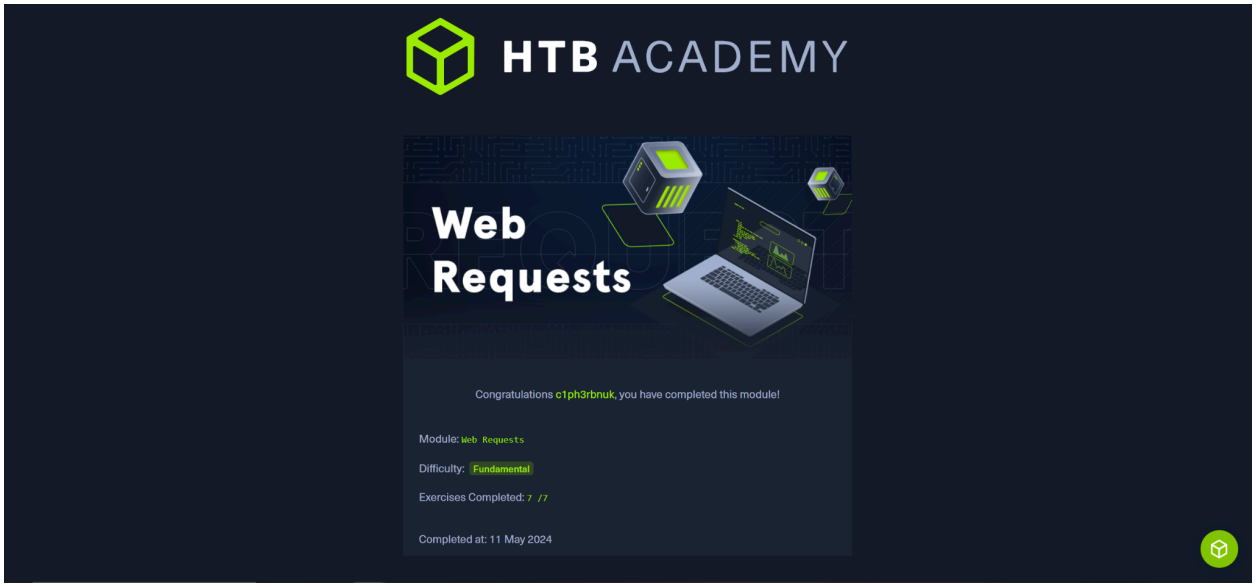
WEB REQUESTS

ASSIGNMENT REPORT



Peter Kinyumu,
cs-sa07-24067,

May 11th, 2024.

1. INTRODUCTION

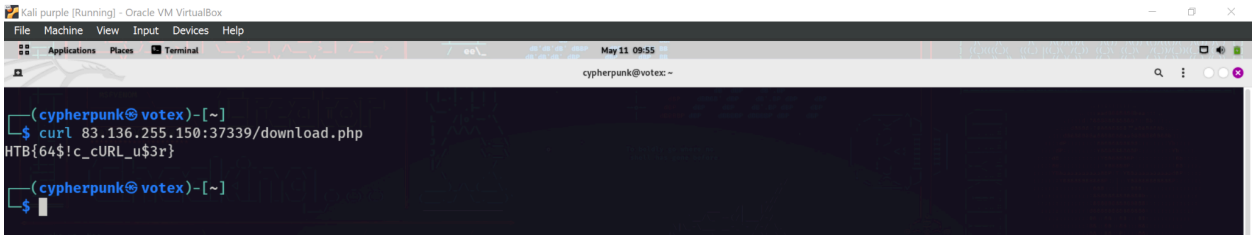
This report documents my completion of the **Web Requests** Module on the HacktheBox platform. This module covered the essentials of HTTP requests and how to send HTTP requests using different HTTP methods with tools like CuRL. Understanding these core concepts of web requests and APIs is crucial for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

