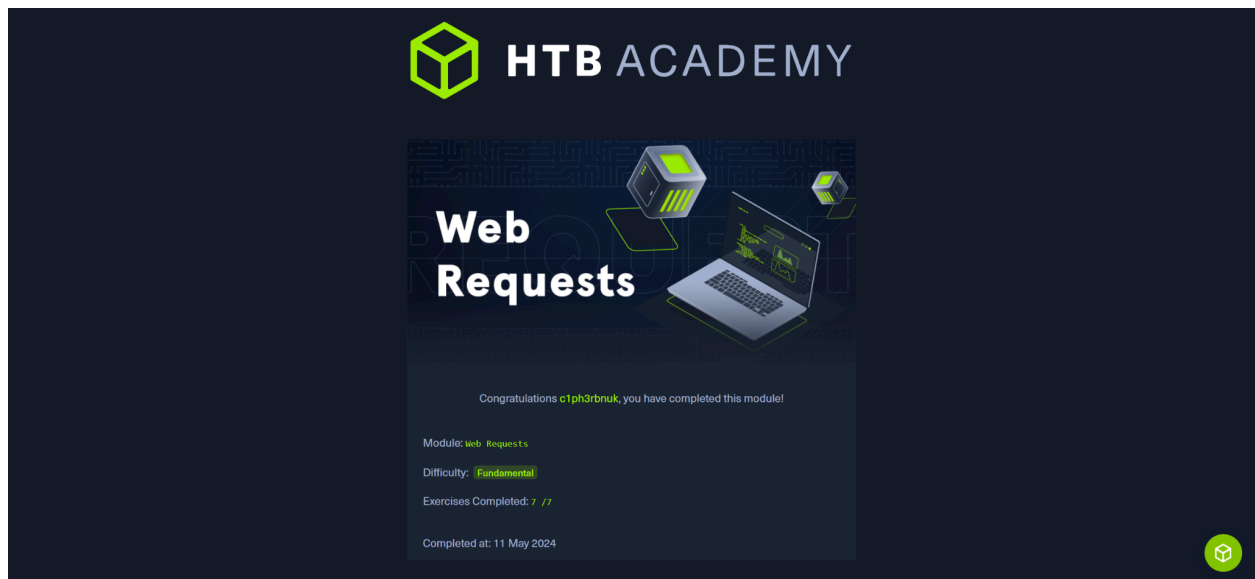


WEB REQUESTS

ASSIGNMENT REPORT



Peter Kinyumu,
cs-sa07-24067,
May 11th, 2024.

1. INTRODUCTION

This report documents my completion of the **Web Requests** Module on the HacktheBox platform. This module covered the essentials of HTTP requests and how to send HTTP requests using different HTTP methods with tools like CuRL. Understanding these core concepts of web requests and APIs is crucial for security analysts to successfully and competently conduct web application security testing.

