Web Requests:

Link to challenge: https://academy.hackthebox.com/module/35

(log in required)

Class: Tier 0 | Fundamental | General

HTTP Fundamentals

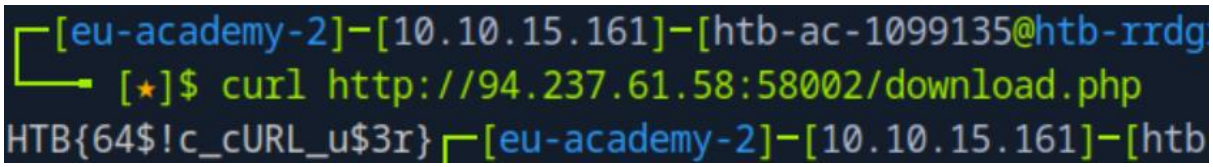
HyperText Transfer Protocol (HTTP):

Question: To get the flag, start the above exercise, then use cURL to download the file returned by '/download.php' in the server shown above.

Answer: HTB{64$!c_cURL_u$3r}

Method: lets initiate curl content retrieve command to the URL:

```
curl http://<target-IP>:<target-port>/download.php
```



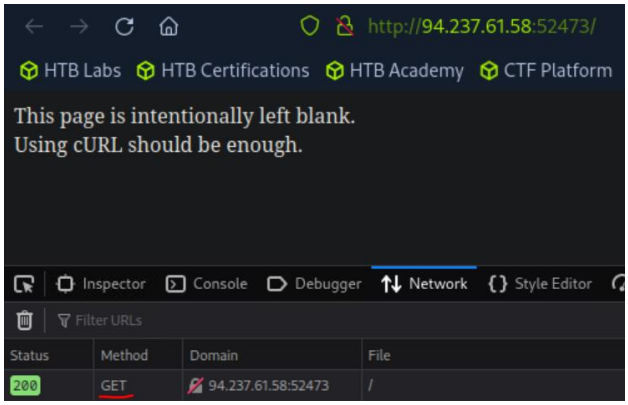
HTTP Requests and Responses:

Question: What is the HTTP method used while intercepting the request? (case-sensitive)

Answer: GET

Method:

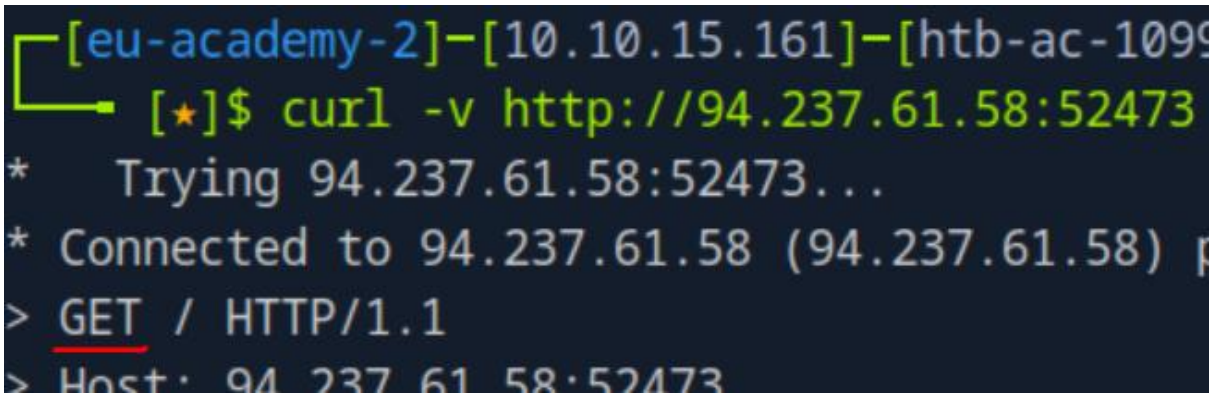
Method 1: lets visit the target website while having the network tab at developer tool on:



Method 2:

We use curl with the flag '-v' to display the request headers:

```
curl -v http://<target-IP>:<target-port>
```



Question: Send a GET request to the above server, and read the response headers to find the version of Apache running on the server, then submit it as the answer. (answer format: X.Y.ZZ)