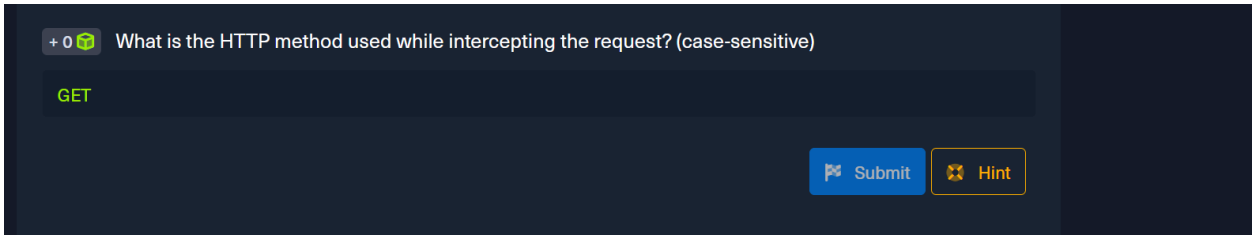
HTTP Fundamentals

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.**



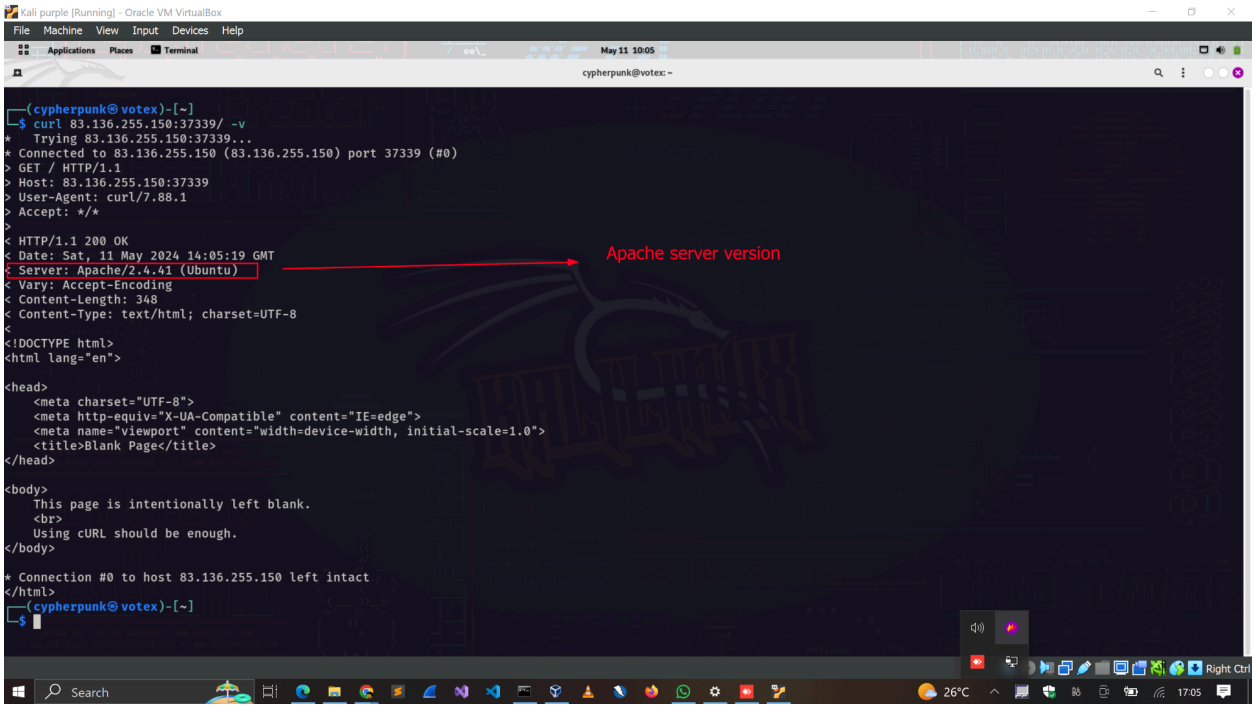
b.

