# Week3: **Assignment 3:-HTB Academy – Web Requests**

Report by: **Aisha Khalifan, cs-cns04-23014**

## Introduction

This is a room about Network protocols. In today's digital era, virtually every app we use connects with the internet through HTTP. HyperText Transfer Protocol (HTTP) is the fundamental language that allows us to access content on the web. It follows a client-server model: clients request resources, and servers process and deliver them.

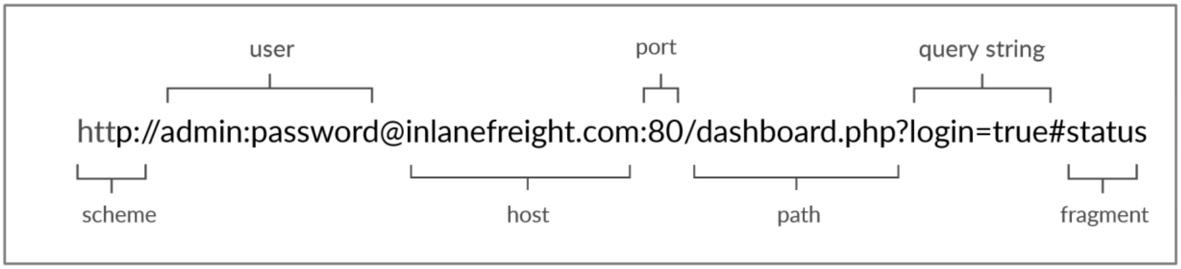
A URL (Uniform Resource Locator) is our entryway to content via HTTP. It's like a structured address: starting with a scheme (like http://) and including components such as host, port, path, query string, and fragments.

Understanding HTTP is crucial for anyone involved in web applications and security. In this report module, we will deal with HTTP methods, how requests and responses are structured, and important tools like cURL for efficient interaction with web services.

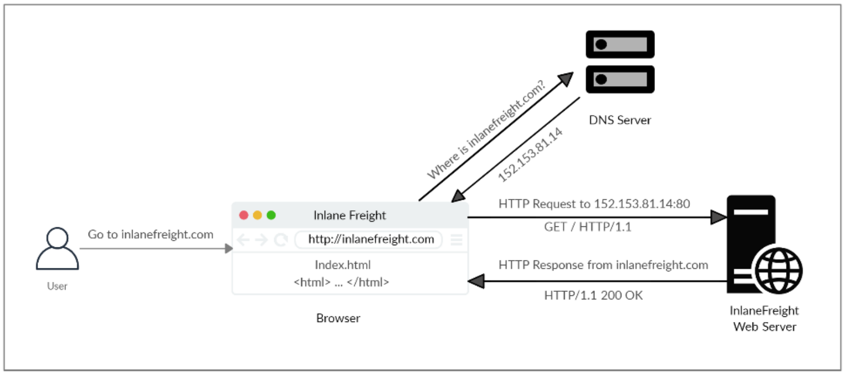
## Methodology

### <u>HTTP Fundamentals</u>

### i. HyperText Transfer Protocol (HTTP)


user
port
query string
http://admin:password@inlanefreight.com:80/dashboard.php?login=true#status
scheme
host
path
fragment

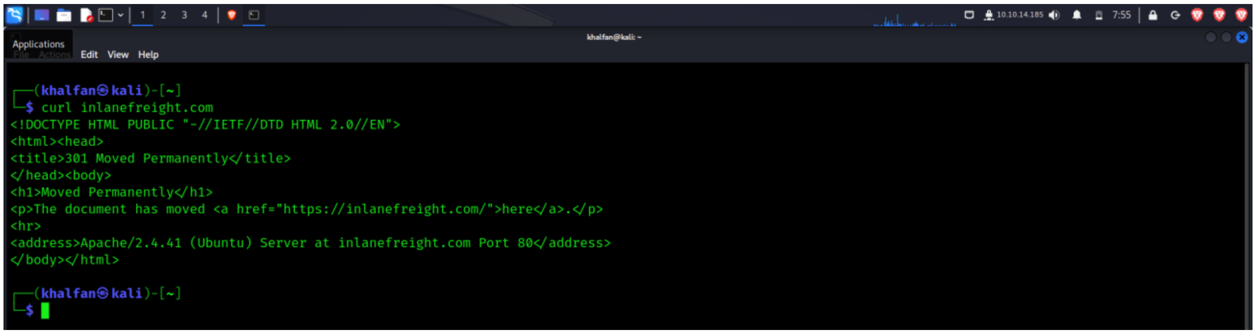
- ♦ Resources over HTTP are accessed via URL(Uniform Resource Locator) which which offers many more specifications than simply specifying a website we want to visit.



- The diagram above presents the anatomy of an HTTP request at a very high level.
- The first time a user enters the URL (inlanefreight.com) into the browser, it sends a request to a DNS (Domain Name Resolution) server to resolve the domain and get its IP.
- The DNS server looks up the IP address for inlanefreight.com and returns it. All domain names need to be resolved this way, as a server can't communicate without an IP address.

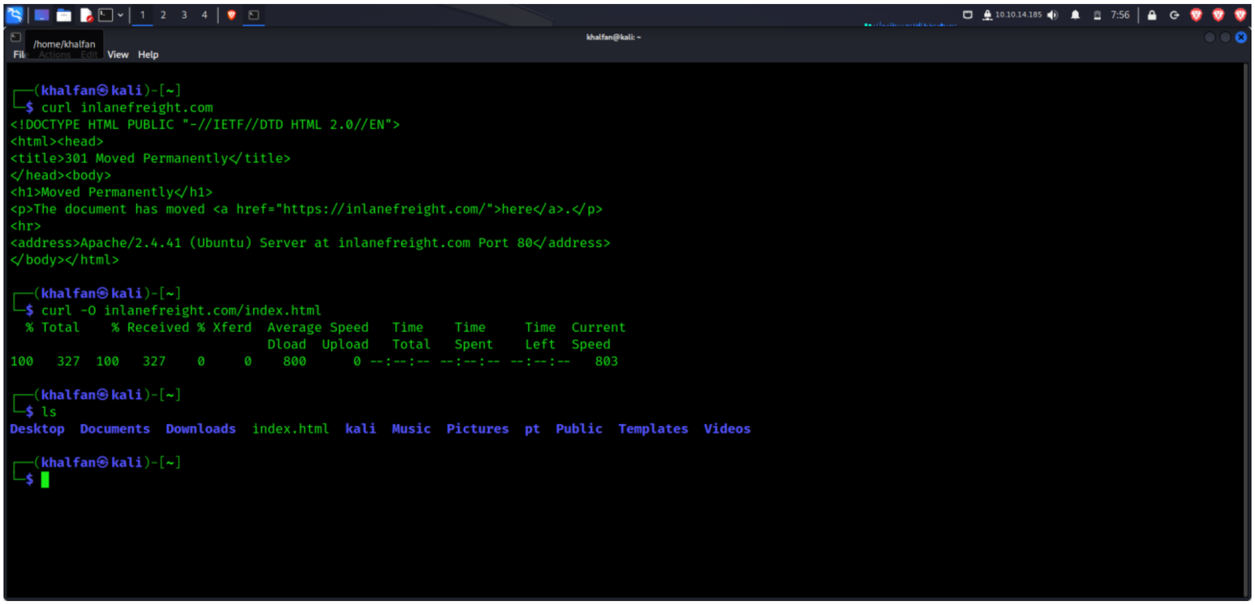
## cURL

- cURL (client URL) is a command-line tool and library that supports HTTP along with many other protocols.
- This makes it a good candidate for scripts as well as automation, making it essential for sending various types of web requests from the command line, which is necessary for many types of web penetration tests.



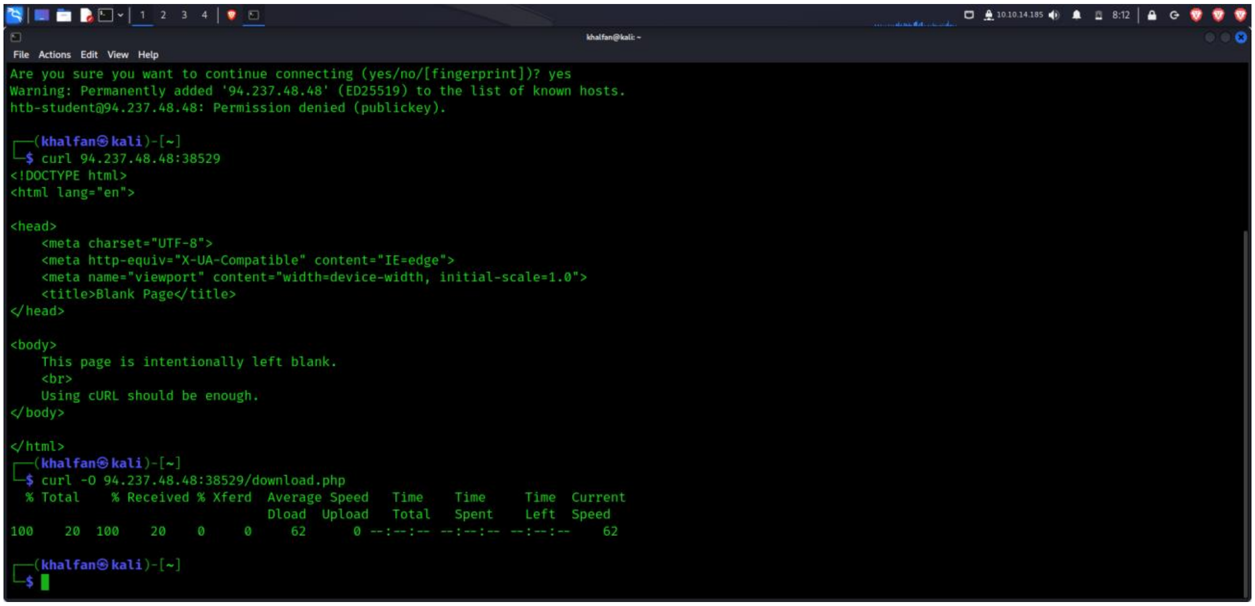
```
┌──(khalfan㉿kali)-[~]
└─$ curl inlanefreight.com
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://inlanefreight.com/">here</a>.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at inlanefreight.com Port 80</address>
</body></html>

┌──(khalfan㉿kali)-[~]
└─$ 
```

