**Lab3实验**

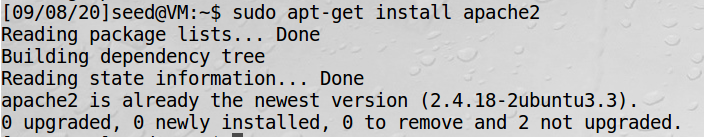
**57118111 王雯**

**实验目的：**

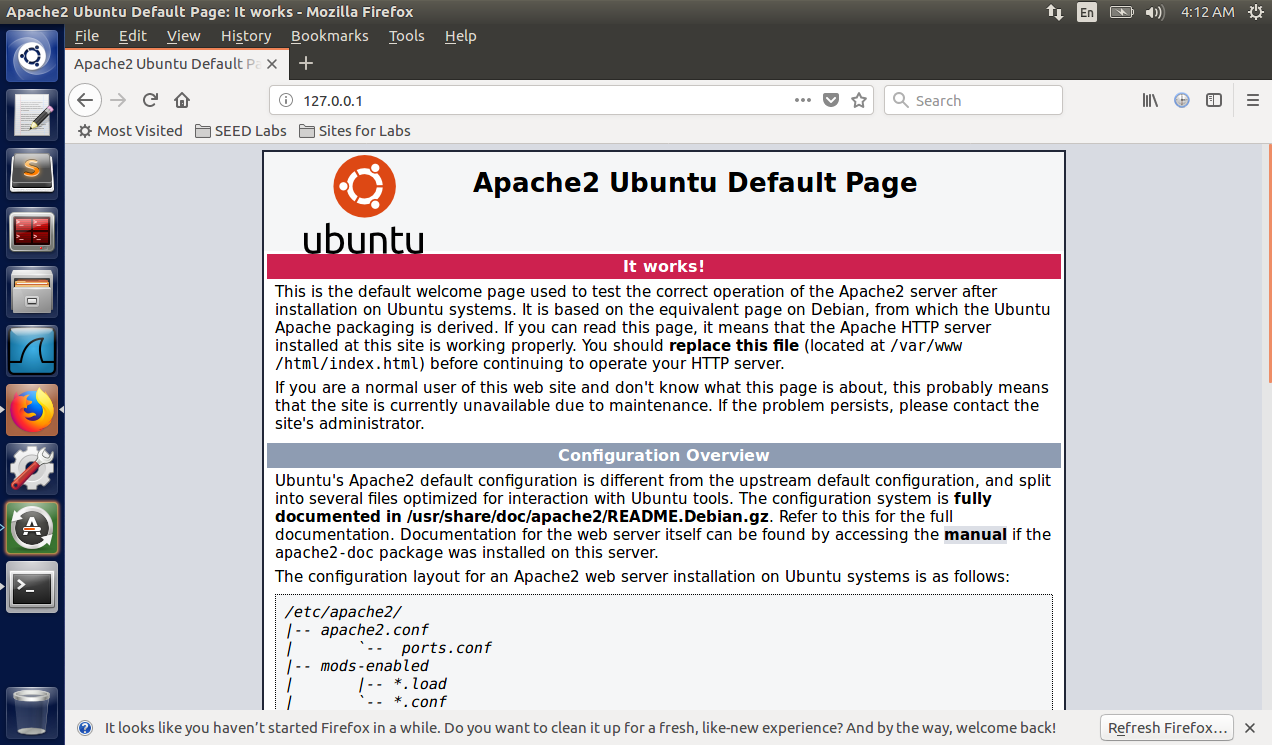
通过该次实验，我们对http网页的基本操作熟练掌握，并且可以获得对Burp Suite软件的基础操作，对拦截的信息可以进行简单分析，查看拦截文件的信息。

**任务一：HTTP基础**

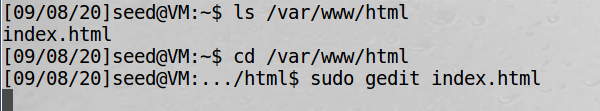
首先我们根据实验手册，在虚拟机中打开terminal终端窗口，输入sudo apt-get install apache2

