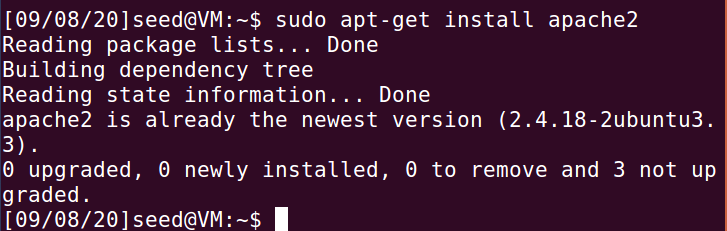
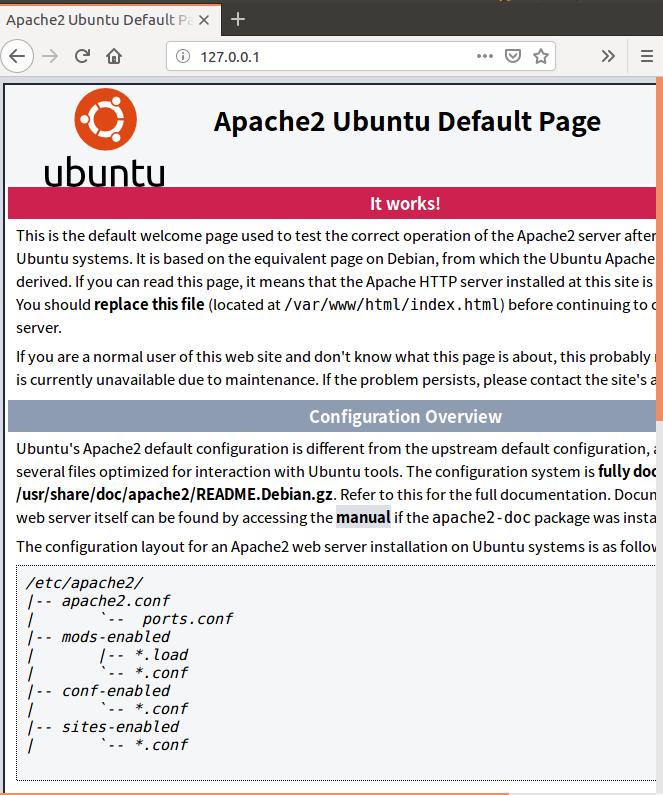
**实验一 HTTP基础**

