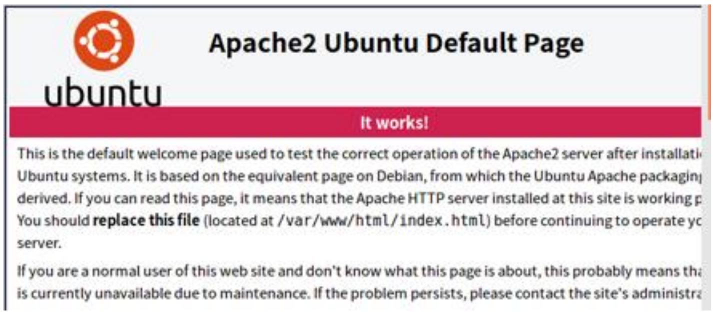
实验 2

57118137 朱旭

任务一：安装 apache 服务器 并用简单页面验证

修改前：



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installati
Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packagin
derived. If you can read this page, it means that the Apache HTTP server installed at this site is working p
You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate yc
server.

If you are a normal user of this web site and don't know what this page is about, this probably means th
is currently unavailable due to maintenance. If the problem persists, please contact the site's administr

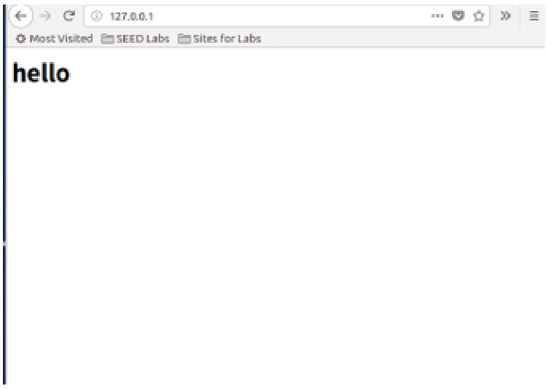
输入命令：~$ cd /var/www/html

…/html$ sudo gedit index.html

打开这个网址，将其修改为：

```
<html>
<head>
<title>hello</title>
</head>
<body>
<h1>hello</h1>
<body>
</html>
```