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



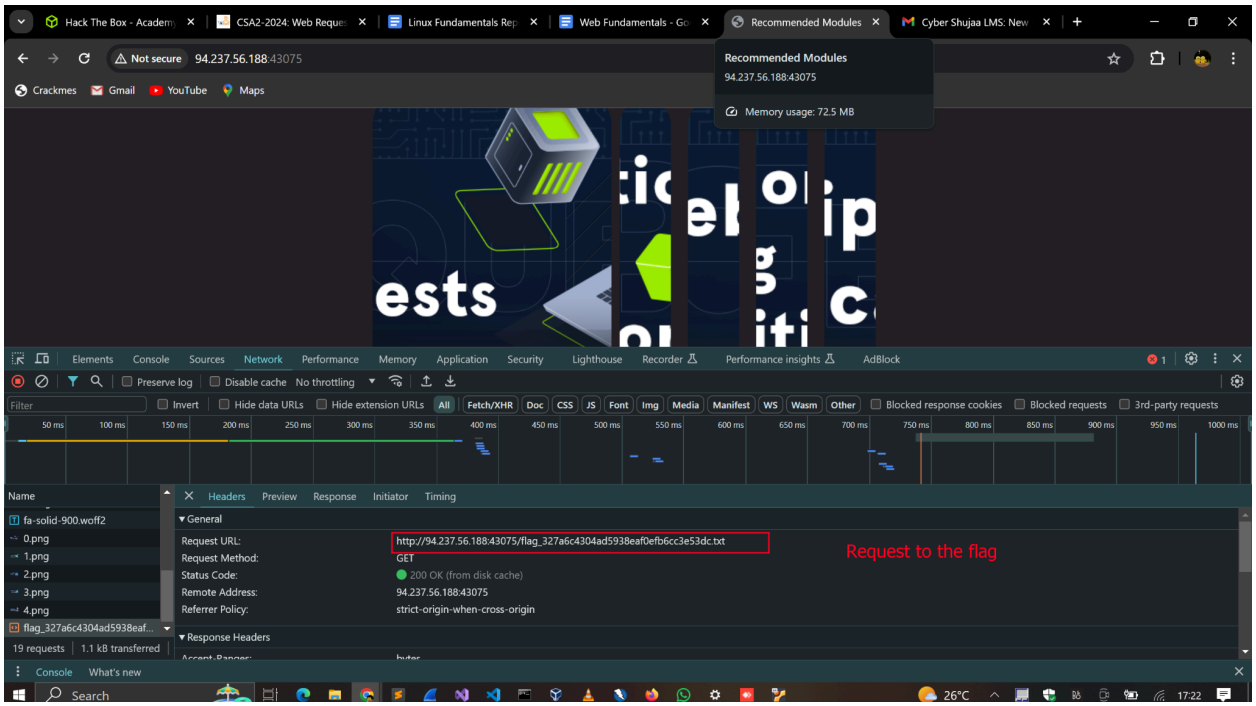
c. **Send a GET request to the above server, and read the response headers to find the version of Apache running on the server, then submit it as the answer. (answer format: X.Y.ZZ)**

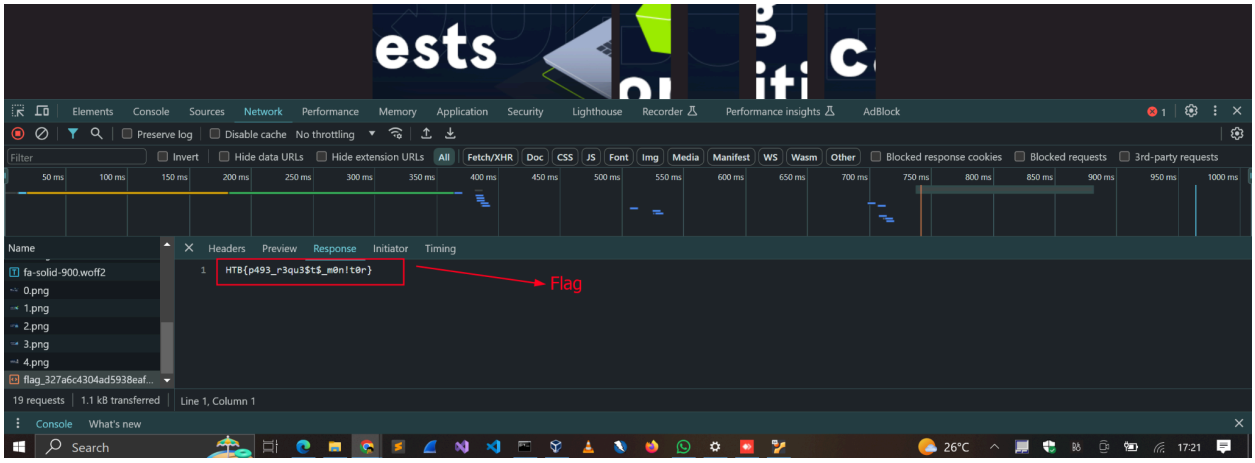
The switch -v instructs curl to be verbose therefore printing information about the request and the response.