Answer: 2.4.41

Method: we use 'curl -I' to retreieve the response headers:

```
curl -I http://<target-IP>:<target-port>
```

```
</html>┌─[eu-academy-2]─[10.10.15.161]─[htb
└──╼ [★]$ curl -I http://94.237.61.58:52473
HTTP/1.1 200 OK
Date: Mon, 23 Sep 2024 07:11:50 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
```

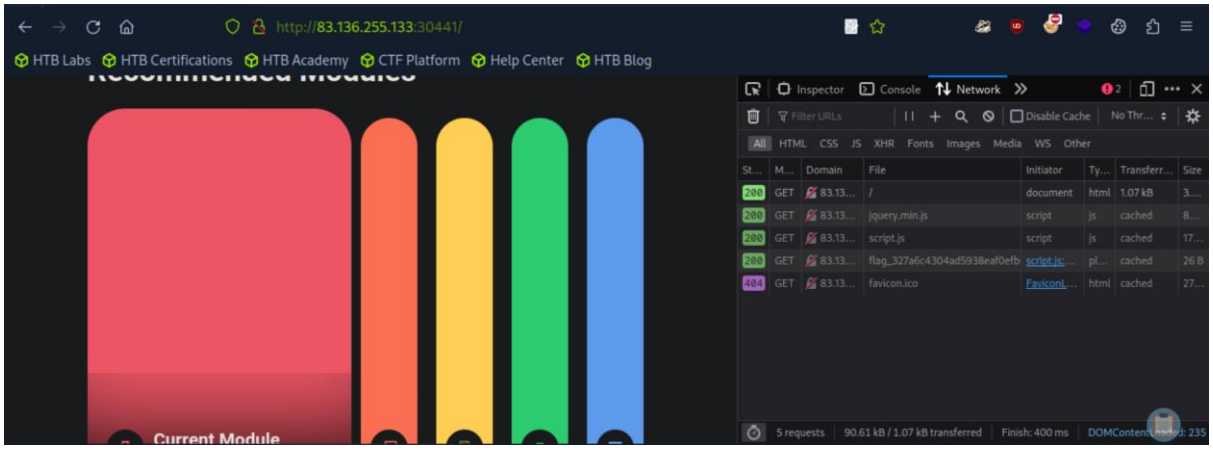
We will have the server header in the response header, along with the server's type (Apache)'s version.

HTTP Headers:

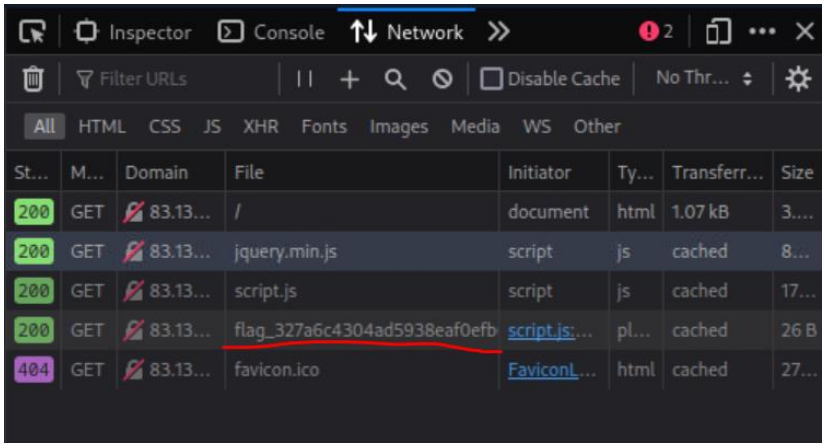
Question: The server above loads the flag after the page is loaded. Use the Network tab in the browser devtools to see what requests are made by the page, and find the request to the flag

Answer: HTB{p493_r3qu3t_m0n!t0r}

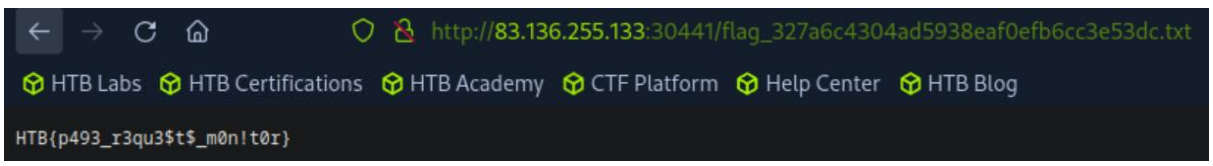
Method: lets open the target website in the browser, while having the development tools → network tab on:



We can see the request to the flag here:



Lets open that page in a new browser tab:



HTTP Methods

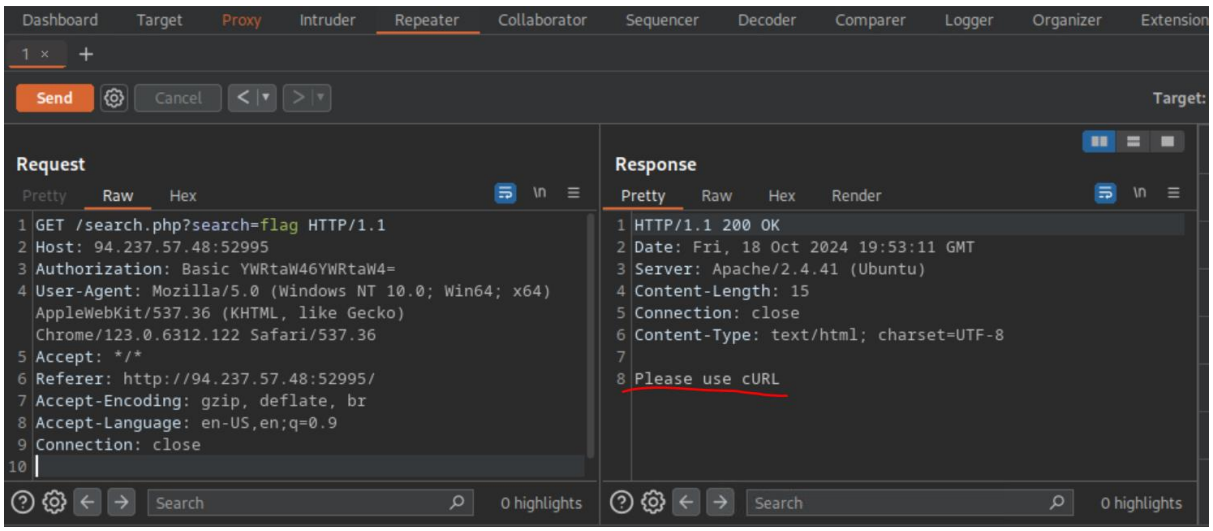
GET:

Question: The exercise above seems to be broken, as it returns incorrect results. Use the browser devtools to see what is the request it is sending when we search, and use cURL to search for 'flag' and obtain the flag.

Answer: HTB{curl_g3773r}

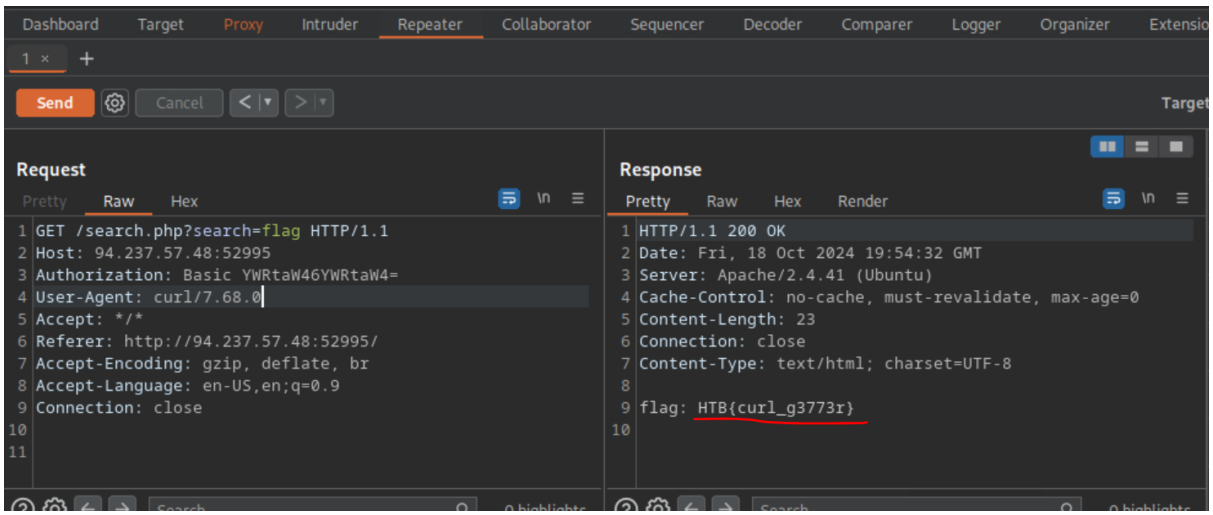
Method: burpsuite repeater will visualize it better.