修改后原网页：



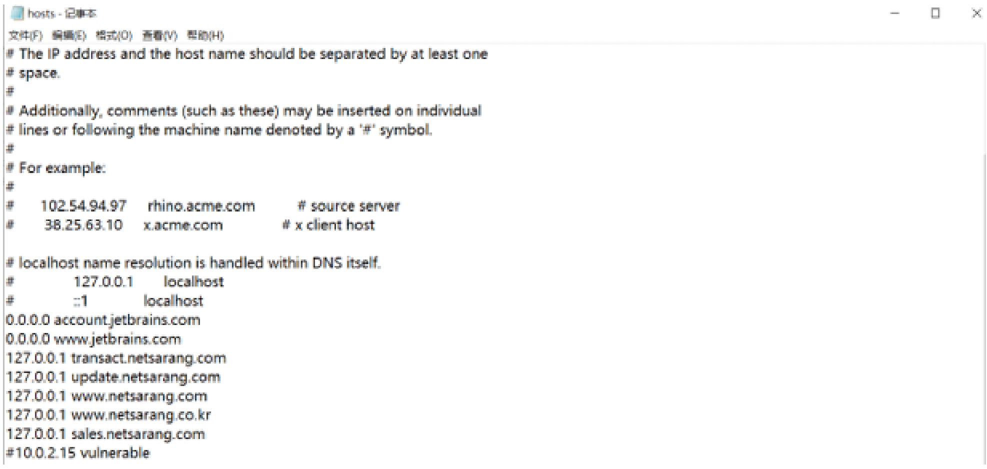
hello

任务二：通过 host 文件解析名称

首先通过命令查询虚拟机的 ip 地址，本机为 192.168.20.4 255.255.255.0

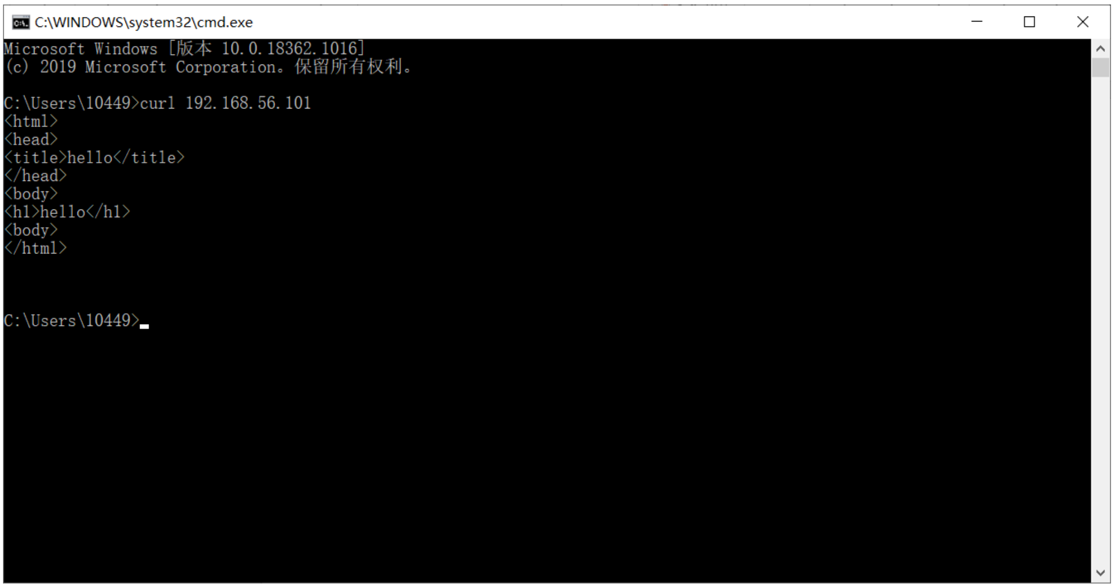
然后在 windows 主机中找到 hosts 文件记事本打开；

加入虚拟机 ip 地址和主机名 vulnerable 并保存



```
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#	127.0.0.1       localhost
#	::1             localhost
0.0.0.0 account.jetbrains.com
0.0.0.0 www.jetbrains.com
127.0.0.1 transact.netsarang.com
127.0.0.1 update.netsarang.com
127.0.0.1 www.netsarang.com
127.0.0.1 www.netsarang.co.kr
127.0.0.1 sales.netsarang.com
#10.0.2.15 vulnerable
```

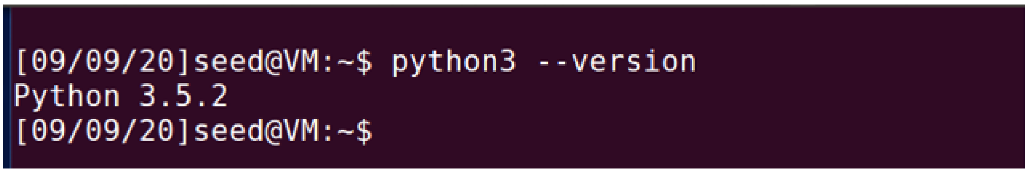
任务三：编写 HTTP 客户端，使用 http 库检索站点的主页



```
Microsoft Windows [版本 10.0.18362.1016]
(c) 2019 Microsoft Corporation。保留所有权利。

C:\Users\10449>curl 192.168.56.101
<html>
<head>
<title>hello</title>
</head>
<body>
<h1>hello</h1>
<body>
</html>


C:\Users\10449>
```

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

查看虚拟机 python 版本：



```
[09/09/20]seed@VM:~$ python3 --version
Python 3.5.2
[09/09/20]seed@VM:~$
```

将以下代码保存为 te.py：

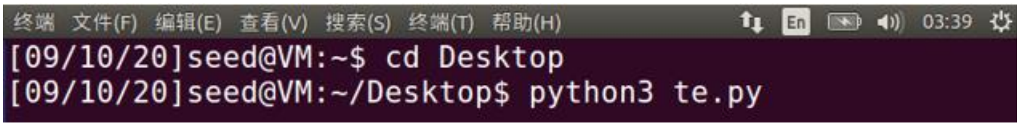
import requests

from requests_toolbelt.utils import dump

resp = requests.get('http://127.0.0.1')

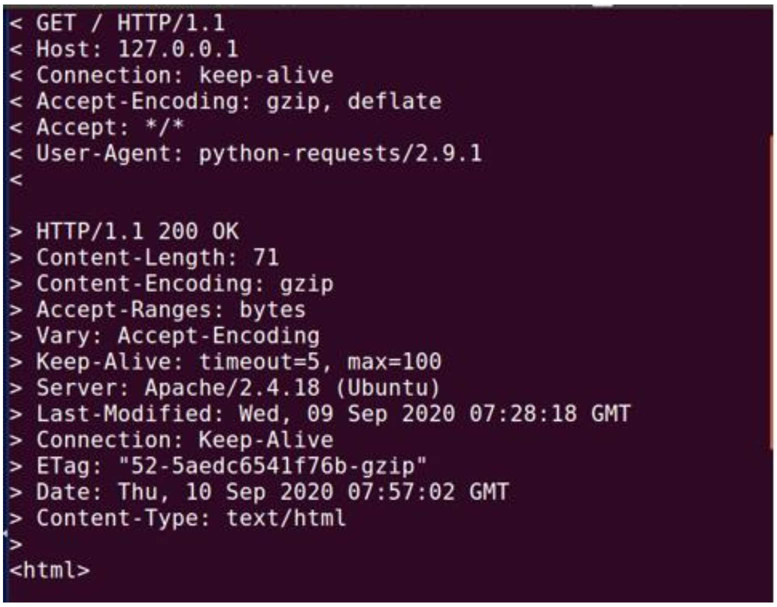
data =dump.dump_all(resp)

print(data.decode('utf-8'))



```
[09/10/20]seed@VM:~$ cd Desktop
[09/10/20]seed@VM:~/Desktop$ python3 te.py
```