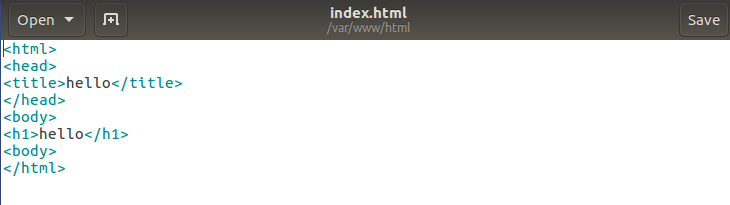


接下来在虚拟机中输入“127.0.0.1”，打开网页界面。

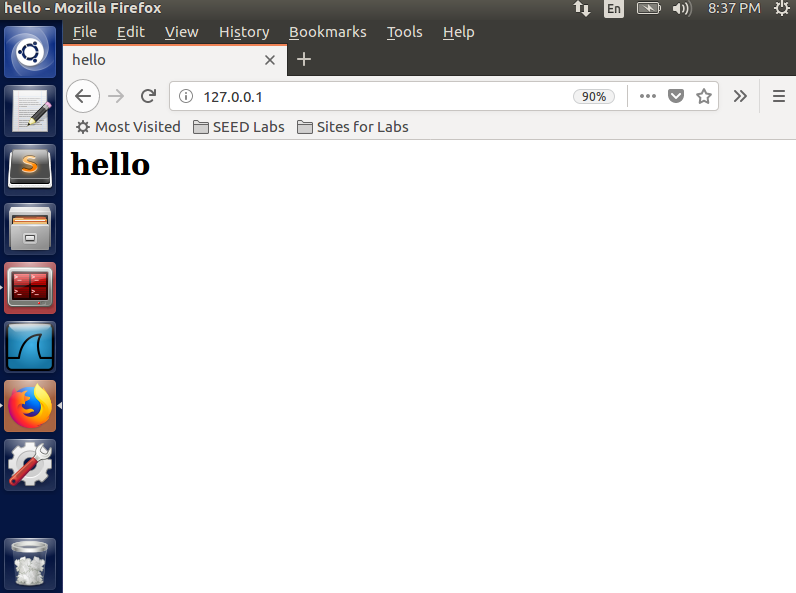


接下来依旧按照步骤，将使用sudogedit index.html指令打开index.html并进行编写

按照实验手册的代码对

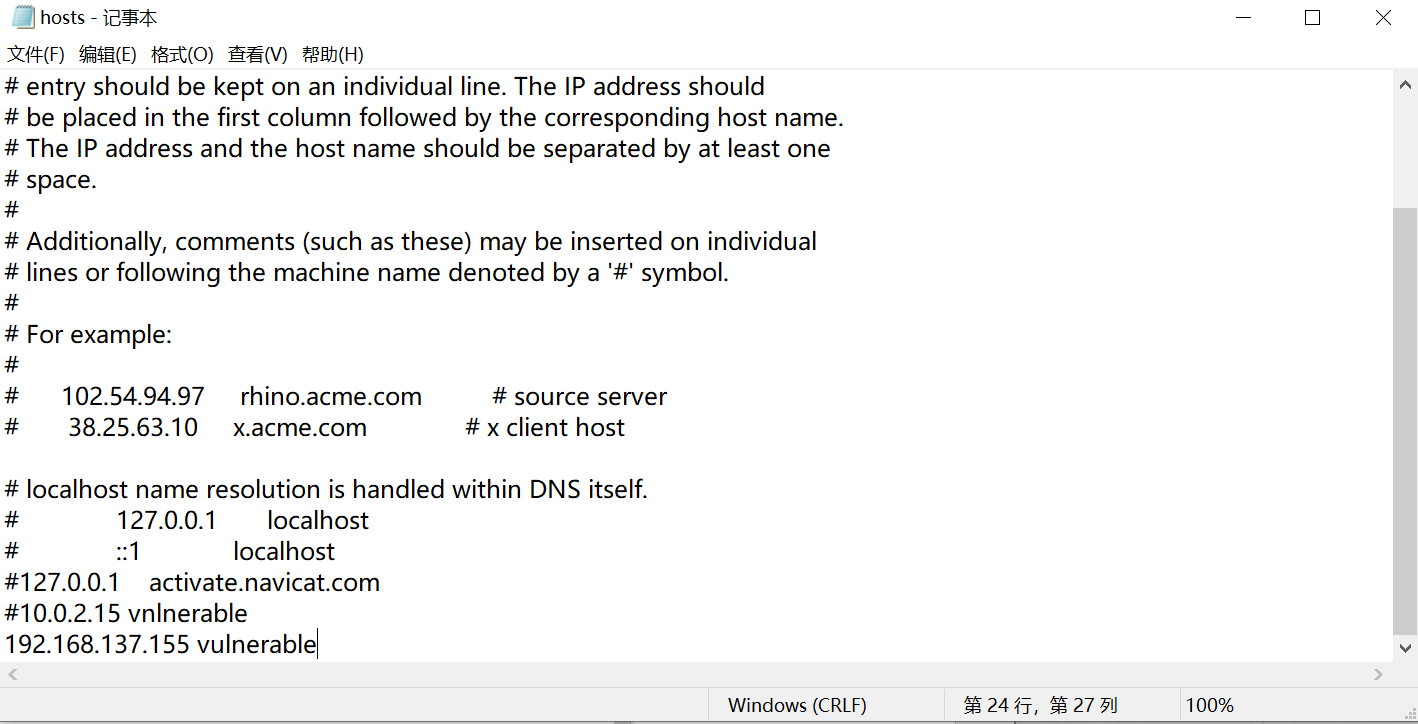


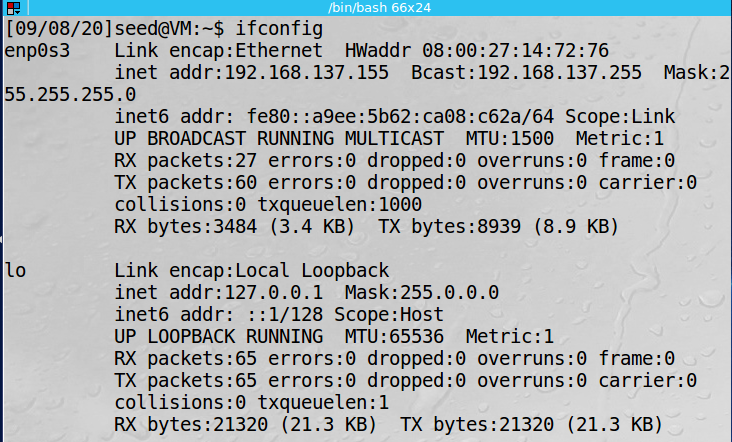
按照上图修改后再继续登录127.0.0.1，页面更改为新主页



**任务二：通过host文件解析名称**

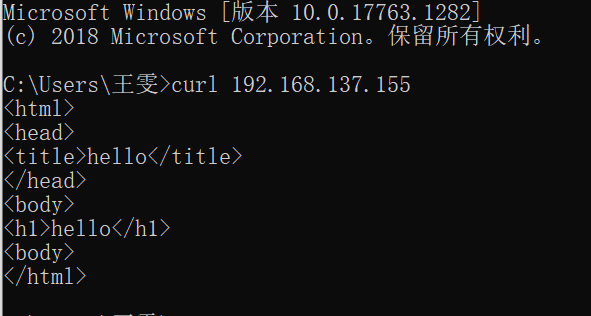
步骤一：在windows主机中找到hosts文件用记事本打开，然后修改hosts文件的虚拟IP地址与主机名（保存要以管理员身份运行记事本）。虚拟机的ip地址，根据实验最开始的环境配置，我们将虚拟机设置为桥接模式，然后在虚拟机上获取IP地址192.168.137.155，之后我们再用主机ping虚拟机，可以ping通。





**任务三：编写HTTP客户端，使用http库检索站点的主页**

步骤一：Windows主机中输入curl和IP地址，可查看编写的Index的文件



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test.py），之后命令行转到文件所在位置

**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**

#include<stdio.h>

#include<stdlib.h>

#include<string.h>

#include<iostream>

#include<winsock2.h>

#include<time.h>

#pragmacomment(lib,"ws2\_32.lib")

voidReadPage(constchar\* 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

structhostent\* h = gethostbyname(host);

if (h == NULL)

return;

//IPV4

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

return;

structin\_addrina;

//解析IP

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

LPSTRipstr = inet\_ntoa(ina);

//Socket封装

structsockaddr\_insi;

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");

intisstart = 0;

while (ret > 0)

{

constintbufsize = 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;

}

int main() {

constchar\* str = "vulnerable";