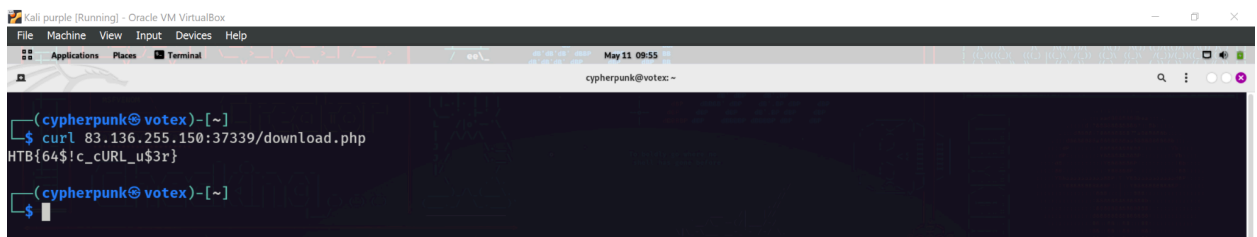
Module completion link

<https://academy.hackthebox.com/achievement/144829/35>

2. ANSWERS TO QUESTIONS

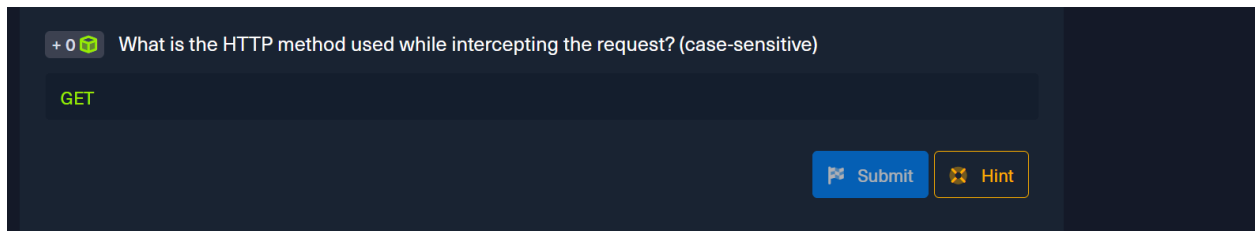
HTTP Fundamentals

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



```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
cypherpunk@vortex: ~
(cypherpunk@vortex)~$ curl 83.136.255.150:37339/download.php
HTB{64$!c_cURL_u$3r}
(cypherpunk@vortex)~$
```

- b. Intercepting requests is a form of MITM(Man in the Middle) attack which uses the GET method.



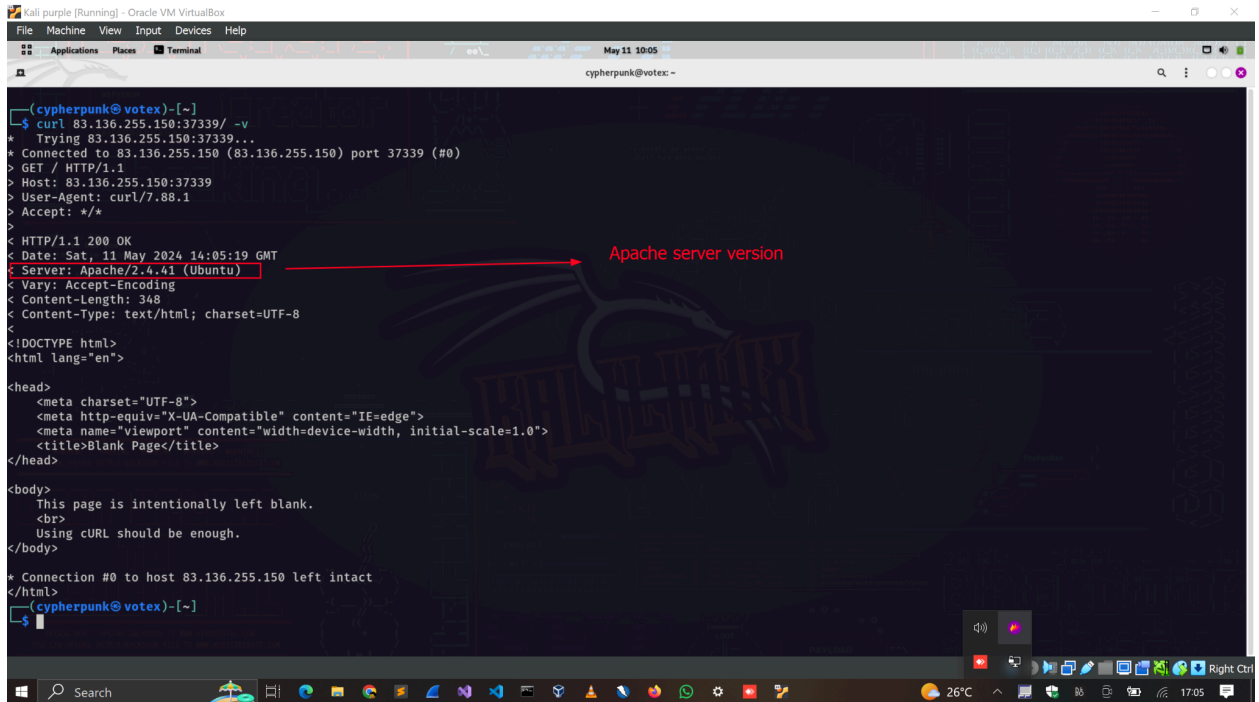
+ 0 What is the HTTP method used while intercepting the request? (case-sensitive)

GET

Submit Hint

- c. 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)