执行 te.py，结果如下



```
< GET / HTTP/1.1
< Host: 127.0.0.1
< Connection: keep-alive
< Accept-Encoding: gzip, deflate
< Accept: */*
< User-Agent: python-requests/2.9.1
<

> HTTP/1.1 200 OK
> Content-Length: 71
> Content-Encoding: gzip
> Accept-Ranges: bytes
> Vary: Accept-Encoding
> Keep-Alive: timeout=5, max=100
> Server: Apache/2.4.18 (Ubuntu)
> Last-Modified: Wed, 09 Sep 2020 07:28:18 GMT
> Connection: Keep-Alive
> ETag: "52-5aedc6541f76b-gzip"
> Date: Thu, 10 Sep 2020 07:57:02 GMT
> Content-Type: text/html
>
<html>
```

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>

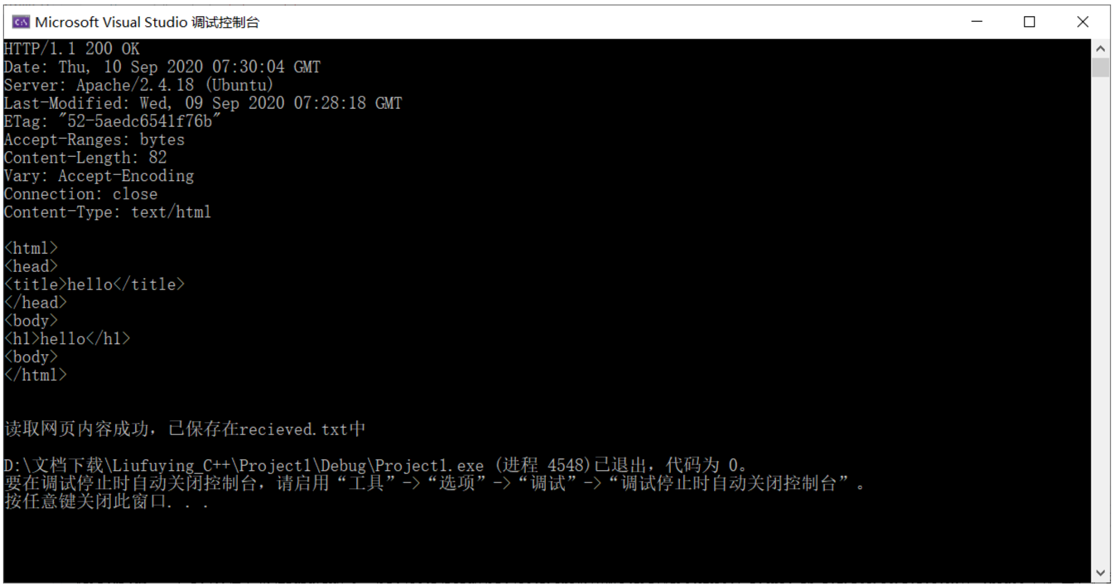
#include <string.h>

```
#include <iostream>

#include <winsock2.h>

#include<time.h>

#pragma comment(lib,"ws2_32.lib")

void ReadPage(const 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;
}
int main() {
    const char* str = "vulnerable";
    ReadPage(str);
    return 0;
    system("pause");
}
```