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.

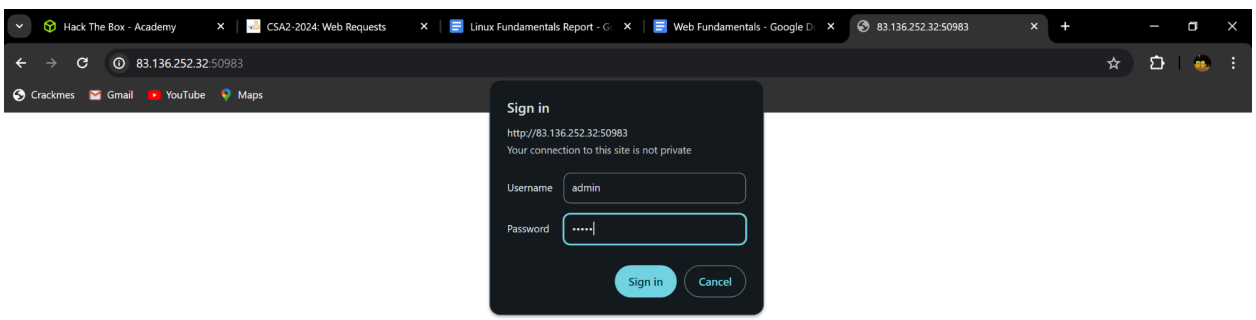
Once the request to retrieve the flag is made, we can note the flag value returned as a response.