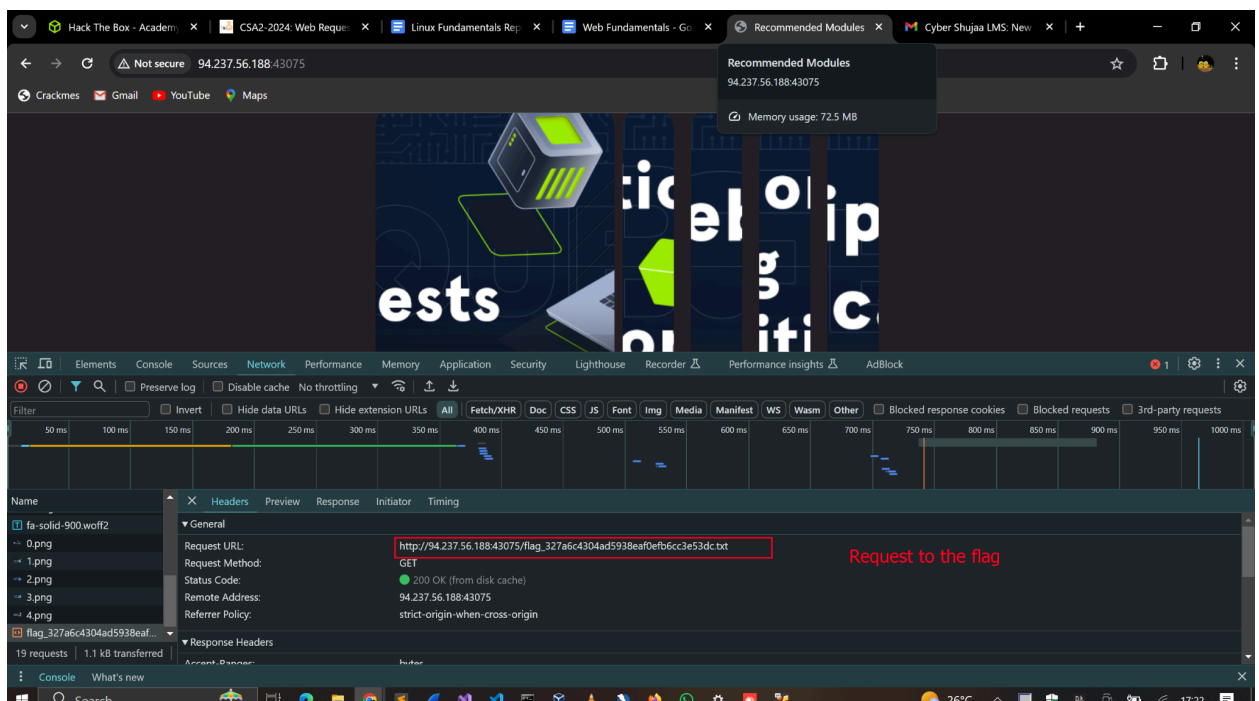
The switch -v instructs curl to be verbose therefore printing information about the request and the response.

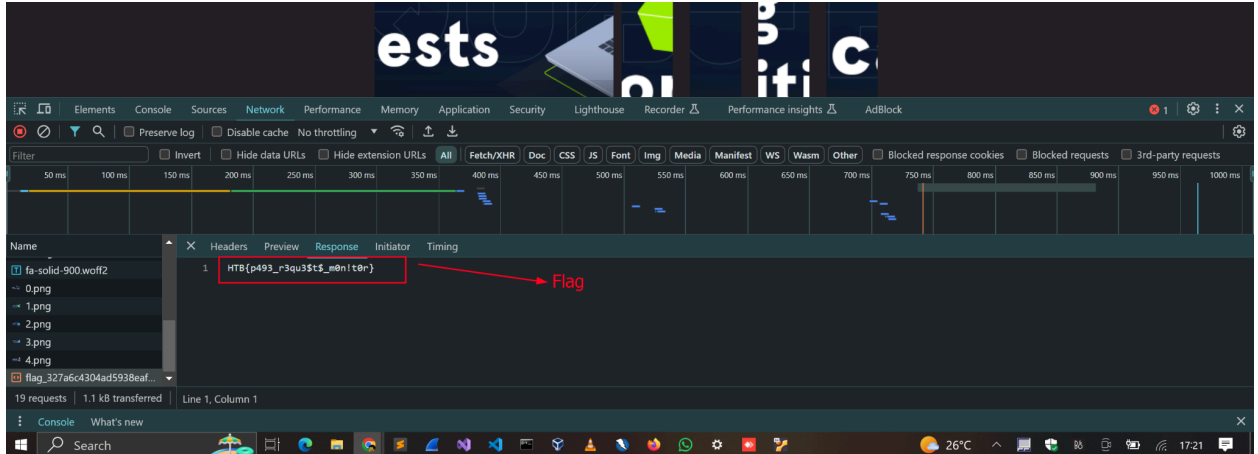


```
(cyberpunk@votex)-[~]
$ curl 83.136.255.150:37339/ -v
* Trying 83.136.255.150:37339...
* Connected to 83.136.255.150 (83.136.255.150) port 37339 (#0)
> GET / HTTP/1.1
> Host: 83.136.255.150:37339
> User-Agent: curl/7.88.1
> Accept: */*
< HTTP/1.1 200 OK
< Date: Sat, 11 May 2024 14:05:19 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Vary: Accept-Encoding
< Content-Length: 348
< Content-Type: text/html; charset=UTF-8
<
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Blank Page</title>
</head>
<body>
  This page is intentionally left blank.
  <br>
  Using cURL should be enough.
</body>
* Connection #0 to host 83.136.255.150 left intact
</html>
(cyberpunk@votex)-[~]
```