- We may also use cURL to download a page or a file and output the content into a file using the -O flag. If we want to specify the output file name, we can use the -o flag and specify the name. Otherwise, we can use -O and cURL will use the remote file name, as follows:



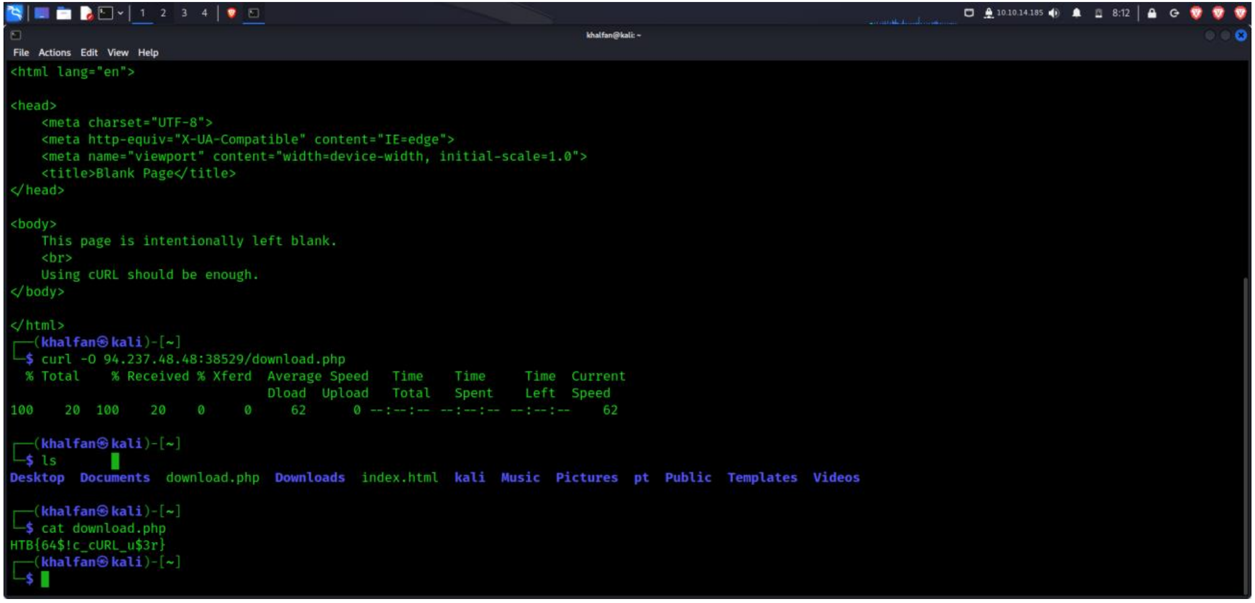
```
┌──(khalfan㉿kali)-[~]
└─$ curl inlanefreight.com
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://inlanefreight.com/">here</a>.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at inlanefreight.com Port 80</address>
</body></html>

┌──(khalfan㉿kali)-[~]
└─$ curl -O inlanefreight.com/index.html
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   327  100   327    0     0    800      0 --:--:-- --:--:-- --:--:--   803

┌──(khalfan㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  index.html  kali  Music  Pictures  pt  Public  Templates  Videos

┌──(khalfan㉿kali)-[~]
└─$ 
```

## Questions



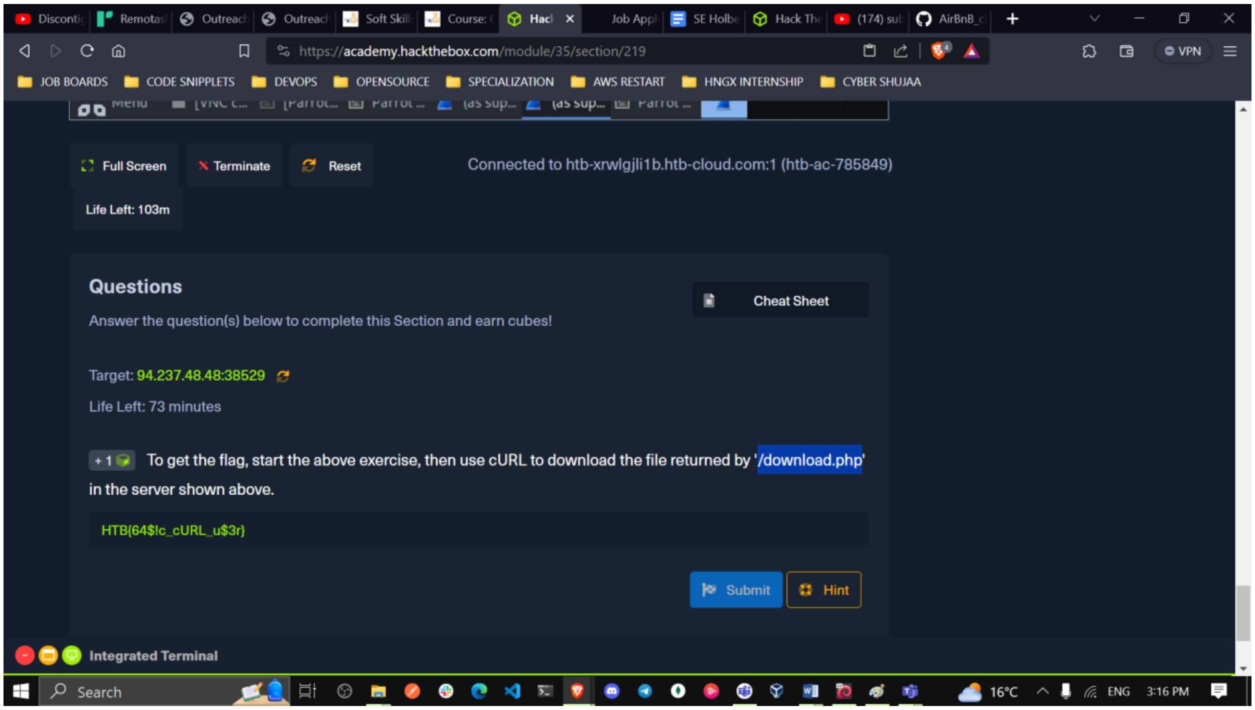
```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '94.237.48.48' (ED25519) to the list of known hosts.
htb-student@94.237.48.48: Permission denied (publickey).

┌──(khalfan㉿kali)-[~]
└─$ curl 94.237.48.48:38529
<!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>

</html>
┌──(khalfan㉿kali)-[~]
└─$ curl -O 94.237.48.48:38529/download.php
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    20  100    20    0     0     62      0 --:--:-- --:--:-- --:--:--    62

┌──(khalfan㉿kali)-[~]
└─$ 
```

- I curl 94.237.48.48:38529
- Then  to download that file /download.php
- curl –o 94.237.48.48:38529/download.php
- then cat to display the contents of download.php



```
<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>

</html>
┌──(khalfan㉿kali)-[~]
└─$ curl -O 94.237.48.48:38529/download.php
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    20  100    20    0     0     62      0 --:--:-- --:--:-- --:--:--    62

┌──(khalfan㉿kali)-[~]
└─$ ls
Desktop  Documents  download.php  Downloads  index.html  kali  Music  Pictures  pt  Public  Templates  Videos

┌──(khalfan㉿kali)-[~]
└─$ cat download.php
HTB{64$!c_cURL_u$3r}
┌──(khalfan㉿kali)-[~]
└─$ 
```

- From the above I get the answers to my question.



Connected to htb-xrwlgjli1b.htb-cloud.com:1 (htb-ac-785849)

Life Left: 103m

Questions

Answer the question(s) below to complete this Section and earn cubes!

Target: 94.237.48.48:38529

Life Left: 73 minutes

+1 To get the flag, start the above exercise, then use cURL to download the file returned by '/download.php' in the server shown above.

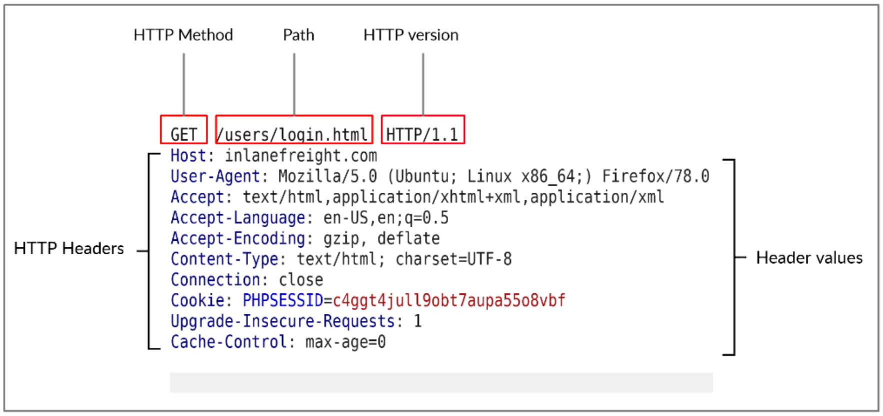
HTB{64$!c_cURL_u$3r}

ii. **HyperText Transfer Protocol Secure (HTTPS)**

iii. **HTTP Requests and Responses**

- An HTTP request is made by the client (e.g. cURL/browser), and is processed by the server (e.g. web server).
- The requests contain all of the details we require from the server, including the resource (e.g. URL, path, parameters), any request data, headers or options we specify, and many other options we will discuss throughout this module.
- Once the server receives the HTTP request, it processes it and responds by sending the HTTP response, which contains the response code, as discussed in a later section, and may contain the resource data if the requester has access to it.