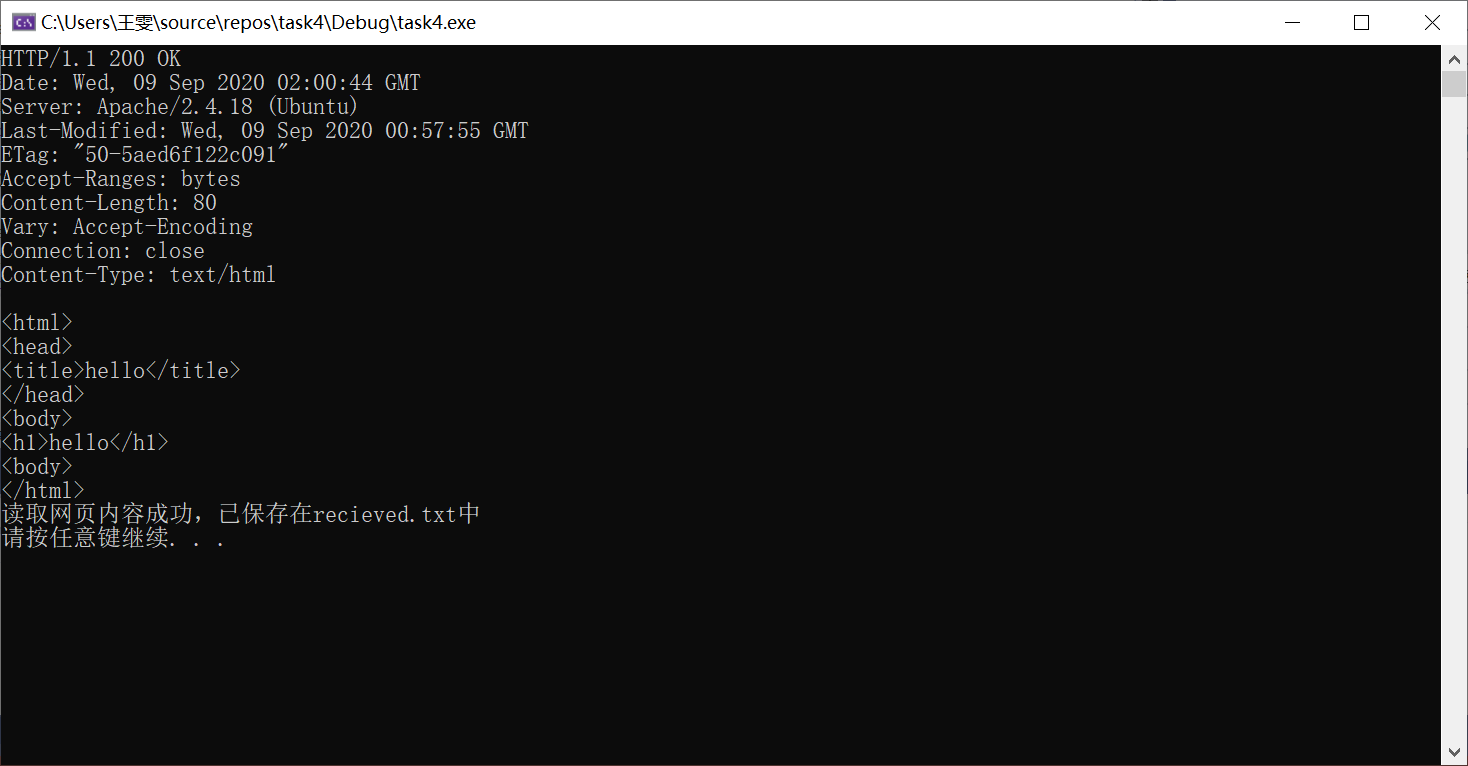
ReadPage(str);

system("pause");

return 0;