任务一：安装apache服务器 并用简单页面验证

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

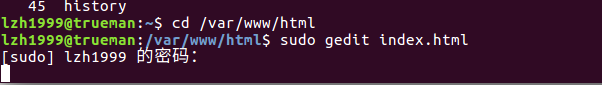


Apache安装完成后，在虚拟机浏览器中输入”127.0.0.1”，成功打开该页面。



在终端输入 cd /var/www/html；

然后使用sudo gedit index.html指令打开index.html（如下）





将其中内容改为：

<html>

<head>

<title>hello</title>

</head>

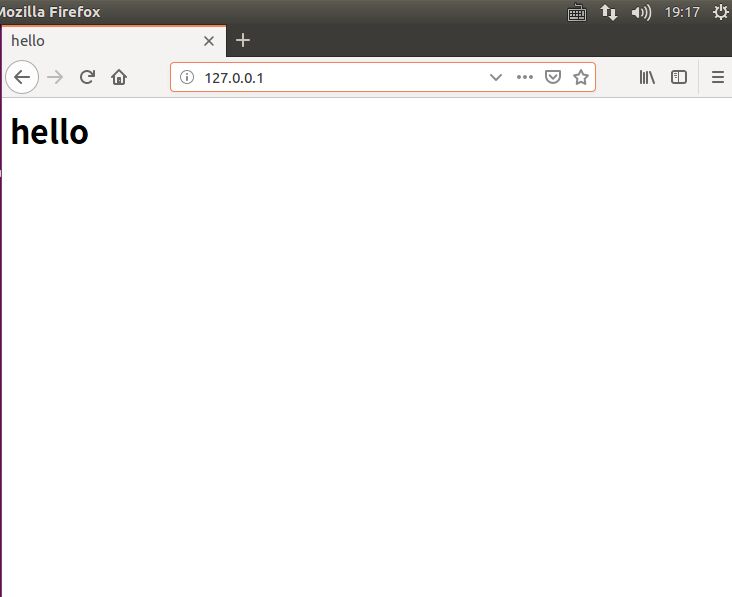
<body>

<h1>hello</h1>

<body>

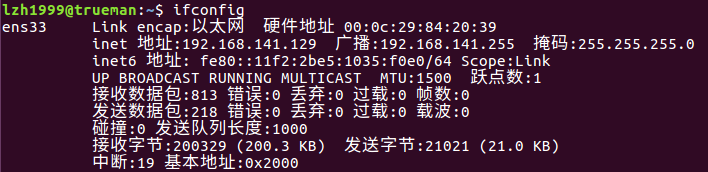
</html>

修改后使用浏览器登录127.0.0.1，页面更改为新主页。

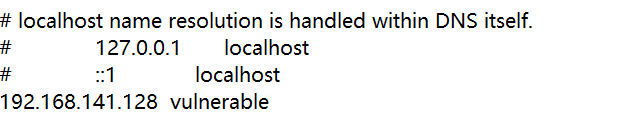


任务二：通过host文件解析名称

用ifconfig命令查看虚拟机ip地址（192.168.141.129）。

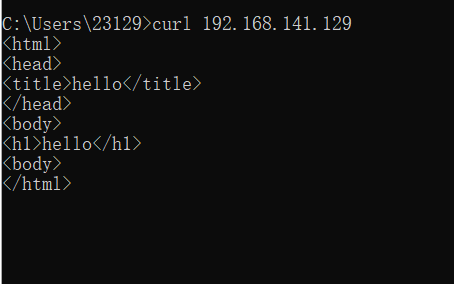


在windows主机中找到hosts文件记事本打开，修改hosts文件加入虚拟机ip地址与主机名vulnerable并保存（C:\Windows\System32\drivers\etc）



任务三：编写HTTP客户端，使用http库检索站点的主页

windows主机中输入curl+虚拟机ip地址（192.168.141.129）可查看编写的index文件内容



虚拟机中输入命令python3 --version 查看到本虚拟机有python3.5。

IMG_256

任务四：编写HTTP客户端以使用套接字检索站点的主页

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() {

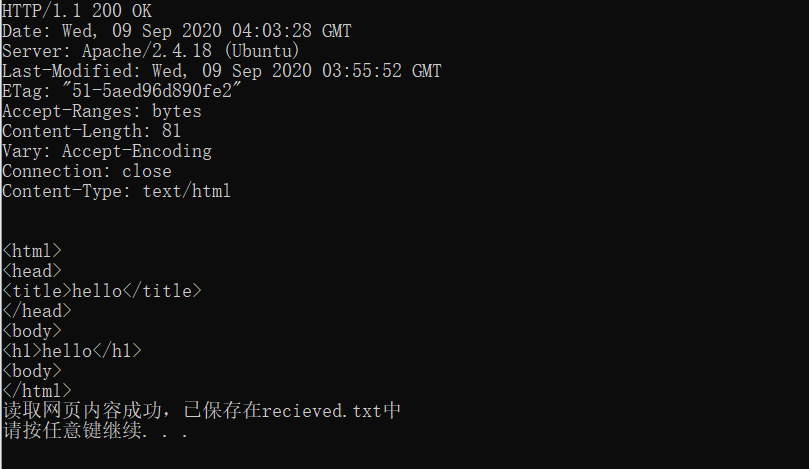
char\* str = "vulnerable";

ReadPage(str);

system("pause");