- d. 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.

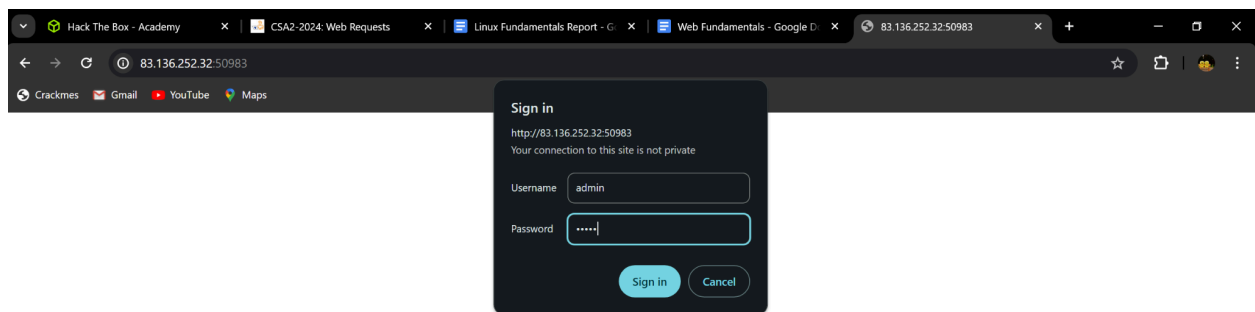
Once the request to retrieve the flag is made, we can note the flag value returned as a response.