}

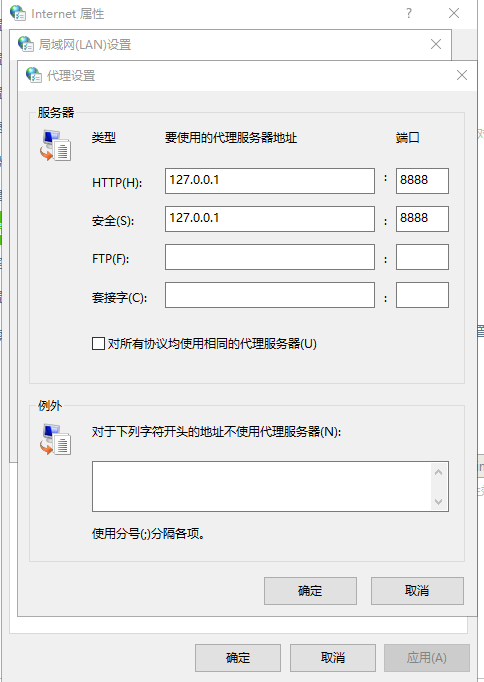
然后执行该文件



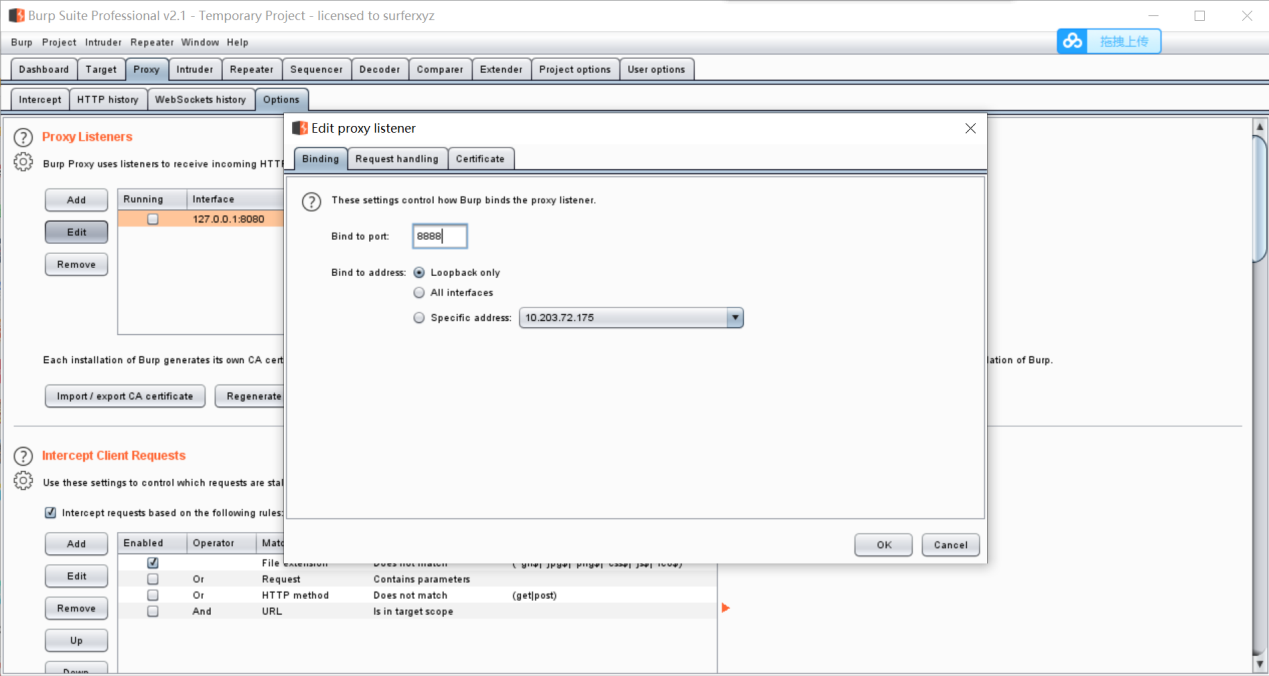
**任务五：下载软件BurpSuite并访问网站查看请求与响应的信息**

步骤一：先下载BurpSuite

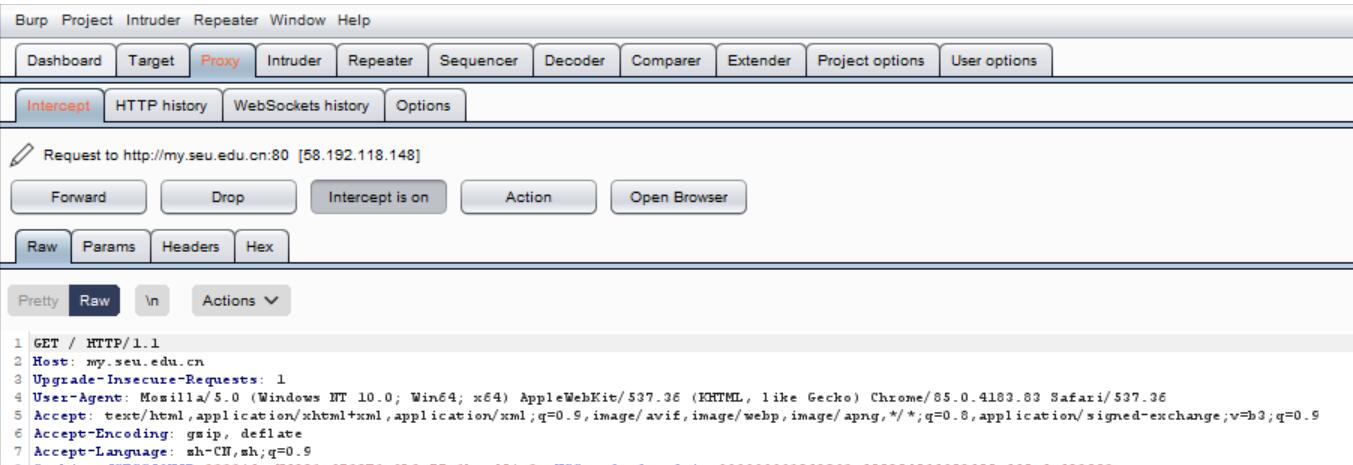
步骤二：对测试浏览器进行代理，地址设为127.0.0.1，端口修改为8888