执行结果如下：

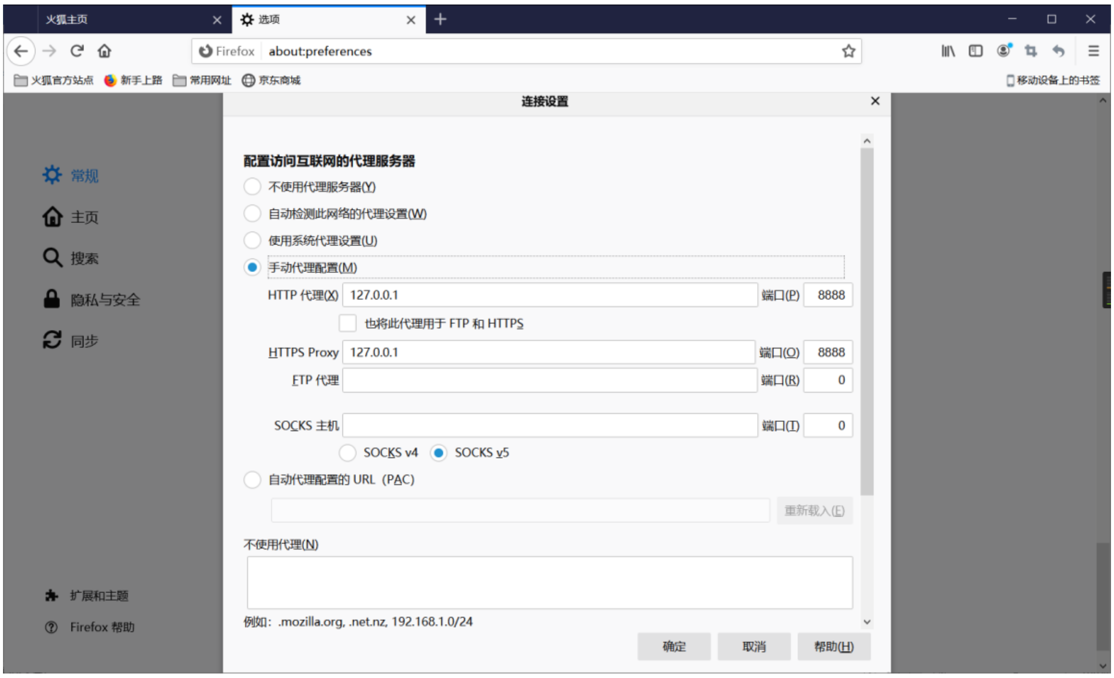


```
HTTP/1.1 200 OK
Date: Thu, 10 Sep 2020 07:30:04 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Wed, 09 Sep 2020 07:28:18 GMT
ETag: "52-5aedc6541f76b"
Accept-Ranges: bytes
Content-Length: 82
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

<html>
<head>
<title>hello</title>
</head>
<body>
<h1>hello</h1>
<body>
</html>


读取网页内容成功，已保存在recieved.txt中

D:\文档下载\Liufuying_C++\Project1\Debug\Project1.exe (进程 4548)已退出，代码为 0。
要在调试停止时自动关闭控制台，请启用“工具”->“选项”->“调试”->“调试停止时自动关闭控制台”。
按任意键关闭此窗口. . .
```

任务五：下载软件 Burp Suite 并访问网站查看请求与响应的信息

因 chrome 版本问题于是选用 Firefox 进行实验

设置代理，地址设为 127.0.0.1,端口修改为 8888



配置访问互联网的代理服务器

○ 不使用代理服务器(Y)
○ 自动检测此网络的代理设置(W)
○ 使用系统代理设置(U)
● 手动代理配置(M)

HTTP 代理(X) 127.0.0.1 端口(P) 8888

□ 也将此代理用于 FTP 和 HTTPS

HTTPS Proxy 127.0.0.1 端口(O) 8888

FTP 代理 端口(R) 0

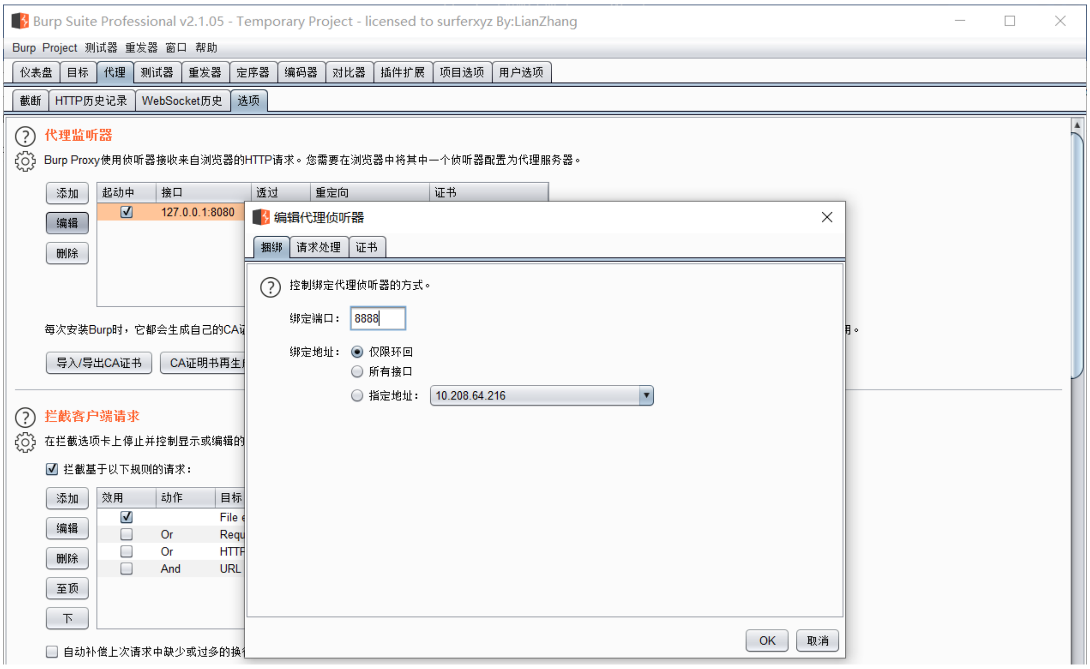
SOCKS 主机 端口(T) 0

○ SOCKS v4 ● SOCKS v5

○ 自动代理配置的 URL（PAC）

不使用代理(N)