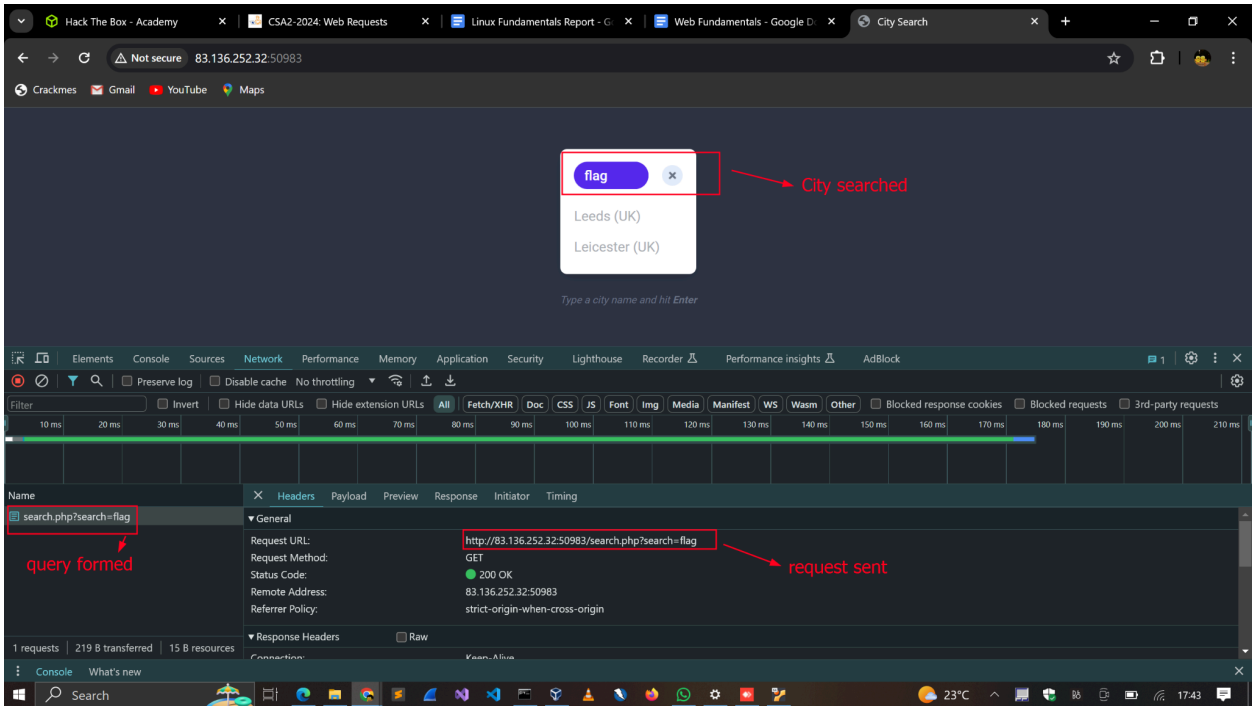


HTTP Methods

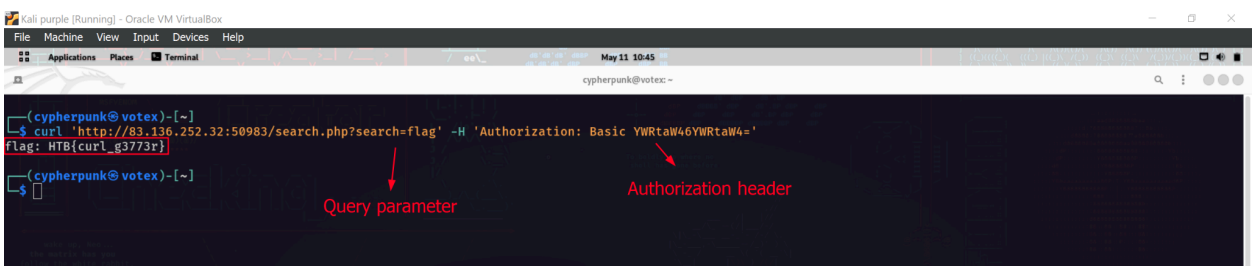
a. **The exercise above seems to be broken, as it returns incorrect results. Use the browser devtools to see what is the request it is sending when we search, and use cURL to search for 'flag' and obtain the flag.**