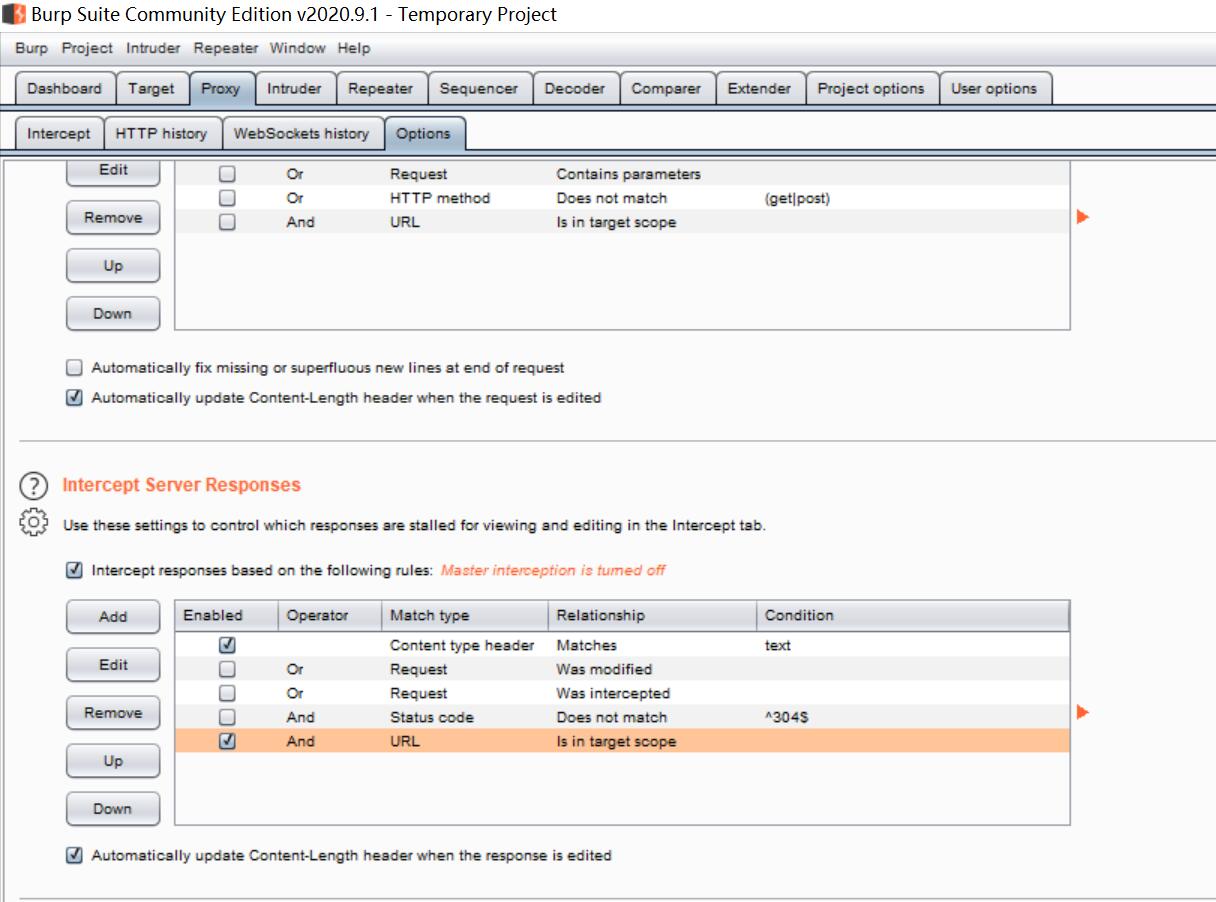
之后打开BurpSuite界面，设置proxy代理，端口改为8888



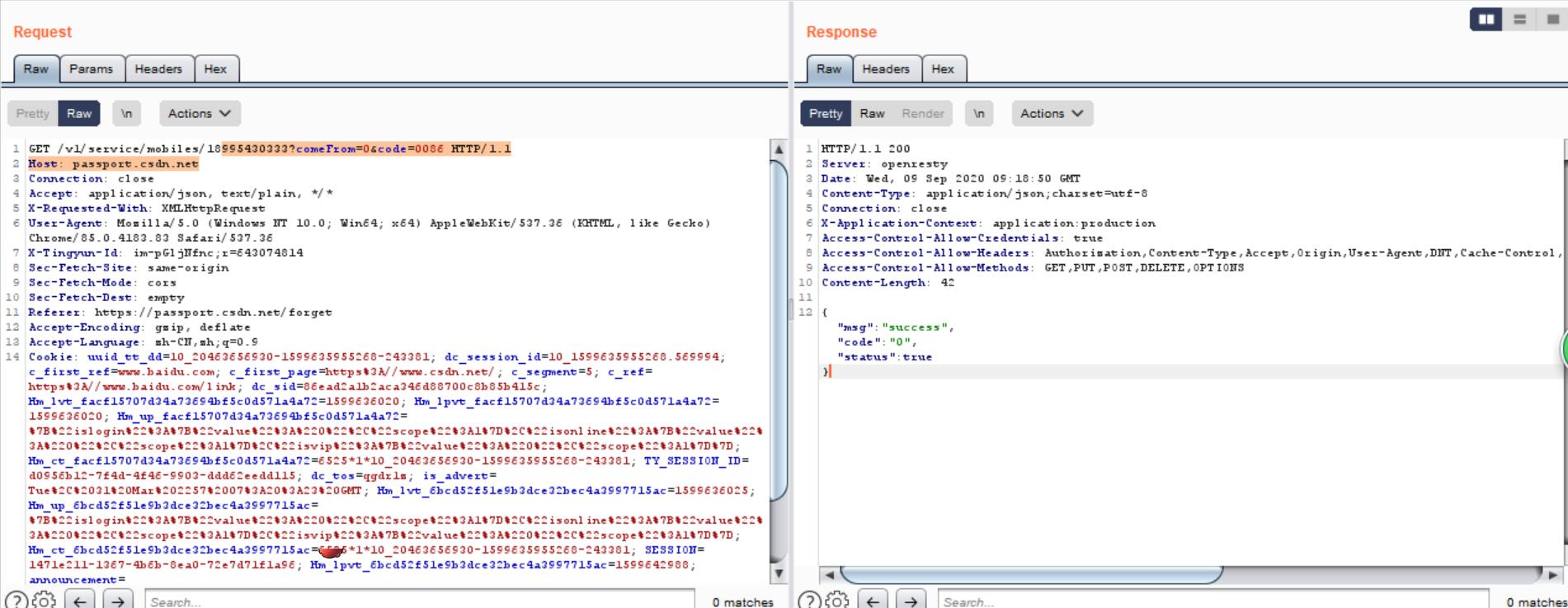
使用浏览器打开my.seu.edu.cn查看拦截情况



步骤五：



步骤六：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 ison按钮进行关闭，在需要拦截时再打开)



**实验总结：**

在这次的实验中，我们对http的基础有了一定的掌握，同时可以通过终端修改代码对网页进行修改。同时我们通过下载Burp Suite软件，对基础的网络拦截，查看有了一定的了解。我们通过对my.seu.edu.cn还有CSDN的验证码功能的拦截，对proxy这个功能有了更深入的了解。实验中遇到的问题：在创建.py文件后，无法通过终端命令的输入，得到与实验手册中的执行结果。在课后会继续请教助教，老师解决这个问题。