例如：.mozilla.org, .net.nz, 192.168.1.0/24


Burp Suite Professional v2.1.05 - Temporary Project - licensed to surferxyz By:LianZhang
Burp Project 测试器 重发器 窗口 帮助
仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项
截断 HTTP历史记录 WebSocket历史 选项
添加
编辑
删除
导入/导出CA证书
CA证明书再生
添加
编辑
删除
至顶
下
编辑代理侦听器
捆绑 请求处理 证书
OK
取消

代理监听器

Burp Proxy使用侦听器接收来自浏览器的HTTP请求。您需要在浏览器中将其中一个侦听器配置为代理服务器。

起动中	接口	透过	重定向	证书
☑	127.0.0.1:8080			

每次安装Burp时，它都会生成自己的CA证 … 用。

拦截客户端请求

在拦截选项卡上停止并控制显示或编辑的

☑ 拦截基于以下规则的请求：

效用	动作	目标
☑		File e
□	Or	Requ
□	Or	HTTF
□	And	URL

□ 自动补偿上次请求中缺少或过多的换

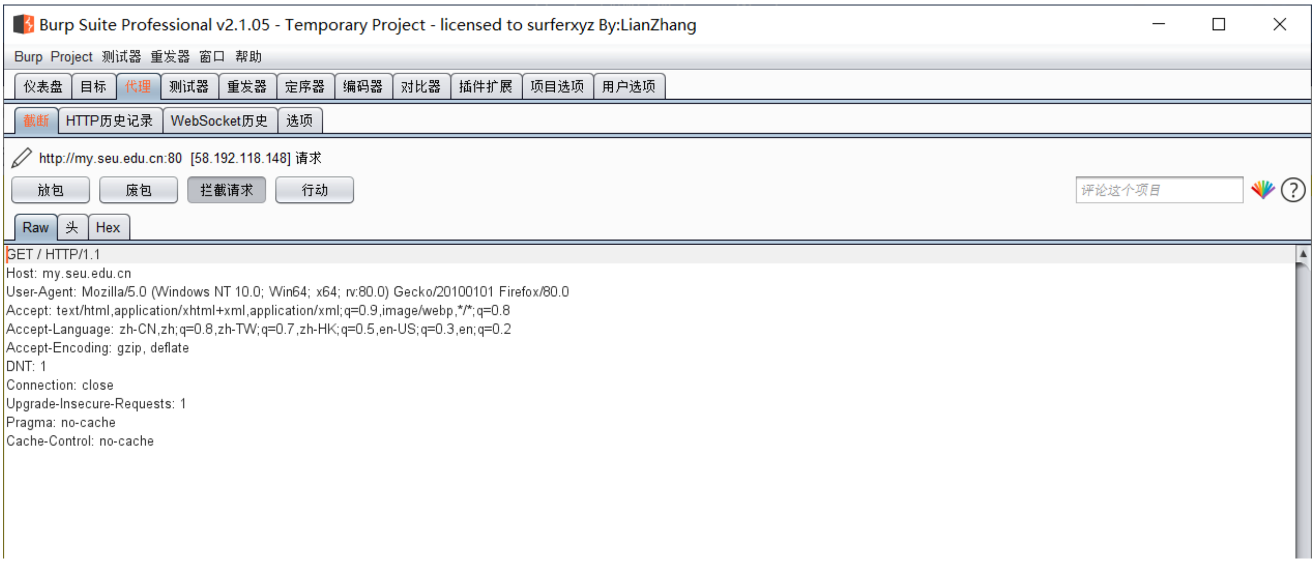
控制绑定代理侦听器的方式。

绑定端口：8888

绑定地址：● 仅限环回
○ 所有接口
○ 指定地址：10.208.64.216

打开 Burp Suite 界面，设置 Proxy 代理，端口改为 8888

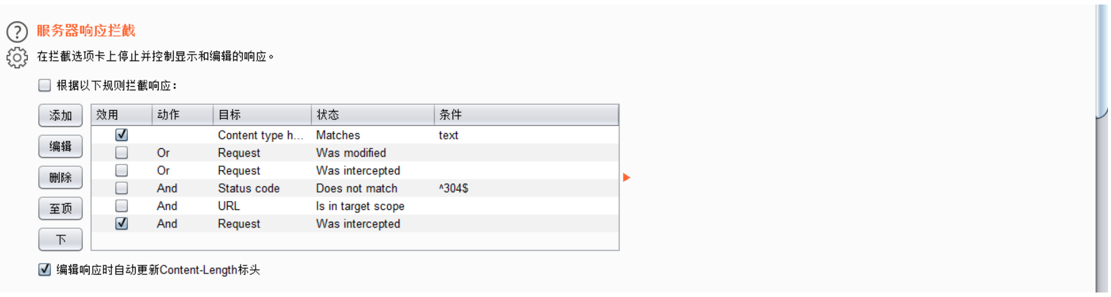
使用浏览器打开 my.seu.edu.cn 查看拦截情况


Burp Suite Professional v2.1.05 - Temporary Project - licensed to surferxyz By:LianZhang
Burp Project 测试器 重发器 窗口 帮助
仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项
截断 HTTP历史记录 WebSocket历史 选项
放包
废包
拦截请求
行动
评论这个项目
Raw 头 Hex

http://my.seu.edu.cn:80 [58.192.118.148] 请求

```
GET / HTTP/1.1
Host: my.seu.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
```