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***

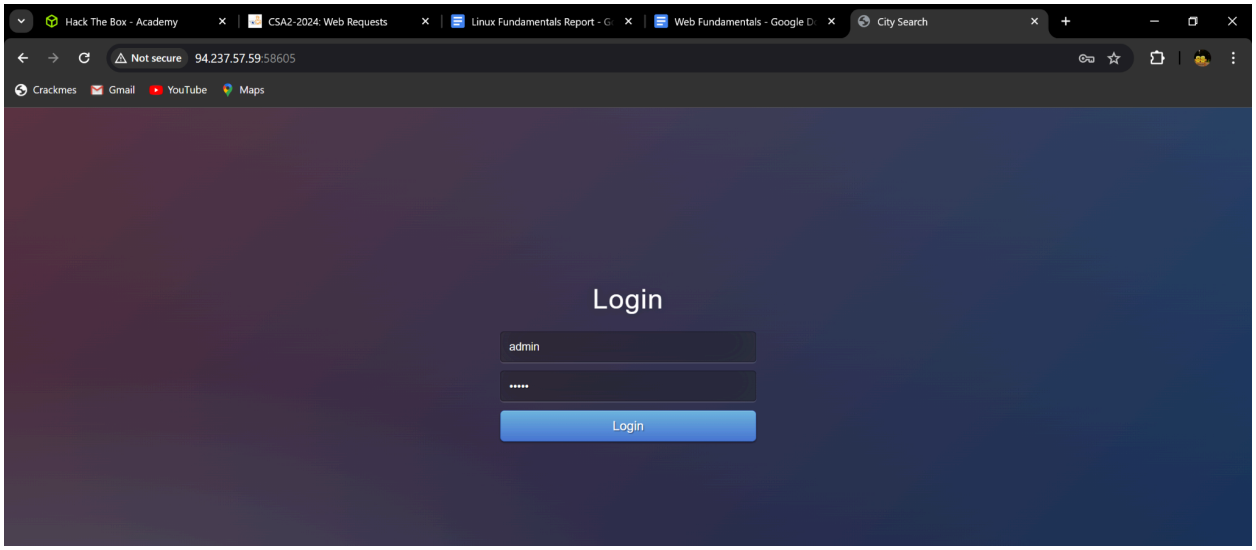


Once we identify the request being sent, we can use CuRL to send a get request to the target and retrieve the flag. Notice we pass the authorization header which is a base64 encoded value of the user credential for authentication.