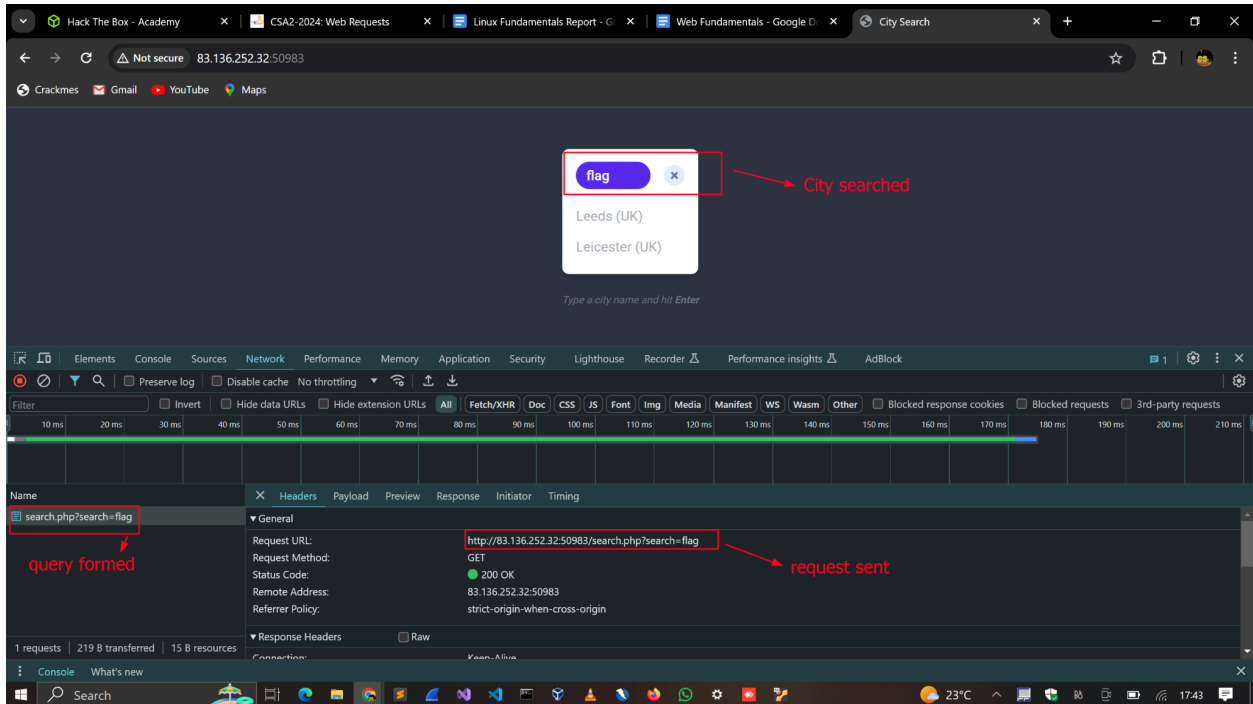


HTTP Methods

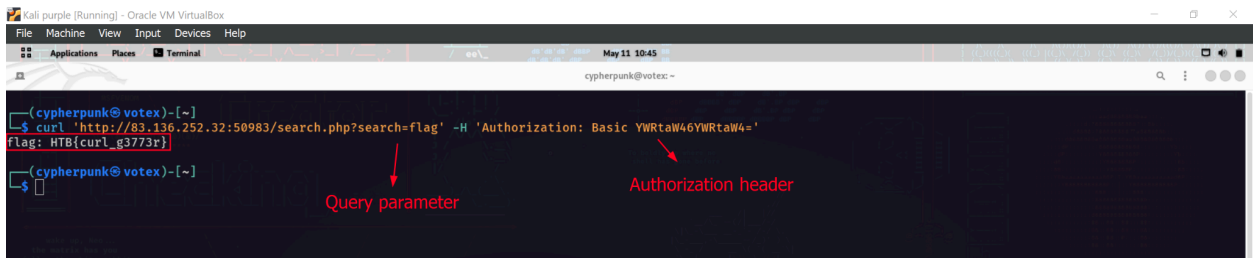
- a. The exercise above seems to be broken, as it returns incorrect results. Use the browser devtools to see what is the request it is sending when we search, and use cURL to search for 'flag' and obtain the flag.



When we search for a city, we can notice that our query is passed to *search.php* forming the search query *search.php?search=flag*

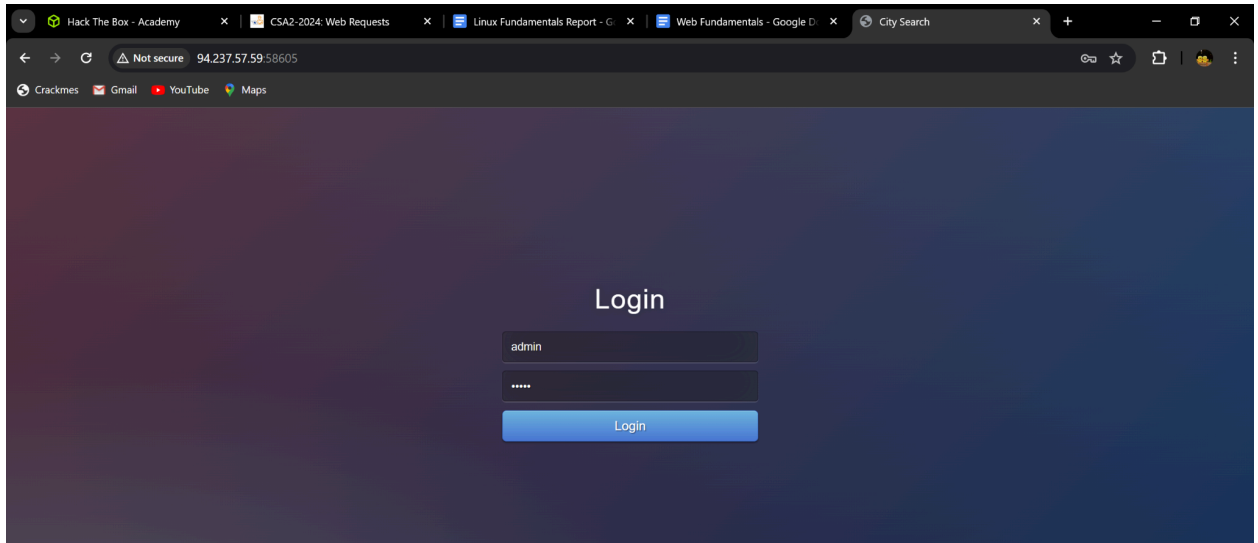


Once we identify the request being sent, we can use CuRL to send a get request to the target and retrieve the flag. Notice we pass the authorization header which is a base64 encoded value of the user credential for authentication.