**Example of a request**

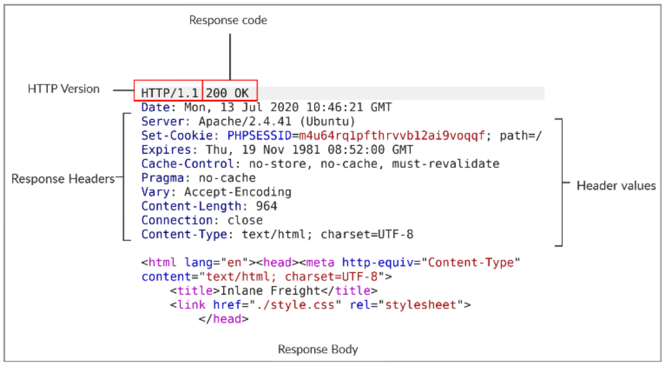


```
GET /users/login.html HTTP/1.1
Host: inlanefreight.com
User-Agent: Mozilla/5.0 (Ubuntu; Linux x86_64;) Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/html; charset=UTF-8
Connection: close
Cookie: PHPSESSID=c4ggt4jull9obt7aupa55o8vbf
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

| **Field** | **Example** | **description** |
|---|---|---|
| Method | GET | **The HTTP method or verb, which specifies the type of action to perform.** |

| | | |
|---|---|---|
| **Path** | /users/login.html | **The path to the resource being accessed. This field can also be suffixed with a query string (e.g. ?username=user).** |
| Version | HTTP/1.1 | The third and final field is used to denote the HTTP version. |

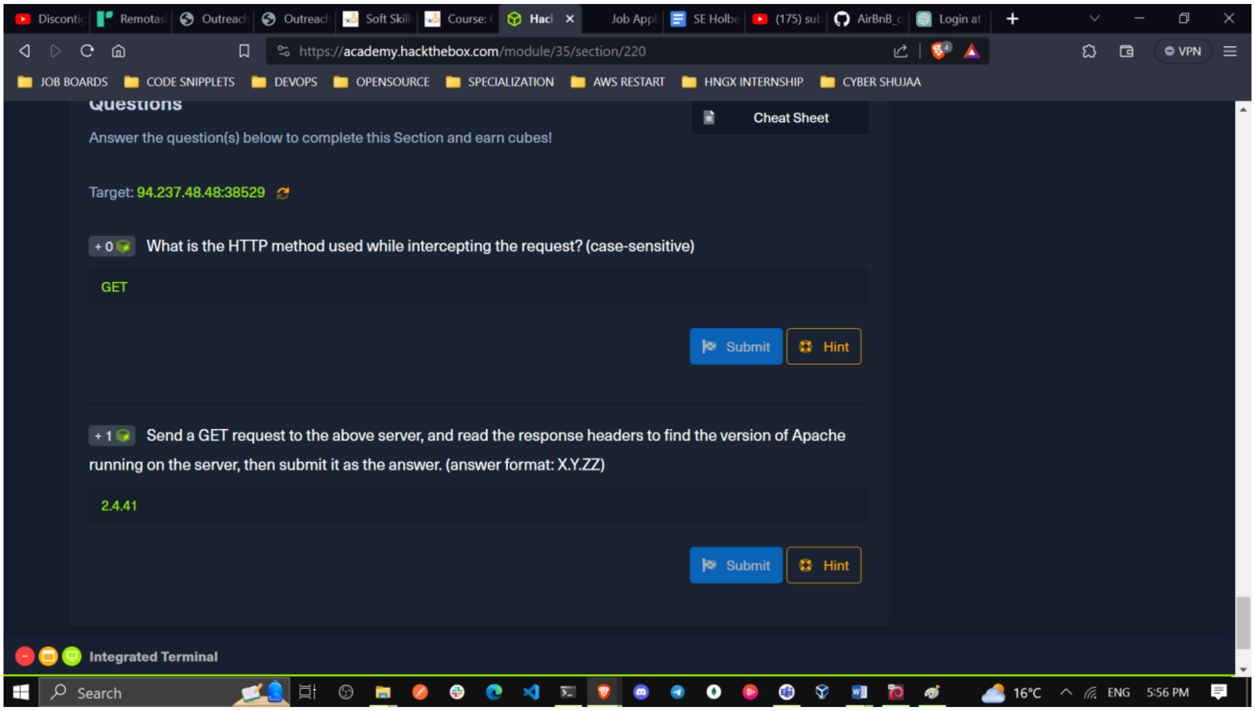
### Example of HTTP Response



```
HTTP/1.1 200 OK
Date: Mon, 13 Jul 2020 10:46:21 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: PHPSESSID=m4u64rqlpfthrvvb12ai9voqqf; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 964
Connection: close
Content-Type: text/html; charset=UTF-8