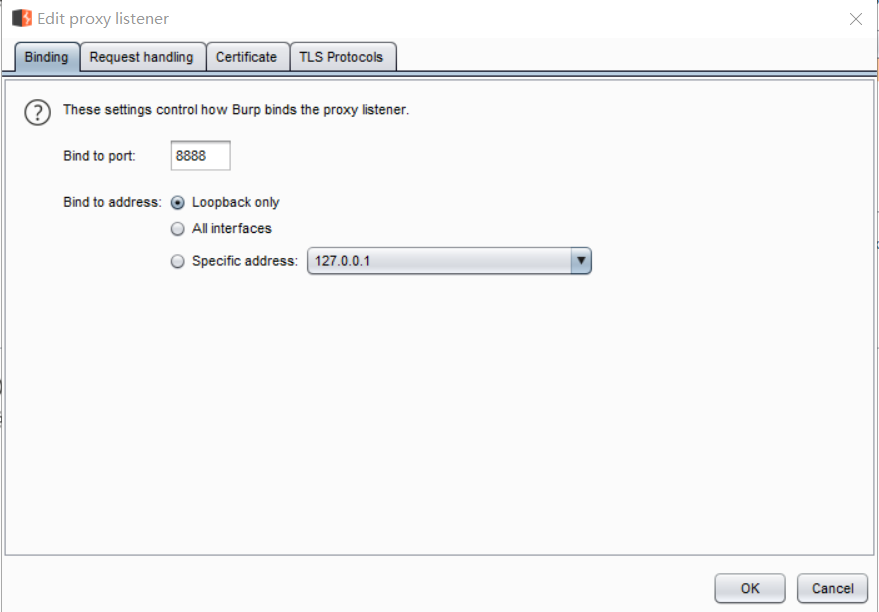
}

然后执行该文件，看到网页定向正确。

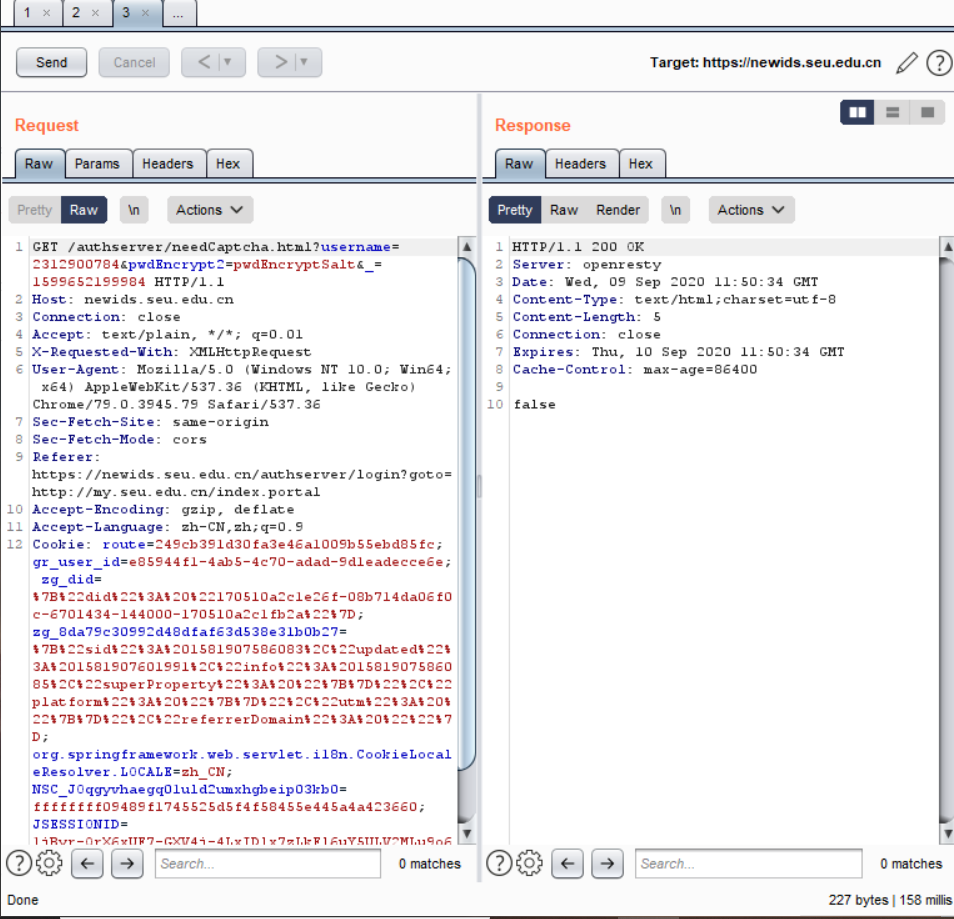


任务五：下载软件Burp Suite并访问网站查看请求与响应的信息

按实验要求下载Burp Suite，并为代理设置地址。



接着安装CA安全证书，并进行抓包，成功抓取。

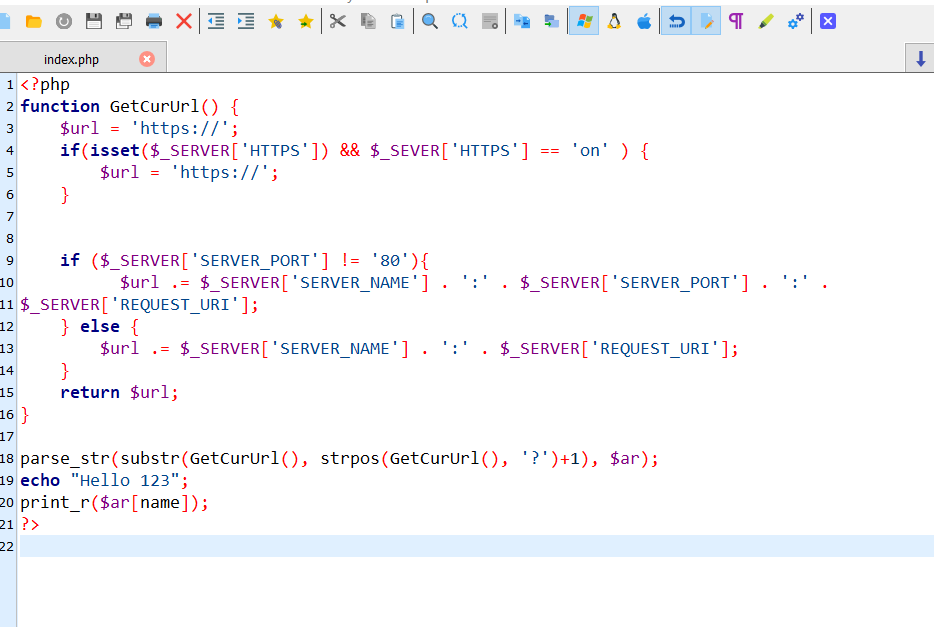