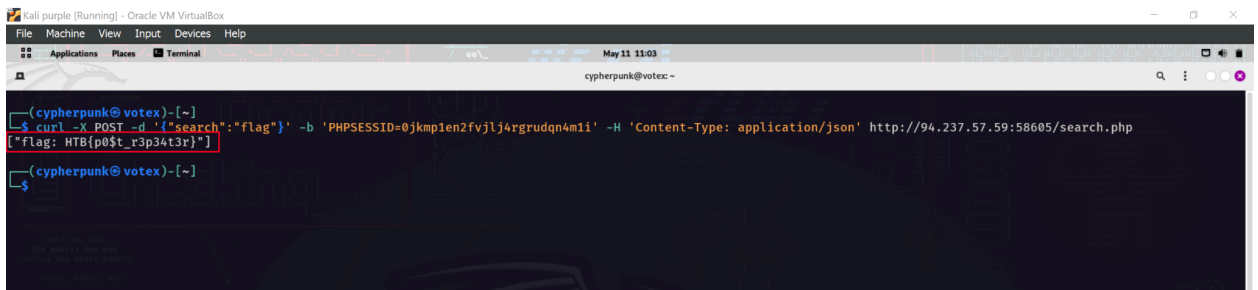
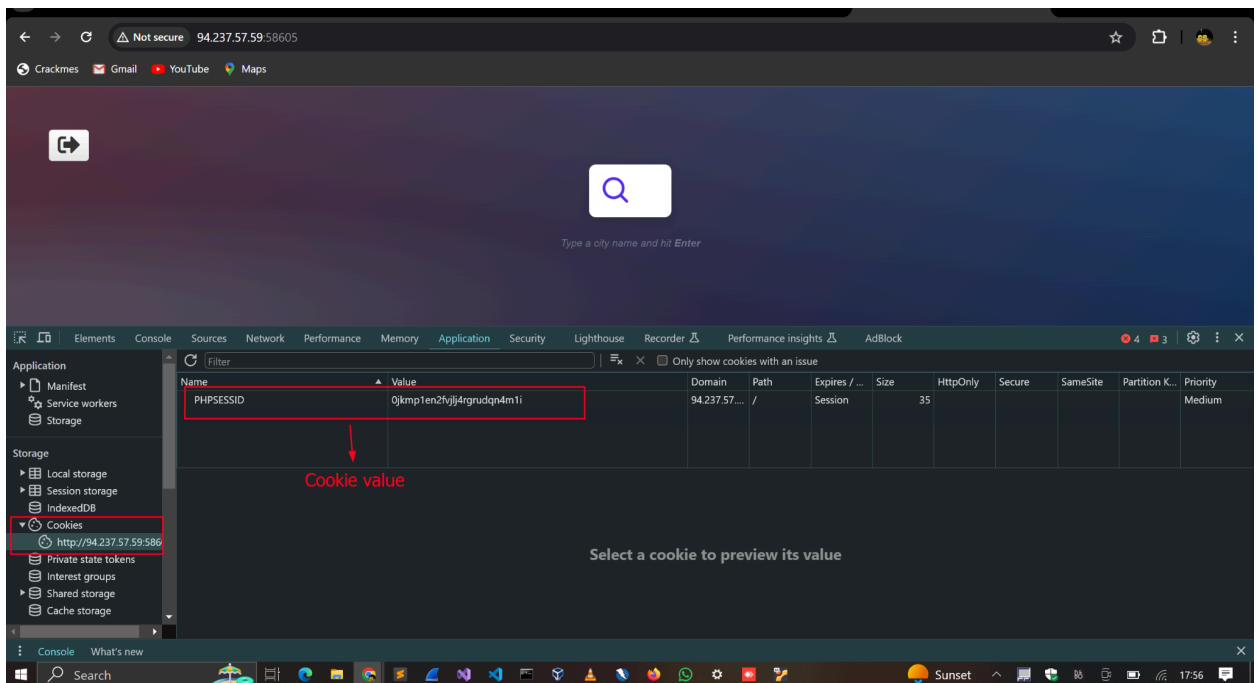


b. Obtain a session cookie through a valid login, and then use the cookie with cURL to search for the flag through a JSON POST request to '/search.php'

We first need to login to the site with valid credentials in order to generate a cookie that we will use to retrieve the flag using the CuRL utility.