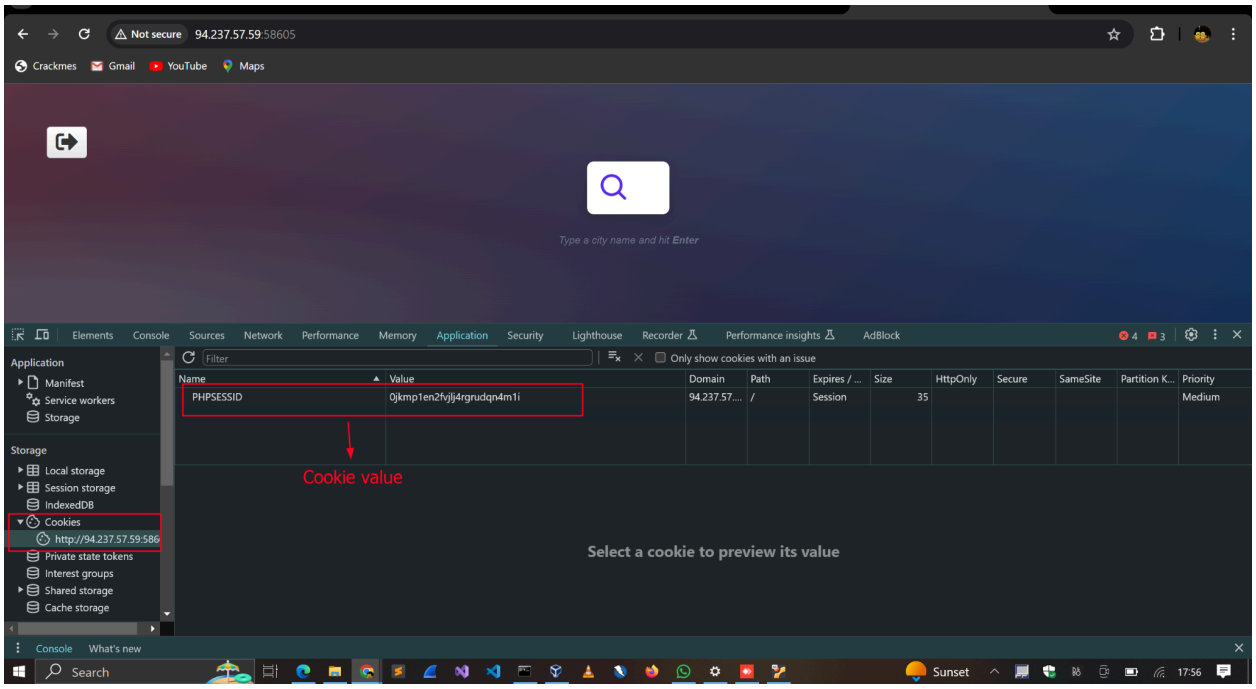


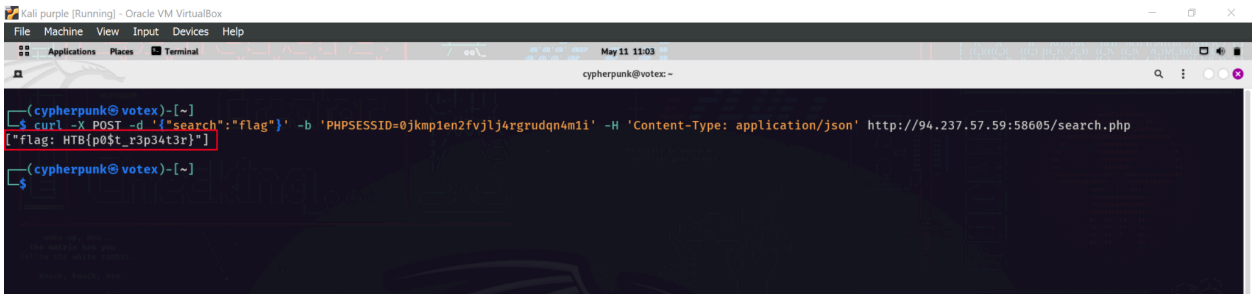
b. Obtain a session cookie through a valid login, and then use the cookie with cURL to search for the flag through a JSON POST request to '/search.php'

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.



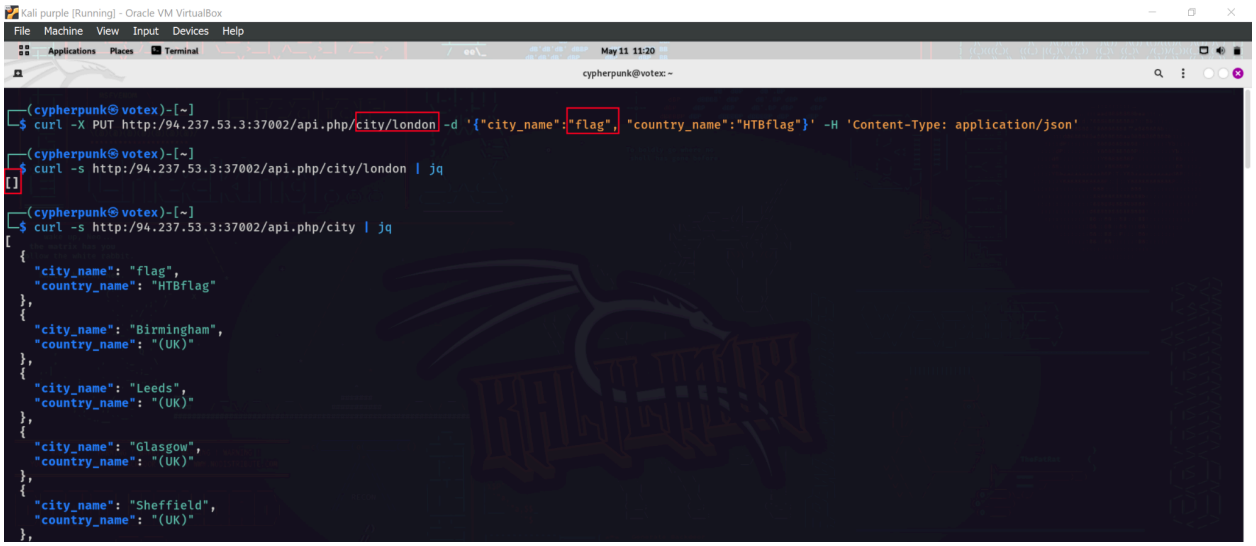
The cookie value can be obtained from **Storage > Cookies**.