更改服务器响应拦截设置



服务器响应拦截

在拦截选项卡上停止并控制显示和编辑的响应。

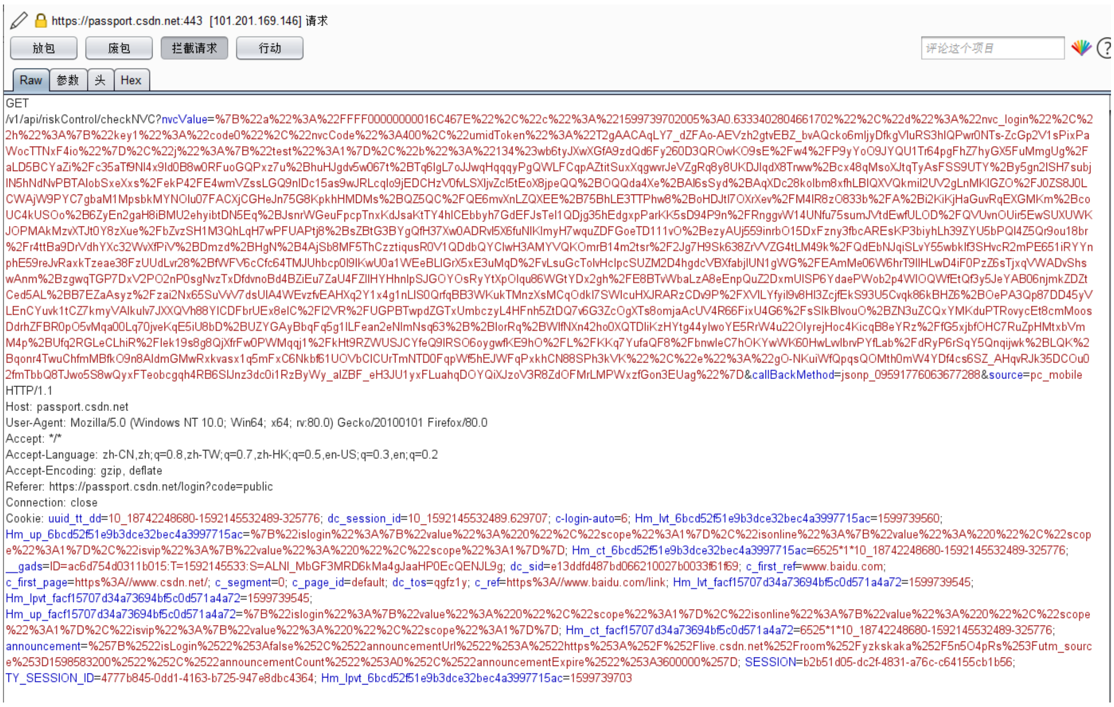
□ 根据以下规则拦截响应：

效用	动作	目标	状态	条件
☑		Content type h...	Matches	text
□	Or	Request	Was modified	
□	Or	Request	Was intercepted	
□	And	Status code	Does not match	^304$
□	And	URL	Is in target scope	
☑	And	Request	Was intercepted	

☑ 编辑响应时自动更新Content-Length标头

测试 CSDN 通过发送验证码找回密码功能，查看 Request 和 Response 功能：

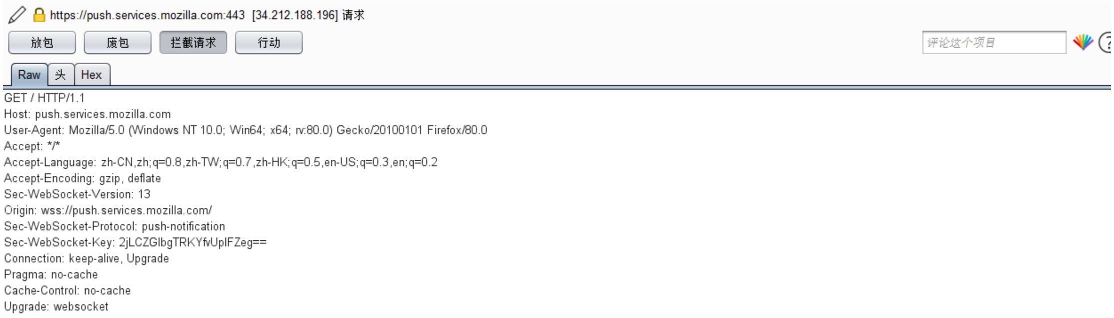
Request:



https://passport.csdn.net:443 [101.201.169.146] 请求

```
GET
/v1/api/riskControl/checkNVC?nvcValue=%7B%22a%22%3A%22FFFF00000000016C467E%22%2C%22c%22%3A%221599739702005%3A0.6333402804661702%22%2C%22d%22%3A%22nvc_login%22%2C%2
2h%22%3A%7B%22key1%22%3A%22code0%22%2C%22nvcCode%22%3A400%2C%22umidToken%22%3A%22T2gAACAqLY7_dZFAo-AEVzh2gtvEBZ_bvAQcko6mljyDfkgVluRS3hlQPwr0NTs-ZcGp2V1sPixPa
WocTTNxF4io%22%7D%2C%22j%22%3A%7B%22test%22%3A1%7D%2C%22b%22%3A%22134%23wb6tyJXwXGfA9zdQd6Fy260D3QROwKO9sE%2Fw4%2FP9yYoO9JYQU1Tr64pgFhZ7hyGX5FuMmgUg%2F
aLD5BCYaZi%2Fc35aTf9Nl4x9ld0B8w0RFuoGQPxz7u%2BhuHJgdv5w067t%2BTq6lgL7oJJwqHqqqyPgQWLFCqpAZtitSuxXqgwrJeVZgRq8y8UKDJlqdX8Trww%2Bcx48qMsoXJtqTyAsFSS9UTY%2By5gn2lSH7subj
lN5hNdNvPBTAlobSxeXxs%2FekP42FE4wmVZssLGQ9nlDc15as9wJRLcqlo9jEDCHzV0fvLSXljvZcl5tEoX8jpeQQ%2BOQQda4Xe%2BAl6sSyd%2BAqXDc28kolbm8xfhLBlQXVQkmil2UV2gLnMKlGZO%2FJ0ZS8J0L
CWAjW9PYC7gbaM1MpsbkMYNOlu07FACXjCGHeJn75G8KpkhHMDMs%2BQZ5QC%2FQE6mvXnLZQXEE%2B75BhLE3TTPhw8%2BoHDJtl7OXrXev%2FM4IR8zO833b%2FA%2Bi2KiKjHaGuvRqEXGMKm%2Bco
UC4kUSOo%2B6ZyEn2gaH8iBMU2ehyibtDN5Eq%2BJsnrWGeuFpcpTnxKdJsaKtTY4hlCEbbyh7GdEFJsTel1QDjg35hEdgxpParKK5sD94P9n%2FRnggvW14UNfu75sumJVtdEwfULOD%2FQVUvnOUir5EwSUXUWK
JOPMAkMzvXTJt0Y8zXue%2FbZvzSH1M3QhLqH7wPFUAPtj8%2BsZBtG3BYgQfH37Xw0ADRvl5X6fuNlKlmyH7wquZDFGoeTD111vO%2BezyAUj559inrbO15DxFzny3fbcAREsKP3biyhLh39ZYU5bPQl4Z5Qr9ou18br
%2Fr4ttBa9DrVdhYXc32WvXfPiV%2BDmzd%2BHgN%2B4AjSb8MF5ThCzztiqusR0V1QDdbQYClwH3AMYVQKOmrB14m2tsr%2F2Jg7H9Sk638ZrVVZG4tLM49k%2FQdEbNJqiSLvY55wbklf3SHvcR2mPE651iRYYn
phE59reJvRaxkTzeae38FzUUdLvr28%2BfWFV6cCfc64TMJUhbcp0I9lKwU0a1WEeBLlGrX5xE3uMqD%2FvLsuGcTolvHclpcSUZM2D4hgdcVBXfabjlUN1gWG%2FEAmMe06W6hrT9llHLwD4iF0PzZ6sTjxqVWADvShs
wAnm%2BzgwqTGP7DxV2PO2nP0sgNvzTxDfdvnoBd4BZiEu7ZaU4FZllHYHhnlpSJGOYOsRyYtXpOlqu86WGtYDx2gh%2FE8BTvWbaLzA8eEnpQuZ2DxmUlSP6YdaePWob2p4WlOQWfEtQf3y5JeYAB06njmkZDZt
Ced5AL%2BB7EZaAsyz%2Fzai2Nx65SuVW7dsUlA4WEvzfvEAHXq2Y1x4g1nLIS0QrfqBB3WKukTMnzXsMCqOdkl7SWlcuHXJRARzCDv9P%2FXVlLYfyil9v8Hl3ZcjfEkS93U5Cvqk86kBHZ6%2BOePA3Qp87DD45yV
LEnCYuvk1tCZ7kmyVAlkulv7JXXQVh88YlCDFbrUEx8elC%2Fl2VR%2FUGPBTwpdZGTxUmbczyL4HFnh5ZtDQ7v6G3ZcOgXTs8omjaAcUV4R66FixU4G6%2FsSlkBlvouO%2BZN3uZCQxYMKduPTRovycEt8cmMoos
DdrhZFBR0pO5vMqa00Lq70jveKqE5iU8bD%2BUZYGAyBbqFq5g1lLFean2eNlmNsq63%2B%2BlorRq%2BWlfNXn42ho0XQTDliKzHYtg44ylwoYE5RrW4u22OlyrejHoc4KicqB8eYRz%2FfG5xjbfOHC7RuZpHMtxbVm
M4p%2BUfq2RGLeCLhiR%2Flek19s8g8QjXfrFw0PWMqqj1%2FkHt9RZWUSJCYfeQ9IRSO6oygwfKE9hO%2FL%2FKKq7YufaQF8%2FbnwleC7hOKYwWK60HwLwlbrvPYfLab%2FdRyP6rSqY5Qnqijwk%2BLQK%2