<html lang="en"><head><meta http-equiv="Content-Type"
content="text/html; charset=UTF-8">
    <title>Inlane Freight</title>
    <link href="./style.css" rel="stylesheet">
        </head>
```

**To send a GET request to the specified target (94.237.48.48:38529) and read the response headers to find the Apache version, you can use the curl command in the terminal. Here's how you can do it:**

**curl -I [http://94.237.48.48:38529](http://94.237.48.48:38529)**



Questions

Answer the question(s) below to complete this Section and earn cubes!

Target: 94.237.48.48:38529

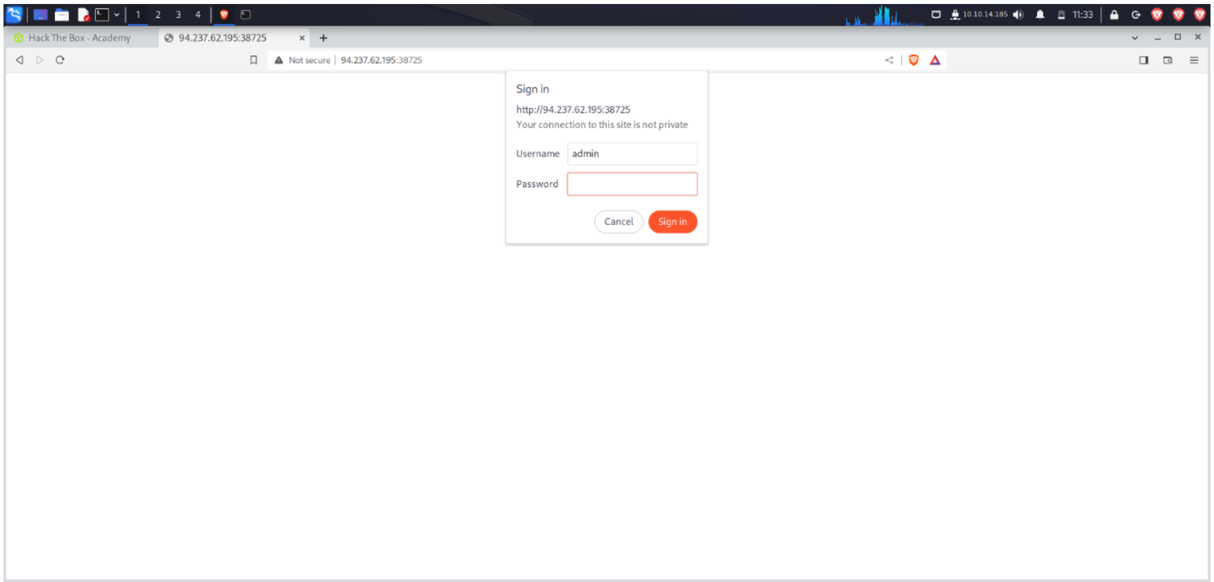
+ 0 What is the HTTP method used while intercepting the request? (case-sensitive)

GET

+ 1 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)

2.4.41

## iv. HTTP Headers



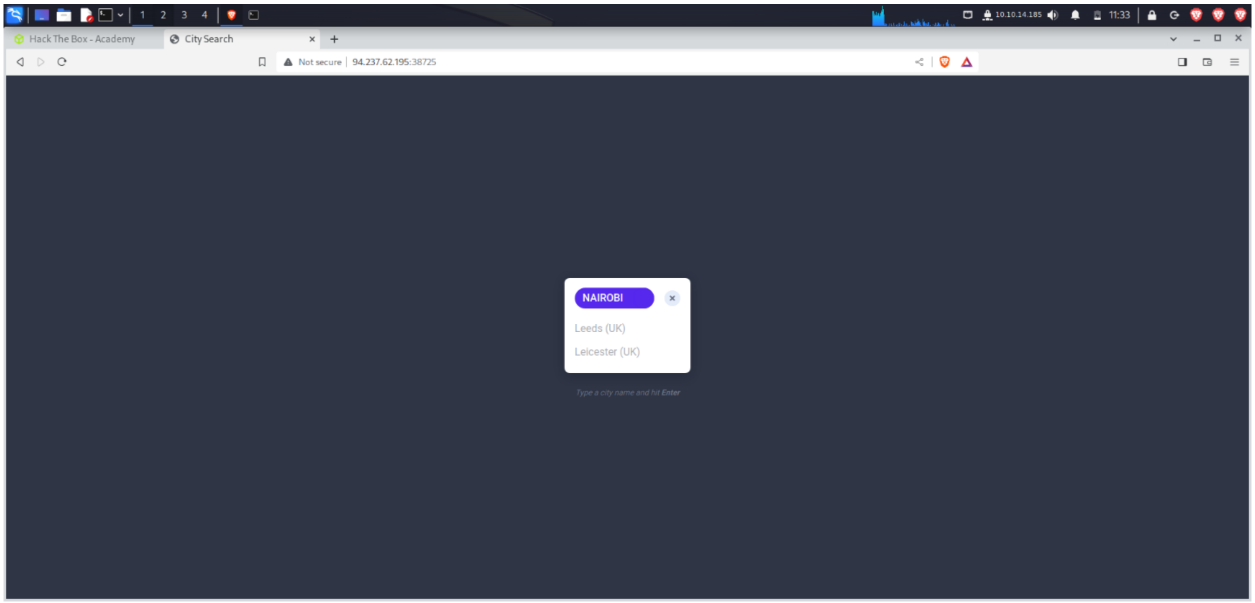
Sign in

http://94.237.62.195:38725

Your connection to this site is not private

Username admin

Password

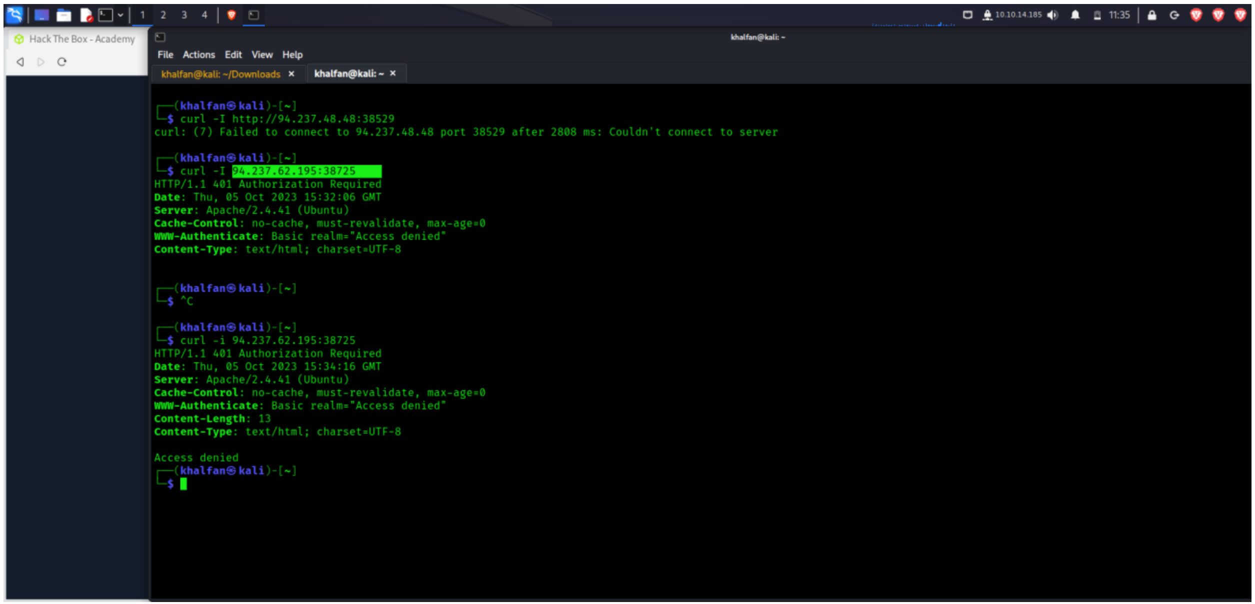


NAIROBI

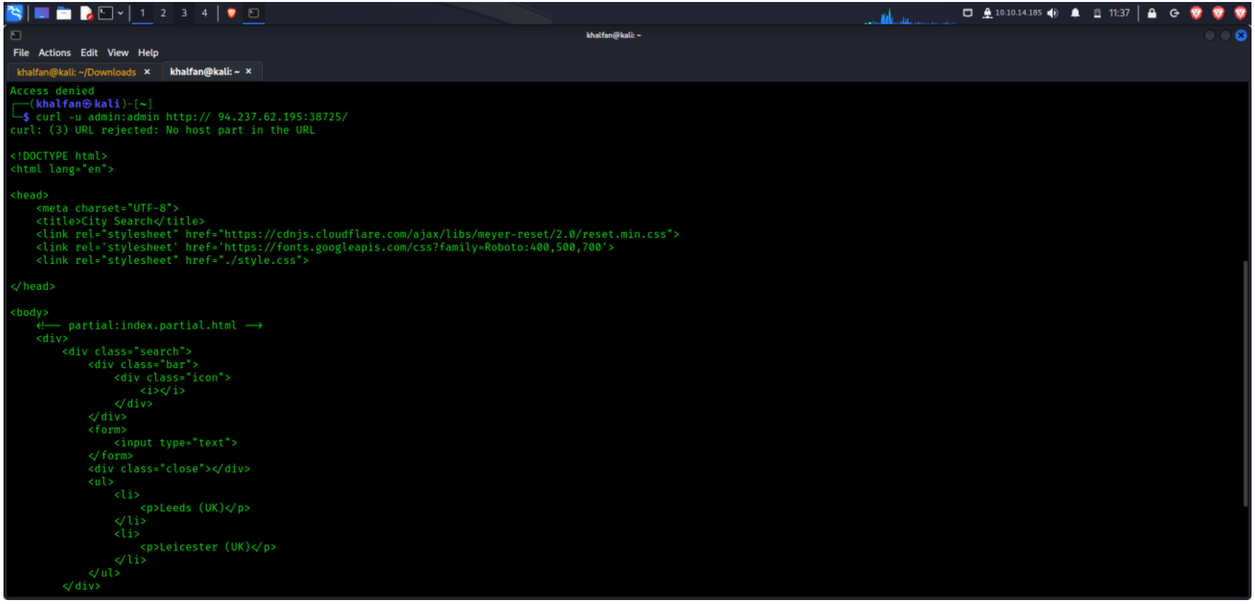
Leeds (UK)

Leicester (UK)

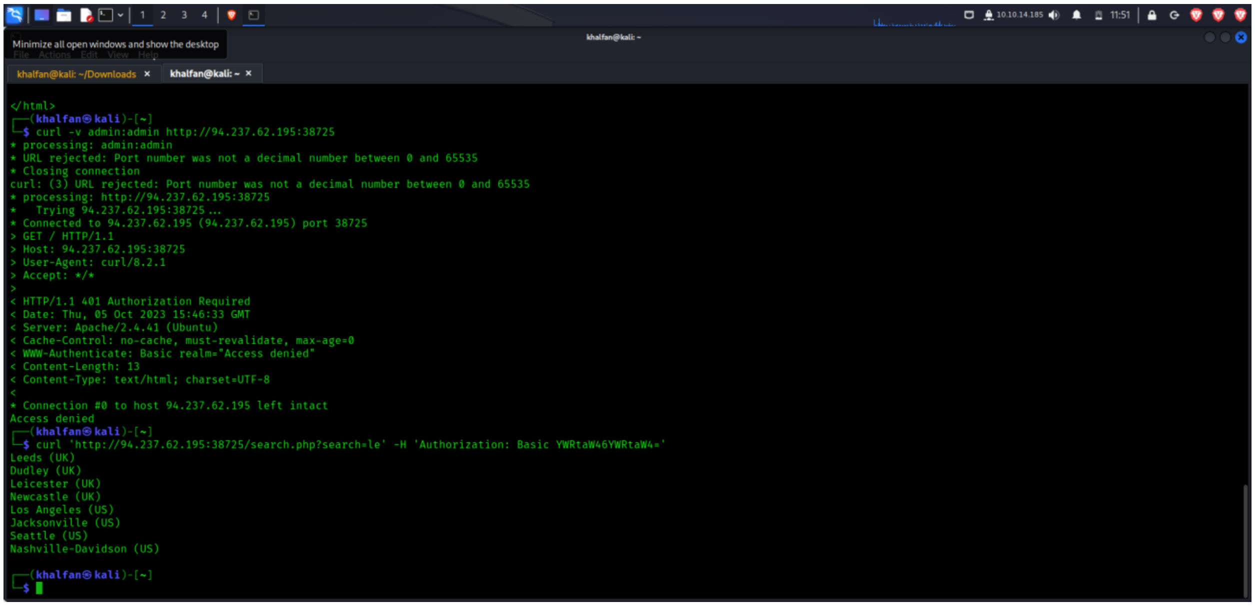
*Type a city name and hit **Enter***



```
┌──(khalfan㉿kali)-[~]
└─$ curl -I http://94.237.48.48:38529
curl: (7) Failed to connect to 94.237.48.48 port 38529 after 2808 ms: Couldn't connect to server

┌──(khalfan㉿kali)-[~]
└─$ curl -I 94.237.62.195:38725
HTTP/1.1 401 Authorization Required
Date: Thu, 05 Oct 2023 15:32:06 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: no-cache, must-revalidate, max-age=0
WWW-Authenticate: Basic realm="Access denied"
Content-Type: text/html; charset=UTF-8


┌──(khalfan㉿kali)-[~]
└─$ ^C

┌──(khalfan㉿kali)-[~]
└─$ curl -i 94.237.62.195:38725
HTTP/1.1 401 Authorization Required
Date: Thu, 05 Oct 2023 15:34:16 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: no-cache, must-revalidate, max-age=0
WWW-Authenticate: Basic realm="Access denied"
Content-Length: 13
Content-Type: text/html; charset=UTF-8