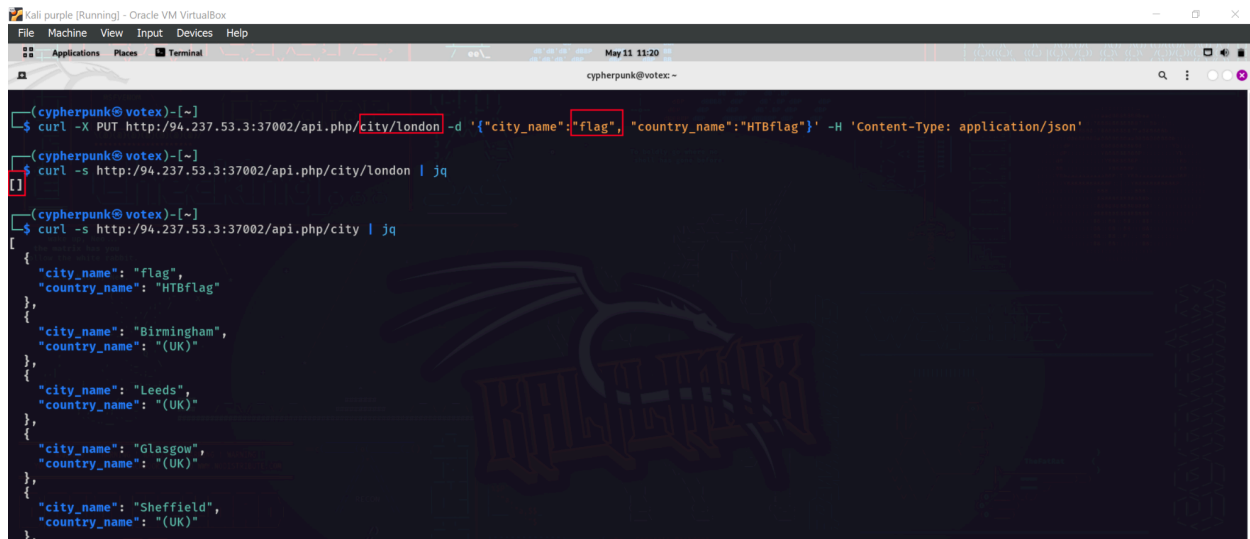
The cookie value can be obtained from **Storage > Cookies**.



Using the cookie value for the authenticated session, we can then send a post request to the target UR, passing the query as JSON data(key-value pair).

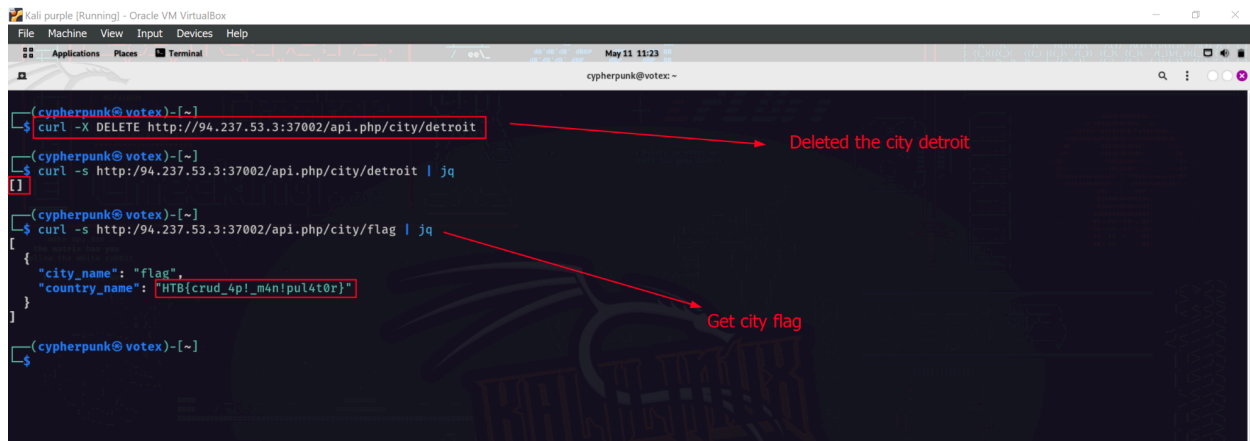
- c. **First, try to update any city's name to be 'flag'. Then, delete any city. Once done, search for a city named 'flag' to get the flag.**