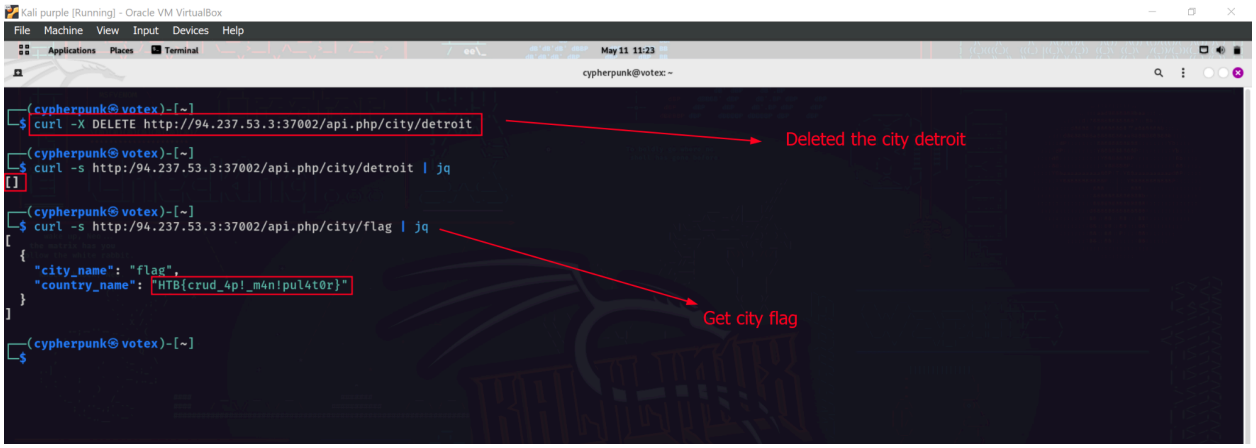


Using the cookie value for the authenticated session, we can then send a post request to the target UR, passing the query as JSON data(key-value pair).

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.

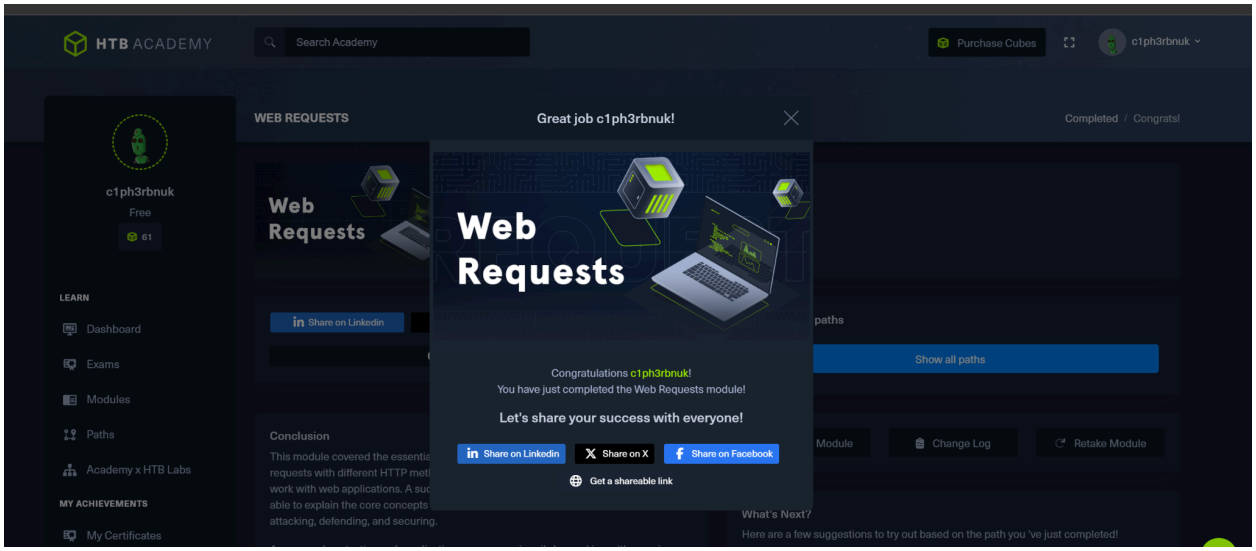


I then proceeded to delete the city Detroit. When we later query it, it does not exist. Finally, when we query the city flag we retrieve the flag value as the country name.



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.