Access denied
┌──(khalfan㉿kali)-[~]
└─$ 
```

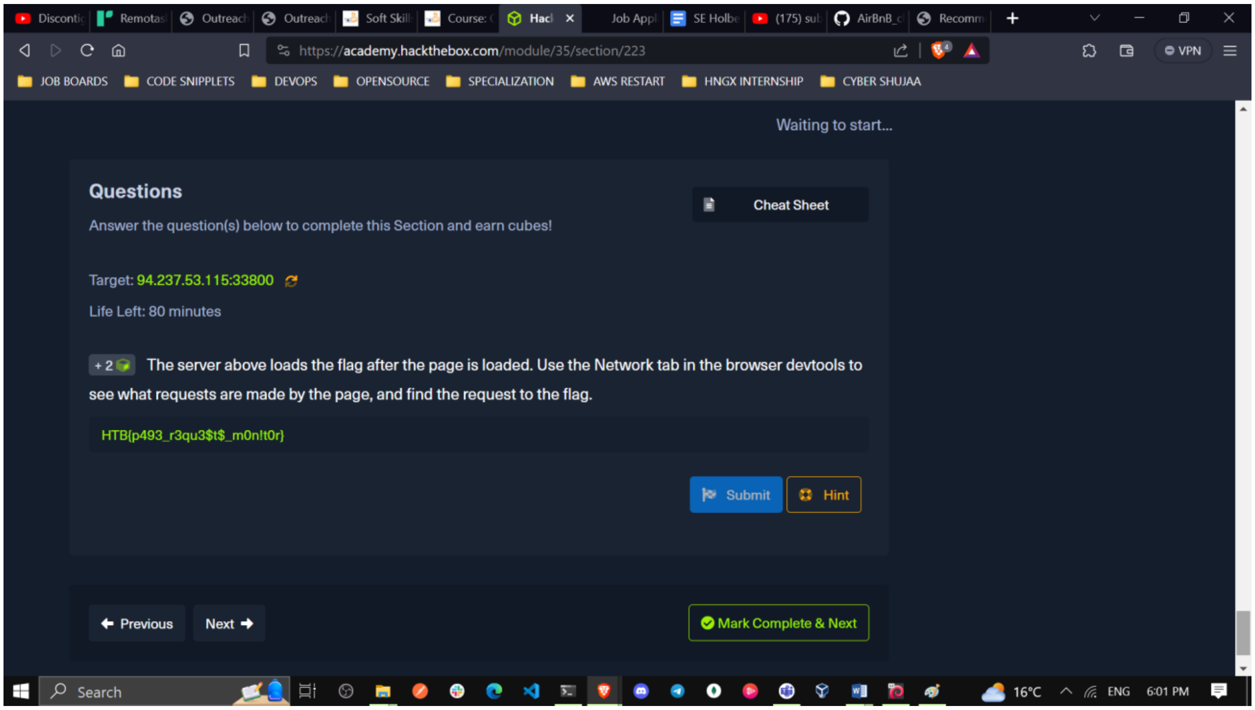


```
Access denied
┌──(khalfan㉿kali)-[~]
└─$ curl -u admin:admin http:// 94.237.62.195:38725/
curl: (3) URL rejected: No host part in the URL

<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="UTF-8">
    <title>City Search</title>
    <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/meyer-reset/2.0/reset.min.css">
    <link rel='stylesheet' href='https://fonts.googleapis.com/css?family=Roboto:400,500,700'>
    <link rel="stylesheet" href="./style.css">

</head>

<body>
    <!-- partial:index.partial.html -->
    <div>
        <div class="search">
            <div class="bar">
                <div class="icon">
                    <i></i>
                </div>
            </div>
            <form>
                <input type="text">
            </form>
            <div class="close"></div>
            <ul>
                <li>
                    <p>Leeds (UK)</p>
                </li>
                <li>
                    <p>Leicester (UK)</p>
                </li>
            </ul>
        </div>
```



Minimize all open windows and show the desktop
khalfan@kali: ~/Downloads
khalfan@kali: ~

```
</html>
┌──(khalfan㉿kali)-[~]
└─$ curl -v admin:admin http://94.237.62.195:38725
* processing: admin:admin
* URL rejected: Port number was not a decimal number between 0 and 65535
* Closing connection
curl: (3) URL rejected: Port number was not a decimal number between 0 and 65535
* processing: http://94.237.62.195:38725
*   Trying 94.237.62.195:38725 ...
* Connected to 94.237.62.195 (94.237.62.195) port 38725
> GET / HTTP/1.1
> Host: 94.237.62.195:38725
> User-Agent: curl/8.2.1
> Accept: */*
>
< HTTP/1.1 401 Authorization Required
< Date: Thu, 05 Oct 2023 15:46:33 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Cache-Control: no-cache, must-revalidate, max-age=0
< WWW-Authenticate: Basic realm="Access denied"
< Content-Length: 13
< Content-Type: text/html; charset=UTF-8
<
* Connection #0 to host 94.237.62.195 left intact
Access denied
┌──(khalfan㉿kali)-[~]
└─$ curl 'http://94.237.62.195:38725/search.php?search=le' -H 'Authorization: Basic YWRtaW46YWRtaW4='
Leeds (UK)
Dudley (UK)
Leicester (UK)
Newcastle (UK)
Los Angeles (US)
Jacksonville (US)
Seattle (US)
Nashville-Davidson (US)