Original request:



in the response we are requested to use curl.

Instead of doing that, we will simply replace the User-Agent to curl:

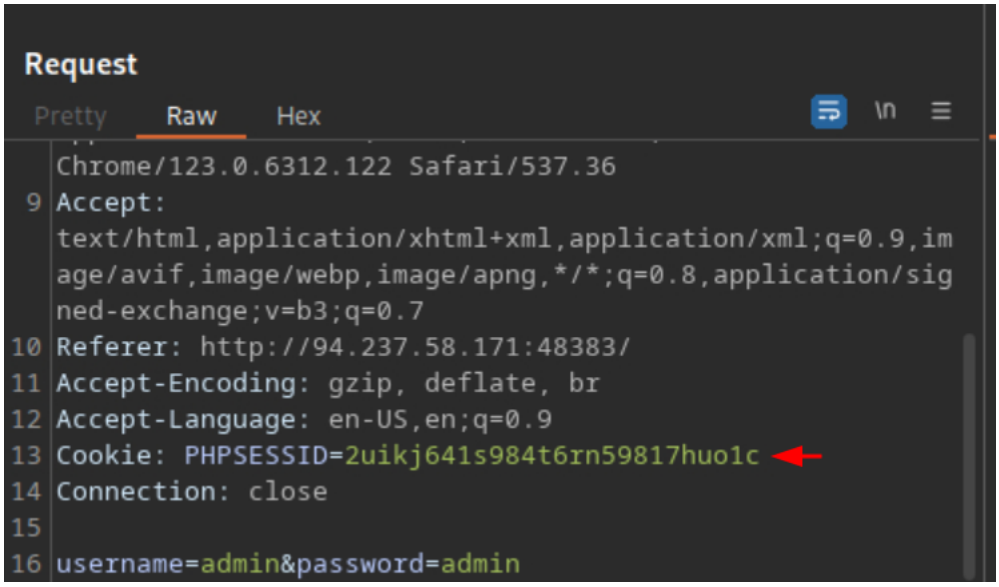


POST:

Question: Obtain a session cookie through a valid login, and then use the cookie with cURL to search for the flag through a JSON POST request to '/search.php'

Answer: HTB{p0$t_r3p34t3r}

Method: First, we will login with the credentials of 'admin:admin' to obtain the cookie's value (using burpsuite):



Once the cookie is obtained and we are loggin in, we can use curl to send the request, looking for the flag:

```
curl -X POST -d '{"search":"flag"}' -b
'PHPSESSID=2uikj641s984t6rn59817huo1c' -H 'Content-Type:
application/json' http://<target-IP>:<target-
port>/search.php
```

We can also use burpsuite search request, chaning the user-agent value to 'curl/7.88.1'.

CRUD API:

Question: First, try to update any city's name to be 'flag'. Then, delete any city. Once done, search for a city named 'flag' to get the flag.

Answer: HTB{crud_4p!_m4n!pul4t0r}

Method: we run the sequence of the following commands:

```
curl -X PUT http://<target-IP>:<target-
port>/api.php/city/london -d '{"city_name":"flag",
"country_name":"HTB"}' -H 'Content-Type: application/json'

curl -X DELETE http://<target-IP>:<target-
port>/api.php/city/south

curl -s http://<target-IP>:<target-port>/api.php/city/flag |
jq
```

*note – the cities of ‘London’ and ‘South’ were picked randomly from the output of the cities list, using the command:

```
curl -s http://<target-IP>:<target-port>/api.php/city | jq
```

*