I used CuRL to update the city London to be flag. You can see that when we query for london, it doesn't exist anymore.



```
(cypherpunk@votex)-[~]
$ curl -X PUT http://94.237.53.3:37002/api.php/city/london -d '{"city_name":"flag", "country_name":"HTBflag"}' -H 'Content-Type: application/json'
(cypherpunk@votex)-[~]
$ curl -s http://94.237.53.3:37002/api.php/city/london | jq
[]
(cypherpunk@votex)-[~]
$ curl -s http://94.237.53.3:37002/api.php/city | jq
[
  {
    "city_name": "flag",
    "country_name": "HTBflag"
  },
  {
    "city_name": "Birmingham",
    "country_name": "(UK)"
  },
  {
    "city_name": "Leeds",
    "country_name": "(UK)"
  },
  {
    "city_name": "Glasgow",
    "country_name": "(UK)"
  },
  {
    "city_name": "Sheffield",
    "country_name": "(UK)"
  }
]
```

I then proceeded to delete the city Detroit. When we later query it, it does not exist. Finally, when we query the city flag we retrieve the flag value as the country name.



```
(cypherpunk@votex)-[~]
$ curl -X DELETE http://94.237.53.3:37002/api.php/city/detroit
(cypherpunk@votex)-[~]
$ curl -s http://94.237.53.3:37002/api.php/city/detroit | jq
[]
(cypherpunk@votex)-[~]
$ curl -s http://94.237.53.3:37002/api.php/city/flag | jq
[
  {
    "city_name": "flag",
    "country_name": "HTB{crud_4p!_m4n!pu!4t0r}"
  }
]
(cypherpunk@votex)-[~]
$
```

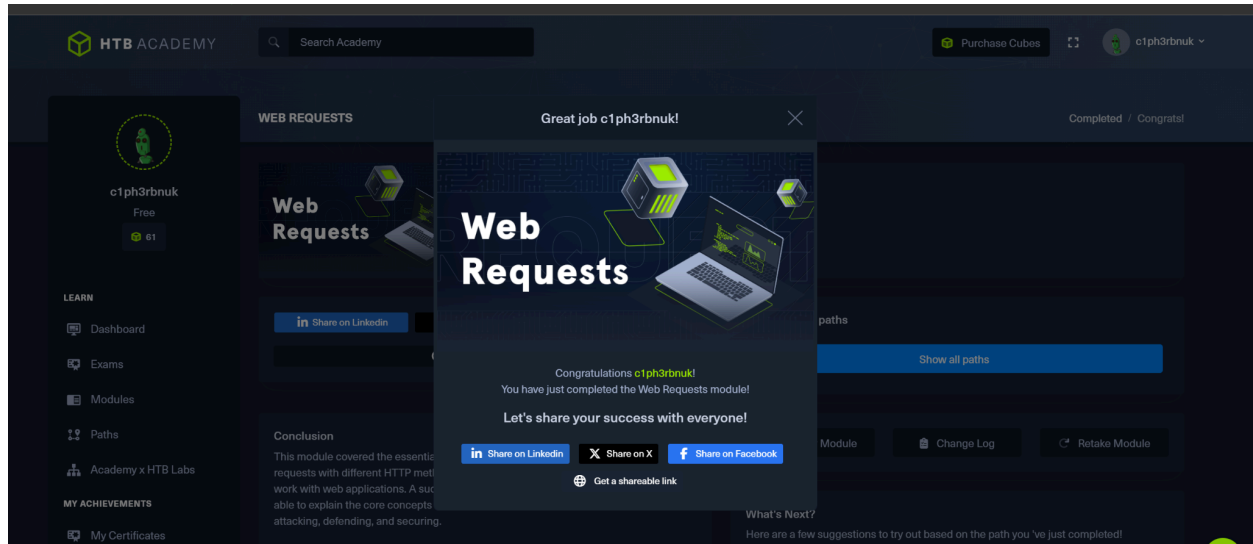
Deleted the city detroit

Get city flag

3. MODULE COMPLETION

The following is a sharable link to the badge I earned after completing the module.

<https://academy.hackthebox.com/achievement/144829/35>



4. CONCLUSION

This module has been very informative and engaging. I have learned how to use the developer tools within the browser and the CuRL utility to send different kinds of requests to API endpoints. Mastering these tools and having them in my arsenal as an aspiring security analyst is empowering. I'm excited to apply them more in the later chapters of the course when testing web applications for vulnerabilities.