┌──(khalfan㉿kali)-[~]
└─$
```



**Questions**

Answer the question(s) below to complete this Section and earn cubes!

Target: 94.237.53.115:33800

Life Left: 80 minutes

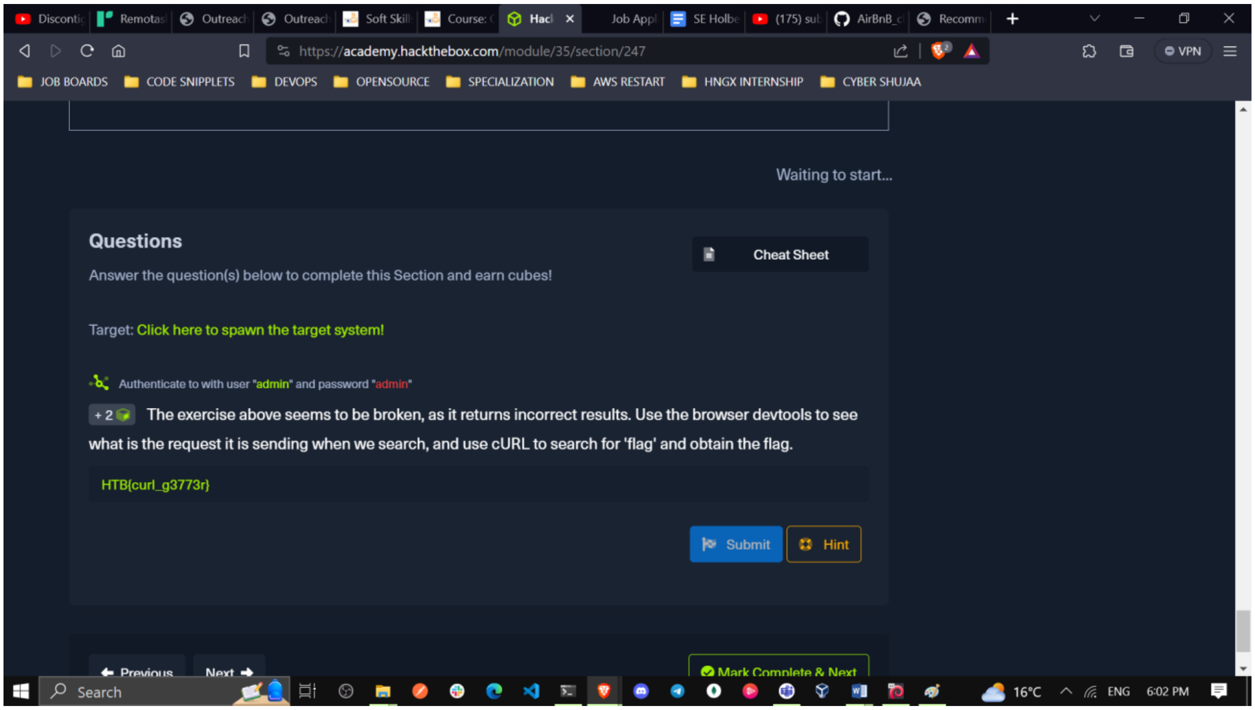
+2 The server above loads the flag after the page is loaded. Use the Network tab in the browser devtools to see what requests are made by the page, and find the request to the flag.

HTB{p493_r3qu3$t$_m0n!t0r}

## HTTP Methods

i. **HTTP Methods and Codes**

ii. **GET**



Waiting to start...

**Questions**

Answer the question(s) below to complete this Section and earn cubes!

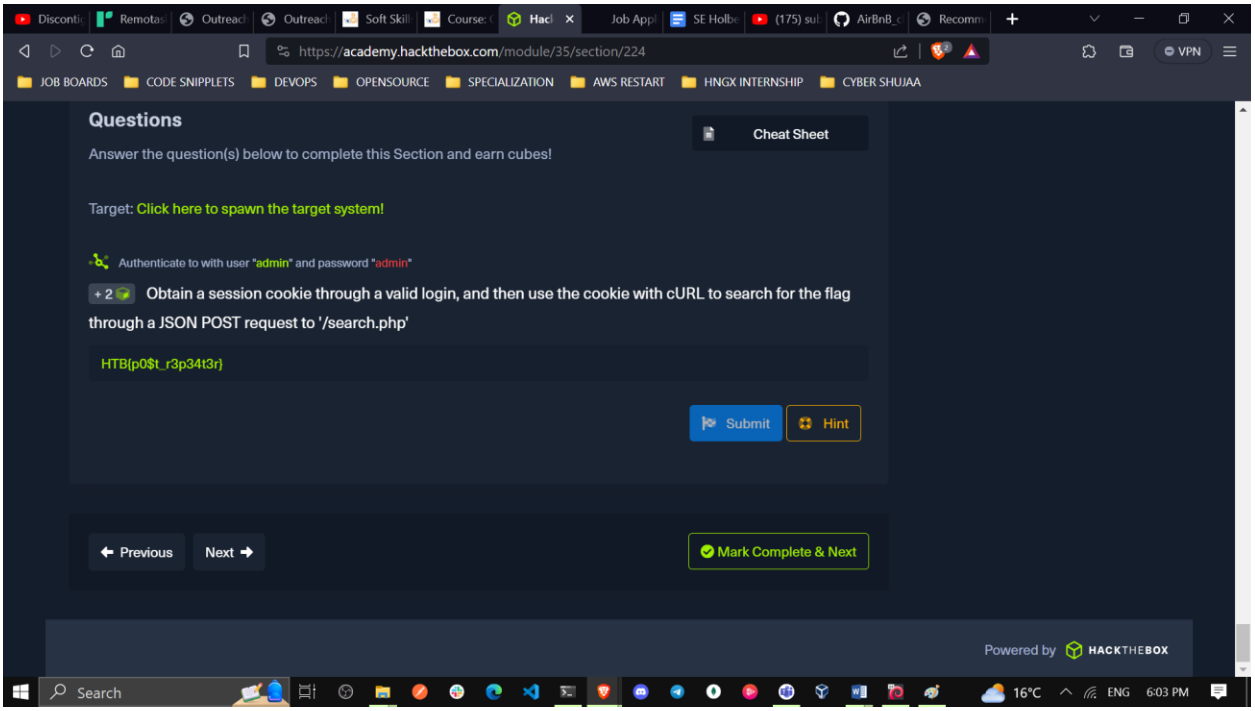
Target: Click here to spawn the target system!

Authenticate to with user "admin" and password "admin"

+2 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.

HTB{curl_g3773r}

iii. **POST**



**Questions**

Answer the question(s) below to complete this Section and earn cubes!

Target: Click here to spawn the target system!

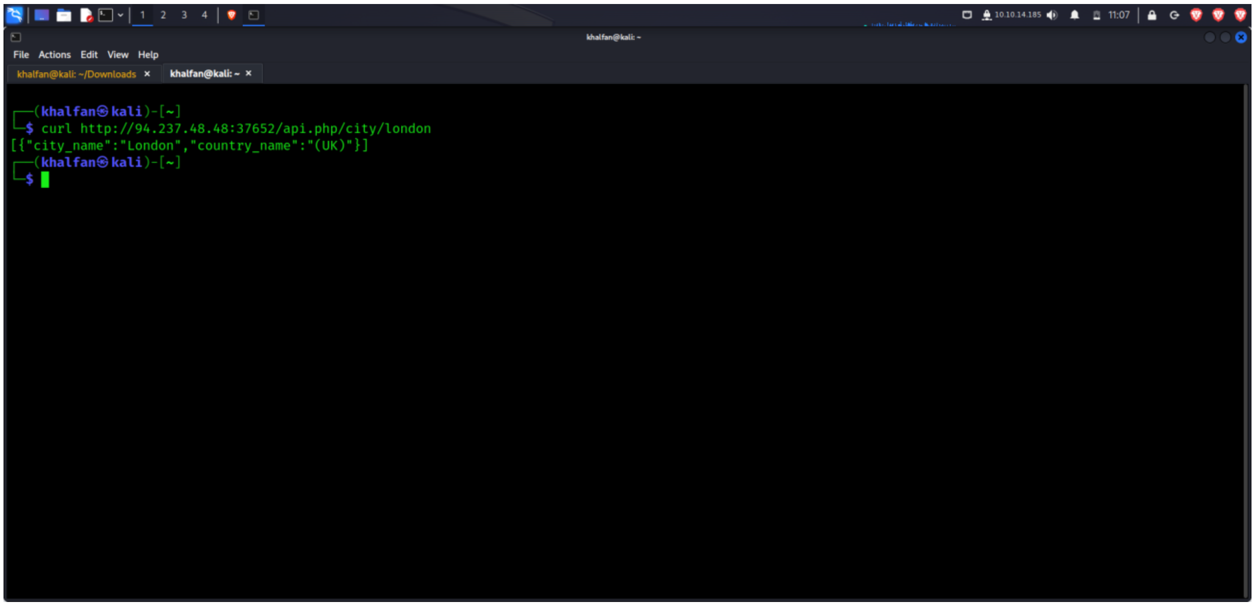
Authenticate to with user "admin" and password "admin"

+2 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'

HTB{p0$t_r3p34t3r}

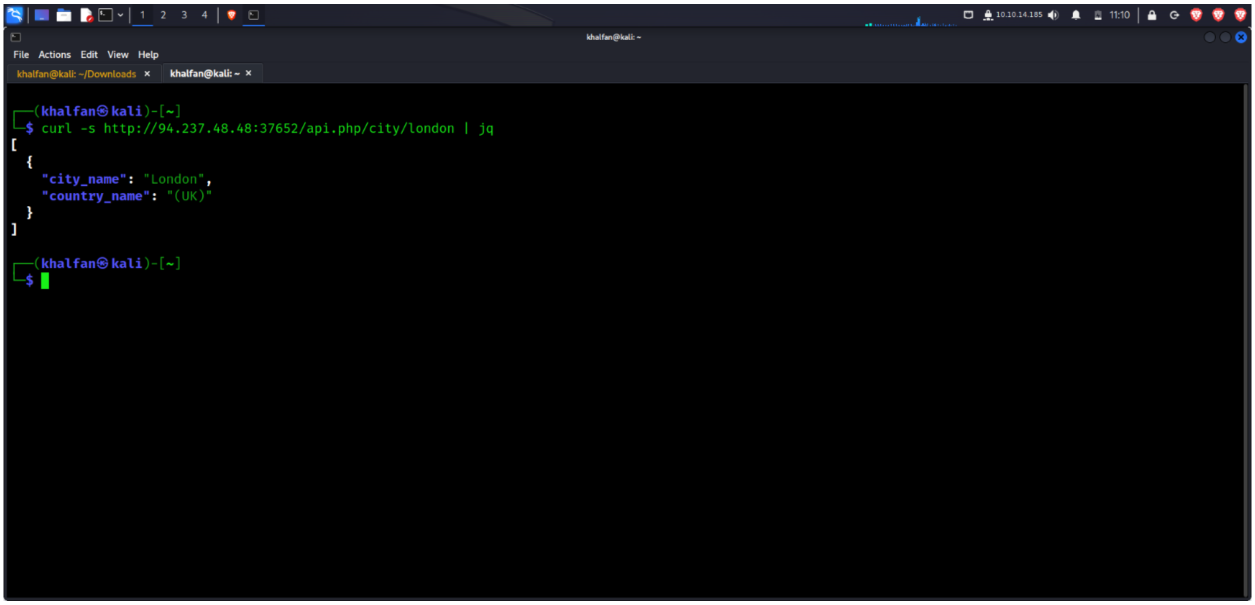
iv. **CRUD API**

**Read London**



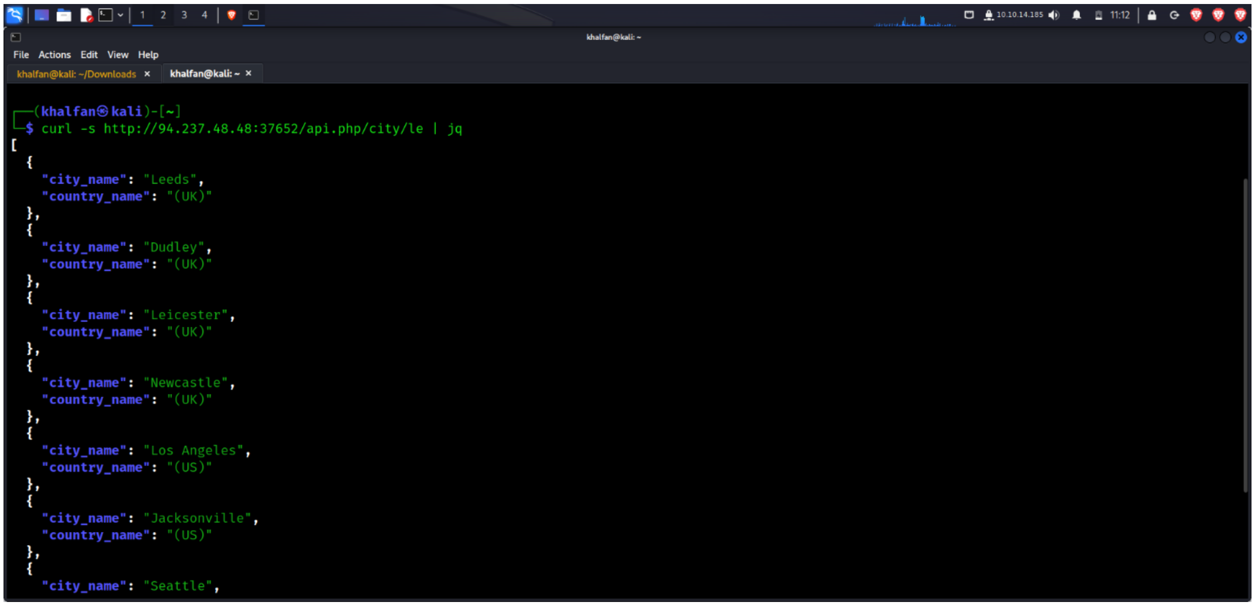
```
┌──(khalfan㉿kali)-[~]
└─$ curl http://94.237.48.48:37652/api.php/city/london
[{"city_name":"London","country_name":"(UK)"}]
┌──(khalfan㉿kali)-[~]
└─$ 
```

Read London in a json way



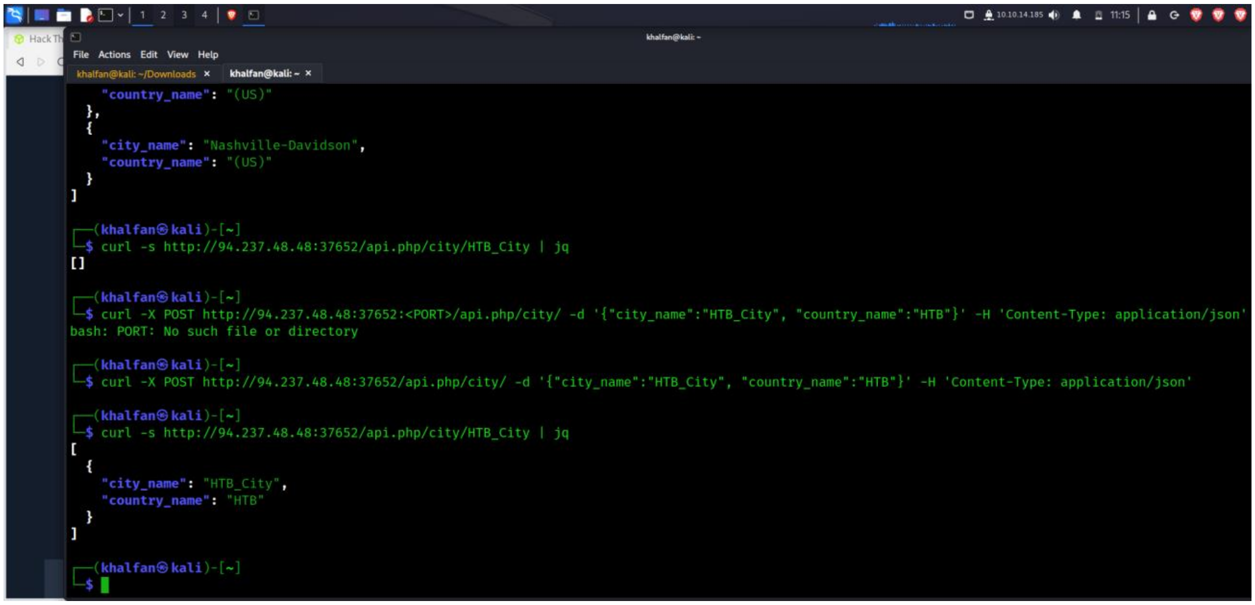
```
┌──(khalfan㉿kali)-[~]
└─$ curl -s http://94.237.48.48:37652/api.php/city/london | jq
[
  {
    "city_name": "London",
    "country_name": "(UK)"
  }
]

