骤 2：对测试浏览器Chrome进行代理设置,地址设为127.0.0.1,端口修改为8888



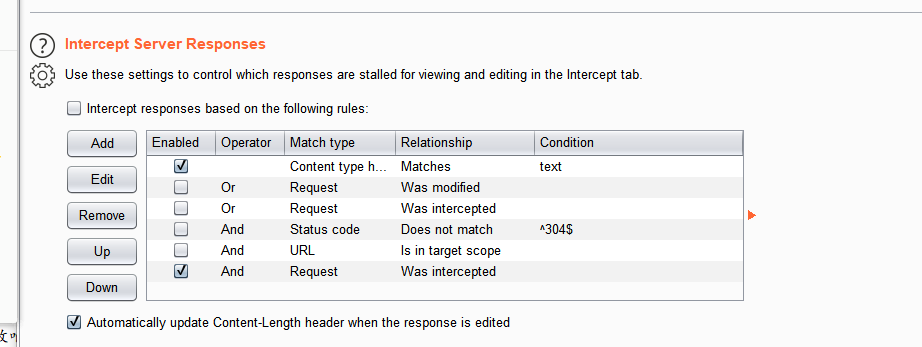
步骤 3：打开Burp Suite界面，设置Proxy代理，端口改为8888（需安装CA安全证书）



步骤 4：使用浏览器打开my.seu.edu.cn查看拦截情况（使用open browser按钮打开浏览器，输入网址后下图会有类似的信息，如果不是对应的地址，请点击forward/drop选择找到响应的my.seu.edu.cn的信息）



步骤 5：



步骤 6：测试CSDN通过发送验证码找回密码功能，查看Request和Response功能(网站进行访问时需要点击forward按钮才能不断发送请求与接收响应，在测试CSDN之前需要对网页进行多次访问，因此可以先关闭拦截，点击Intercept is on按钮进行关闭，在需要拦截时再打开)