**实验二 使用PHP和Mysql搭建一个简单的站点**

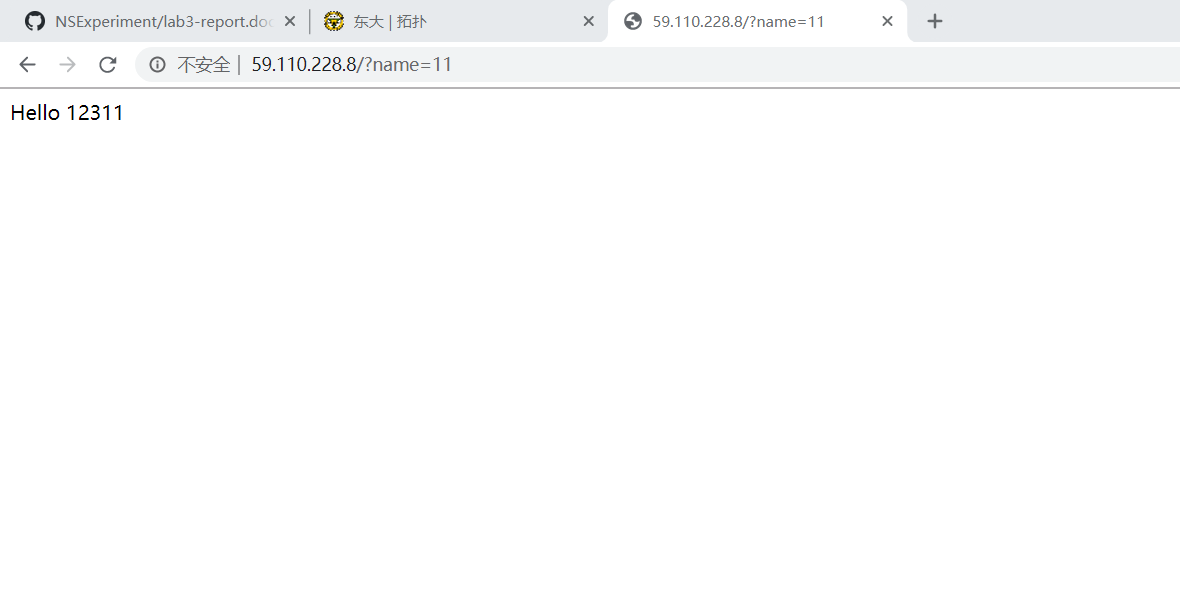
任务一：在虚拟机中安装PHP（使用以前的Apache安装），编写一个脚本以回显URL中的参数。

可能是由于vmware的原因，物理机并不能总是ping通虚拟机，严重影响了实验进度（连接方式无论是网桥还是NAT）。因此选择采用在一个租用的公网ip服务器上进行此实验。

按实验要求书写代码如下。

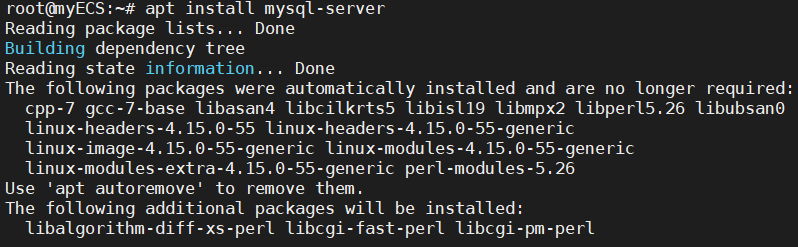