┌──(khalfan㉿kali)-[~]
└─$ 
```

search a term and get all matching results:

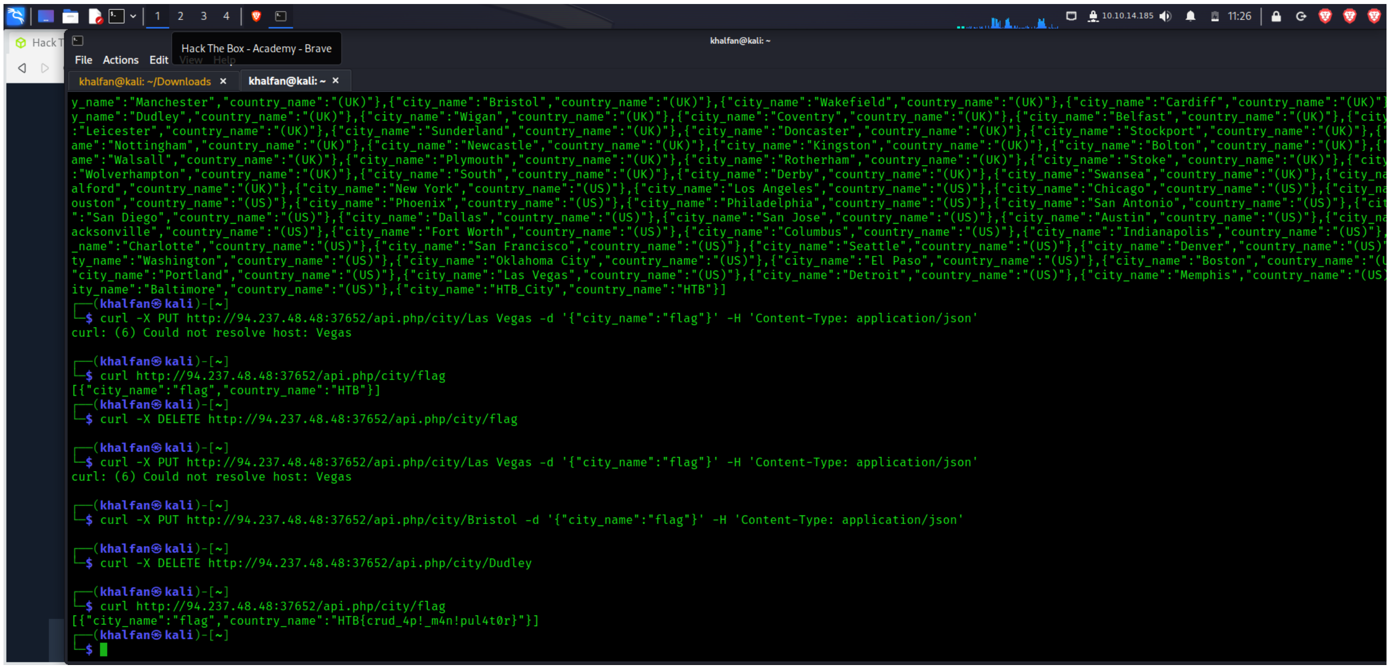


```
┌──(khalfan㉿kali)-[~]
└─$ curl -s http://94.237.48.48:37652/api.php/city/le | jq
[
  {
    "city_name": "Leeds",
    "country_name": "(UK)"
  },
  {
    "city_name": "Dudley",
    "country_name": "(UK)"
  },
  {
    "city_name": "Leicester",
    "country_name": "(UK)"
  },
  {
    "city_name": "Newcastle",
    "country_name": "(UK)"
  },
  {
    "city_name": "Los Angeles",
    "country_name": "(US)"
  },
  {
    "city_name": "Jacksonville",
    "country_name": "(US)"
  },
  {
    "city_name": "Seattle",
```

We create a city HTB



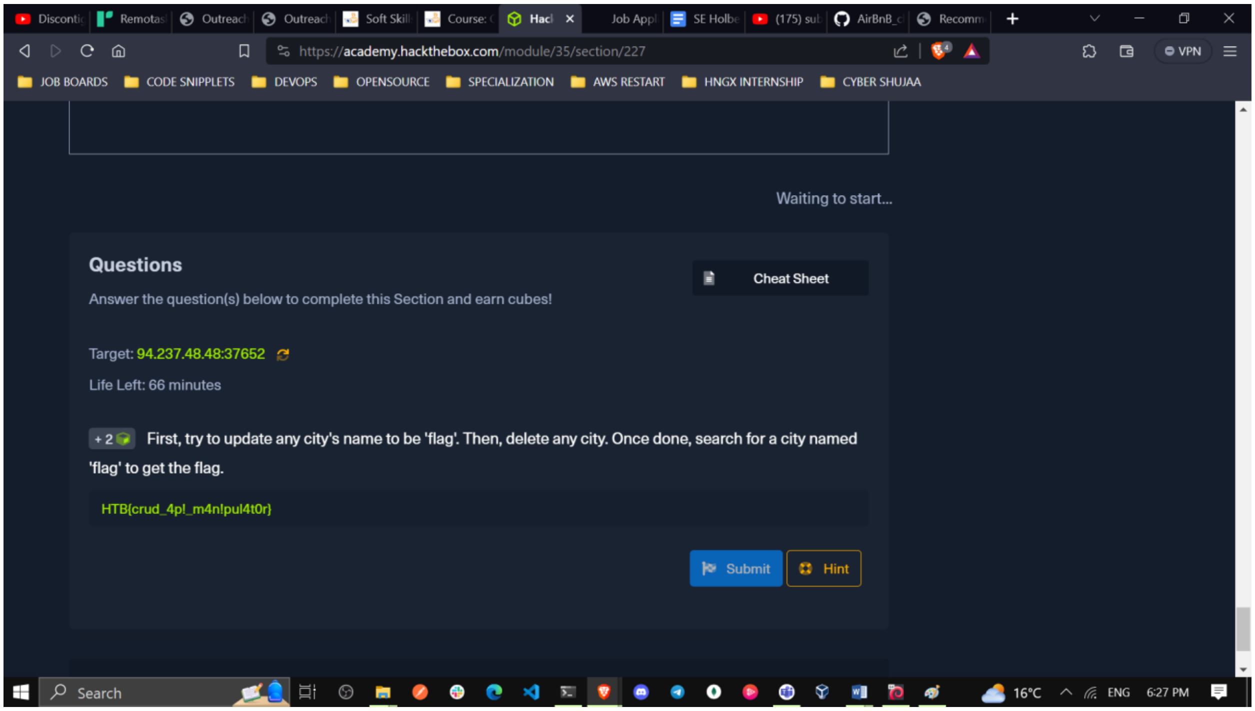
```
    "country_name": "(US)"
  },
  {
    "city_name": "Nashville-Davidson",
    "country_name": "(US)"
  }
]

