CSCI 400 Lab 5

**Name: Christopher Gonzalez**

**Class Section: CSCI 400 02 [35583]**

**Date: October 20, 2024**

**Instructions**:

* Login to your account at <https://pwn.college/>

**pwn.college username: Chris\_B\_Gonzalez**

**A screenshot of a computer

Description automatically generated**

* Go to the Intro to Cybersecurity dojo: <https://pwn.college/intro-to-cybersecurity/>
* Review short videos above challenges in Talking Web: <https://pwn.college/intro-to-cybersecurity/talking-web/>
* Complete challenges 1,2,4,5,7,8,10,11,13,14 in Talking Web. (You can skip the Python ones for this submission, but you're welcome to give those a try if you have Python knowledge and time.)

**Challenge 1: level1**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge by typing “/challenge/run”. Upon starting the challenge, I was instructed to make an HTTP request to 127.0.0.1:80 using the curl command. Therefore, I pressed CTRL+C to regain the command line and entered “curl 127.0.0.1:80”. This immediately gave me the flag as highlighted in white.**

**Challenge 2: level2**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge by typing “/challenge/run”. This challenge is like the first one in the sense that I must make an HTTP request to 127.0.0.1 on port 80, but this time I was required to use the nc command. To complete this task, I regained the command line and entered “nc 127.0.0.1 80”. This allowed me to connect with the web server and make my requests. The request I made was “GET / HTTP/1.0” followed by “Host: 127.0.0.1”. This informs the web server that I am requesting the contents provided in the given address. After pressing enter twice, I was given the flag.**

**Challenge 4: level4**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge by typing “/challenge/run”. For this challenge, I was asked to use curl once again to retrieve the flag, but I also had to set the host header to the one provided in the image. First, I regained access of the command line and entered the following:**

**“curl -H “Host: 73d6d08a53c0bbe5d4d8758096a1bd7d” 127.0.0.1”**

**This command sets the host name to the one desired by the challenge and make the HTTP request to the web server at the same time. After pressing enter, I was given the flag.**

**Challenge 5: level5**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge by typing “/challenge/run”. The challenge required me to use the nc command to make an HTTP request once again, but I had to set the host HTTP to the one provided. I began by regaining control of the terminal and entering “nc 127.0.0.1:80”. This is to establish a connection with the web server first. Once the connection was established, I proceeded by typing “GET /HTTP/1.1” and “Host: c05f26877535cb9682b11cd8c61b0712” which makes the request to the server and sets the HTTP header at the same time. Afterwards, I was given the flag.**

**Challenge 7: level7**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge by typing “/challenge/run”. This challenge required me to set the path in an HTTP request using curl. The path I was asked to set was /e8cbd396d2acea2e3680251cbc2f4e83, so I proceeded to enter “curl 127.0.0.1/e8cbd396d2acea2e3680251cbc2f4e83”, which gave me the flag.**

**Challenge 8: level8**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge by typing “/challenge/run”. I was required to make an HTTP request using the path provided to me, so I began by regaining control of the command line and typed “nc 127.0.0.1 80”. This is so a connection is established with the target web server. Once the connection was made, I entered “GET /0b36fbb6a65fdd8055eaf5777d159ba9” which established the path, followed by “Host: 127.0.0.1”. After pressing enter twice, the flag was revealed to be below.**

**Challenge 10: level10**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge by typing “/challenge/run”. For this challenge, I had to make an HTTP request with the given path, but it was also necessary to encode the path by filling the blank spaces with %20. I regained control of the command line and entered**

**“curl 127.0.0.1:80/9564b1d1%203ff043b7/6641daaf%20ef0dffe9”. If looked at closely, there are two instances where I had to enter “%20” within the given path due to the fact there were two blank spaces in the initial path. After pressing enter, I was given the flag.**

**Challenge 11: level11**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge by typing “/challenge/run”. Like the previous challenge, I had to make an HTTP request and encode the given path. I began by regaining control of the command line and typed “nc 127.0.0.1 80” to establish a connection with the target web server. I proceeded the challenge by entering “GET /6795dfec%200888e3e3/8cdac74d%209daad326”, which encoded the path given to me. Then, I entered “Host: 127.0.0.1” and pressed enter twice, giving me the flag.**

**Challenge 13: level13**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge by typing “/challenge/run”. This challenge required me to enter the argument provided to me when making an HTTP request using curl. I began by regaining access to the command line and entered “curl 127.0.0.1:80/resource?a=4a38fcca97f042cff340c5a8c8a64a2d”. The portion containing “a=” and afterwards represents the argument I was prompted to include when making my HTTP request. After hitting enter, I was given the flag.**

**Challenge 14: level14**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge by typing “/challenge/run”. For this challenge, I had to make an HTTP request while specifying the argument provided to me. After regaining control of the command line, I established a connection with the web server by entering “nc 127.0.0.1 80”. Then, I proceeded to enter “GET /path?a=b16f03a6b68f3ae5ec50471a9e712b9a HTTP/1.1”, where the value of the argument can be seen after “a=” and “Host: 127.0.0.1”. After this, I was given the flag.**