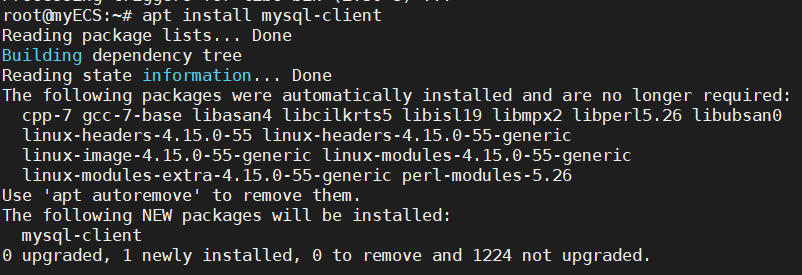
然后在浏览器访问租用的公网ip，设置name=11，得到如下结果。



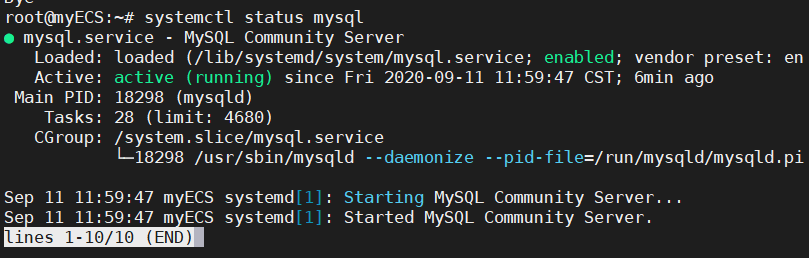
任务二：安装mysql服务

按要求安装myqsl-server和myqsl-client。





输入指令systemctl status mysql查看mysql状态发现其已经启动。



按路径/etc/mysql/debian.cnf打开文件，查看mysql为我们创建的的一个用户，找到用户名和密码。