┌──(khalfan㉿kali)-[~]
└─$ curl -s http://94.237.48.48:37652/api.php/city/HTB_City | jq
[]

┌──(khalfan㉿kali)-[~]
└─$ curl -X POST http://94.237.48.48:37652:<PORT>/api.php/city/ -d '{"city_name":"HTB_City", "country_name":"HTB"}' -H 'Content-Type: application/json'
bash: PORT: No such file or directory

┌──(khalfan㉿kali)-[~]
└─$ curl -X POST http://94.237.48.48:37652/api.php/city/ -d '{"city_name":"HTB_City", "country_name":"HTB"}' -H 'Content-Type: application/json'

┌──(khalfan㉿kali)-[~]
└─$ curl -s http://94.237.48.48:37652/api.php/city/HTB_City | jq
[
  {
    "city_name": "HTB_City",
    "country_name": "HTB"
  }
]

┌──(khalfan㉿kali)-[~]
└─$ 
```


Hack The Box - Academy - Brave
File Actions Edit View Help
khalfan@kali: ~/Downloads
khalfan@kali: ~
10.10.14.185
11:26

```
y_name":"Manchester","country_name":"(UK)"},{"city_name":"Bristol","country_name":"(UK)"},{"city_name":"Wakefield","country_name":"(UK)"},{"city_name":"Cardiff","country_name":"(UK)"}
y_name":"Dudley","country_name":"(UK)"},{"city_name":"Wigan","country_name":"(UK)"},{"city_name":"Coventry","country_name":"(UK)"},{"city_name":"Belfast","country_name":"(UK)"},{"city
:"Leicester","country_name":"(UK)"},{"city_name":"Sunderland","country_name":"(UK)"},{"city_name":"Doncaster","country_name":"(UK)"},{"city_name":"Stockport","country_name":"(UK)"},{"
ame":"Nottingham","country_name":"(UK)"},{"city_name":"Newcastle","country_name":"(UK)"},{"city_name":"Kingston","country_name":"(UK)"},{"city_name":"Bolton","country_name":"(UK)"},{"
ame":"Walsall","country_name":"(UK)"},{"city_name":"Plymouth","country_name":"(UK)"},{"city_name":"Rotherham","country_name":"(UK)"},{"city_name":"Stoke","country_name":"(UK)"},{"city
:"Wolverhampton","country_name":"(UK)"},{"city_name":"South","country_name":"(UK)"},{"city_name":"Derby","country_name":"(UK)"},{"city_name":"Swansea","country_name":"(UK)"},{"city_na
alford","country_name":"(UK)"},{"city_name":"New York","country_name":"(US)"},{"city_name":"Los Angeles","country_name":"(US)"},{"city_name":"Chicago","country_name":"(US)"},{"city_na
ouston","country_name":"(US)"},{"city_name":"Phoenix","country_name":"(US)"},{"city_name":"Philadelphia","country_name":"(US)"},{"city_name":"San Antonio","country_name":"(US)"},{"cit
":"San Diego","country_name":"(US)"},{"city_name":"Dallas","country_name":"(US)"},{"city_name":"San Jose","country_name":"(US)"},{"city_name":"Austin","country_name":"(US)"},{"city_na
acksonville","country_name":"(US)"},{"city_name":"Fort Worth","country_name":"(US)"},{"city_name":"Columbus","country_name":"(US)"},{"city_name":"Indianapolis","country_name":"(US)"},
_name":"Charlotte","country_name":"(US)"},{"city_name":"San Francisco","country_name":"(US)"},{"city_name":"Seattle","country_name":"(US)"},{"city_name":"Denver","country_name":"(US)"
ty_name":"Washington","country_name":"(US)"},{"city_name":"Oklahoma City","country_name":"(US)"},{"city_name":"El Paso","country_name":"(US)"},{"city_name":"Boston","country_name":"(U
"city_name":"Portland","country_name":"(US)"},{"city_name":"Las Vegas","country_name":"(US)"},{"city_name":"Detroit","country_name":"(US)"},{"city_name":"Memphis","country_name":"(US
ity_name":"Baltimore","country_name":"(US)"},{"city_name":"HTB_City","country_name":"HTB"}]
┌──(khalfan㉿kali)-[~]
└─$ curl -X PUT http://94.237.48.48:37652/api.php/city/Las Vegas -d '{"city_name":"flag"}' -H 'Content-Type: application/json'
curl: (6) Could not resolve host: Vegas

┌──(khalfan㉿kali)-[~]
└─$ curl http://94.237.48.48:37652/api.php/city/flag
[{"city_name":"flag","country_name":"HTB"}]
┌──(khalfan㉿kali)-[~]
└─$ curl -X DELETE http://94.237.48.48:37652/api.php/city/flag

┌──(khalfan㉿kali)-[~]
└─$ curl -X PUT http://94.237.48.48:37652/api.php/city/Las Vegas -d '{"city_name":"flag"}' -H 'Content-Type: application/json'
curl: (6) Could not resolve host: Vegas

┌──(khalfan㉿kali)-[~]
└─$ curl -X PUT http://94.237.48.48:37652/api.php/city/Bristol -d '{"city_name":"flag"}' -H 'Content-Type: application/json'

┌──(khalfan㉿kali)-[~]
└─$ curl -X DELETE http://94.237.48.48:37652/api.php/city/Dudley

┌──(khalfan㉿kali)-[~]
└─$ curl http://94.237.48.48:37652/api.php/city/flag
[{"city_name":"flag","country_name":"HTB{crud_4p!_m4n!pul4t0r}"}]
┌──(khalfan㉿kali)-[~]
└─$ 
```

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

**HTB{crud_4p!_m4n!pul4t0r}**



Waiting to start...

Questions

Cheat Sheet

Answer the question(s) below to complete this Section and earn cubes!

Target: 94.237.48.48:37652

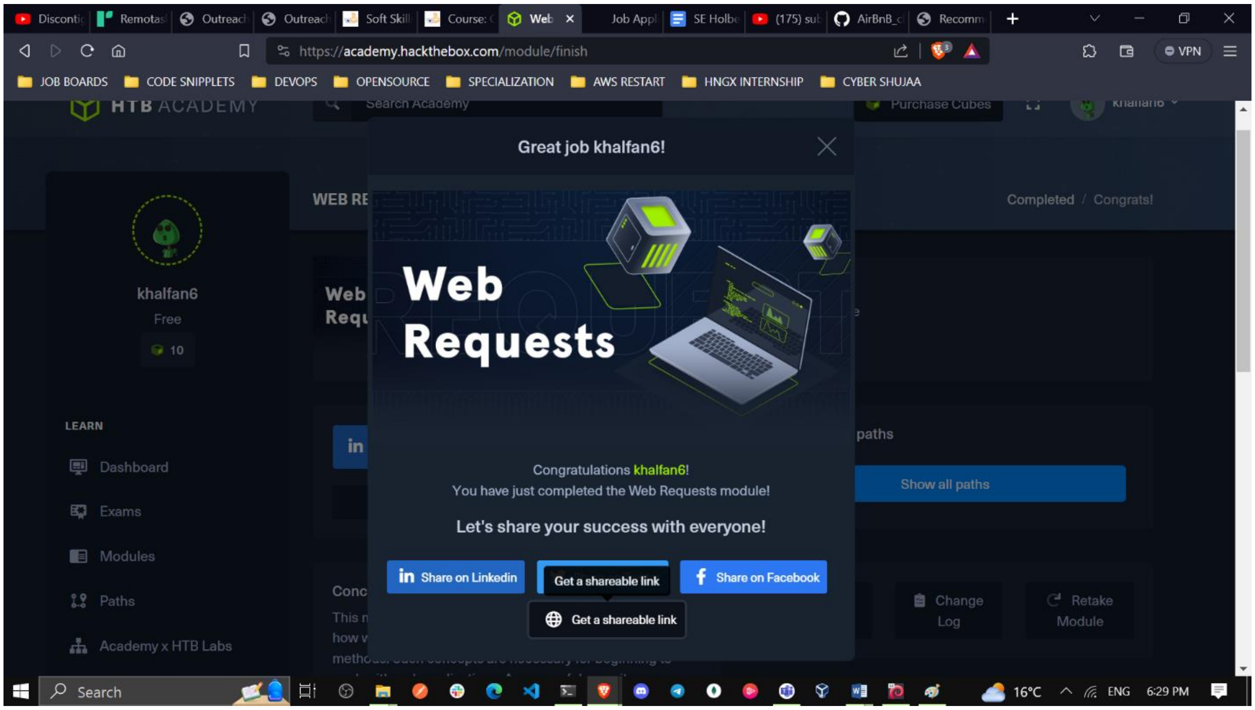
Life Left: 66 minutes

+ 2 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.

HTB{crud_4p!_m4n!pul4t0r}

Submit Hint

The following is the link to my module: https://academy.hackthebox.com/achievement/785849/35



Great job khalfan6!

Congratulations khalfan6!
You have just completed the Web Requests module!

Let's share your success with everyone!

## Conclusion

This module has effectively shown the essential elements of web application interactions. We covered the fundamentals of HTTP and HTTPS, grasped requests and responses, understood the significance of headers, methods, and response codes, and honed the ability to utilize common HTTP methods for seamless data handling. The module's emphasis on API interaction has broadened my perspective, showcasing the potential of integrating external services into our projects. By mastering these concepts, I am better equipped to create efficient, interactive, and data-driven web applications. The knowledge gained here forms a solid foundation, empowering me to navigate the complexities of web development with proficiency and enabling me to build impactful digital experiences for users