Bqonr4TwuChfmMBfkO9n8AldmGMwRxkvasx1q5mFxC6Nkbf61UOVbClCUrTmNTD0FqpWf5hEJWFqPxkhCN88SPh3kVK%22%2C%22e%22%3A%22gO-NKuiWfQpqsQOMth0mW4YDf4cs6SZ_AHqvRJk35DCOu0
2fmTbbQ8TJwo5S8wQyxFTeobcgqh4RB6SlJnz3dc0i1RzByWy_alZBF_eH3JU1yxFLuahqDOYQiXJzoV3R8ZdOFMrLMPWxzfGon3EUag%22%7D&callBackMethod=jsonp_0959177606367728&source=pc_mobile
HTTP/1.1
Host: passport.csdn.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: https://passport.csdn.net/login?code=public
Connection: close
Cookie: uuid_tt_dd=10_18742248680-1592145532489-325776; dc_session_id=10_1592145532489.629707; c-login-auto=6; Hm_lvt_6bcd52f51e9b3dce32bec4a3997715ac=1599739560;
Hm_up_6bcd52f51e9b3dce32bec4a3997715ac=%7B%22islogin%22%3A%7B%22value%22%3A%220%22%2C%22scope%22%3A1%7D%2C%22isonline%22%3A%7B%22value%22%3A%220%22%2C%22scop
e%22%3A1%7D%2C%22isvip%22%3A%7B%22value%22%3A%220%22%2C%22scope%22%3A1%7D%7D; Hm_ct_6bcd52f51e9b3dce32bec4a3997715ac=6525*1*10_18742248680-1592145532489-325776;
__gads=ID=ac6d754d0311b015:T=1592145533:S=ALNI_MbGF3MRD6kMa4gJaaHP0EcQENJL9g; dc_sid=e13ddfd487bd066210027b0033f61f69; c_first_ref=www.baidu.com;
c_first_page=https%3A//www.csdn.net/; c_segment=0; c_page_id=default; dc_tos=qgfz1y; c_ref=https%3A//www.baidu.com/link; Hm_lvt_facf15707d34a73694bf5c0d571a4a72=1599739545;
Hm_lpvt_facf15707d34a73694bf5c0d571a4a72=1599739545;
Hm_up_facf15707d34a73694bf5c0d571a4a72=%7B%22islogin%22%3A%7B%22value%22%3A%220%22%2C%22scope%22%3A1%7D%2C%22isonline%22%3A%7B%22value%22%3A%220%22%2C%22scope
%22%3A1%7D%2C%22isvip%22%3A%7B%22value%22%3A%220%22%2C%22scope%22%3A1%7D%7D; Hm_ct_facf15707d34a73694bf5c0d571a4a72=6525*1*10_18742248680-1592145532489-325776;
announcement=%257B%2522isLogin%2522%253Afalse%252C%2522announcementUrl%2522%253A%2522https%253A%252F%252Flive.csdn.net%252Froom%252Fyzkskaka%252F5n5O4pRs%253Futm_sourc
e%253D1598583200%2522%252C%2522announcementCount%2522%253A0%252C%2522announcementExpire%2522%253A3600000%257D; SESSION=b2b51d05-dc2f-4831-a76c-c64155cb1b56;
TY_SESSION_ID=4777b845-0dd1-4163-b725-947e8dbc4364; Hm_lpvt_6bcd52f51e9b3dce32bec4a3997715ac=1599739703
```

Response:


https://push.services.mozilla.com:443 [34.212.188.196] 请求
放包
废包
拦截请求
行动
评论这个项目
Raw
头
Hex

```
GET / HTTP/1.1
Host: push.services.mozilla.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Sec-WebSocket-Version: 13
Origin: wss://push.services.mozilla.com/
Sec-WebSocket-Protocol: push-notification
Sec-WebSocket-Key: 2jLCZGlbgTRKYfvUpIFZeg==
Connection: keep-alive, Upgrade
Pragma: no-cache
Cache-Control: no-cache
Upgrade: websocket
```