Introduction

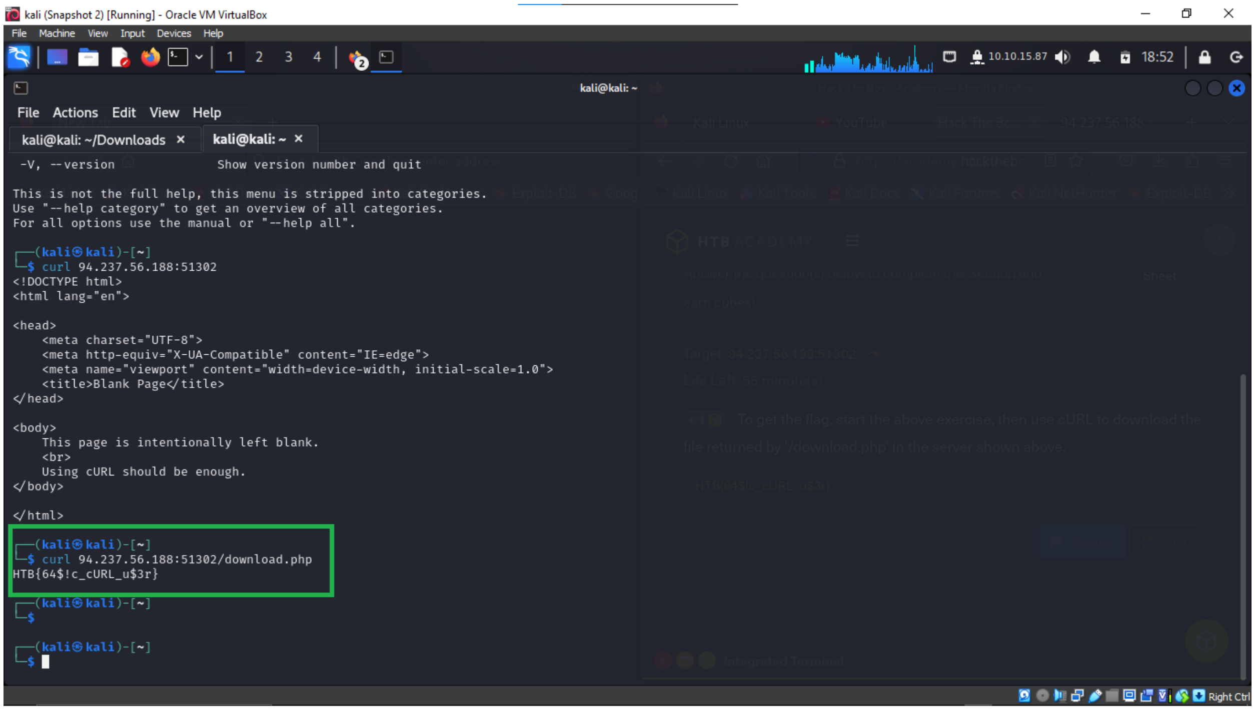
In the modern digital era, understanding web requests and network interactions is essential for anyone involved in web development, cybersecurity, or network administration. This report delves into various scenarios involving web requests, highlighting the importance of tools like cURL and browser devtools in navigating and manipulating network communications. Each question and answer in this report provides a glimpse into common tasks and challenges faced in these fields.

Detailed Questions and Answers

Q1: To get the flag, start the above exercise, then use cURL to download the file returned by '/download. Php' in the server shown above.

A1: (HTB {64$! c_cURL_u$3r})

This response illustrates the use of cURL, a powerful command-line tool, to download files from a server. It demonstrates the ease of fetching resources like in this case we are using Curl to request server located in Ip address 94.237.56.188 on port number 51302 for whatever resource is provided by 'download.php'.


kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.10.15.87
18:52
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~

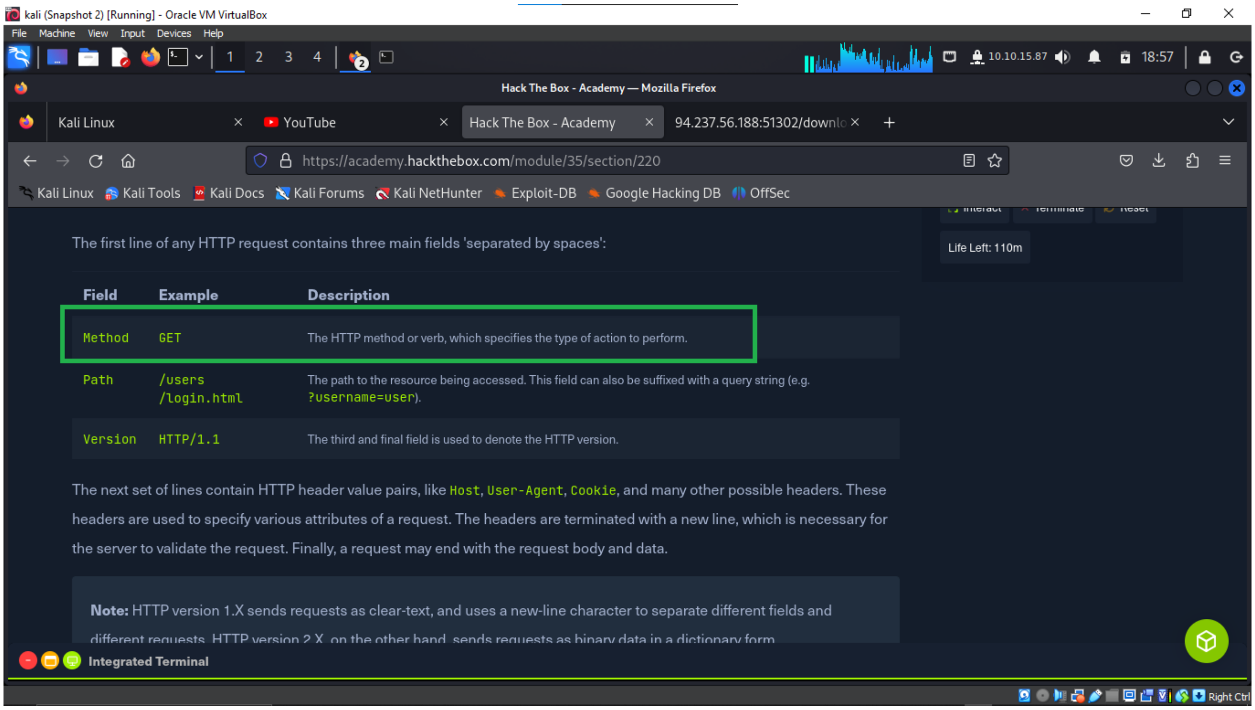
```
 -V, --version              Show version number and quit

This is not the full help, this menu is stripped into categories.
Use "--help category" to get an overview of all categories.
For all options use the manual or "--help all".

┌──(kali㉿kali)-[~]
└─$ curl 94.237.56.188:51302
<!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>

┌──(kali㉿kali)-[~]
└─$ curl 94.237.56.188:51302/download.php
HTB{64$!c_cURL_u$3r}
┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$ 
```

Q2: What is the HTTP method used while intercepting the request? (Case-sensitive)

A2: GET

Identifying the HTTP method (GET in this case) is crucial in understanding how web browsers interact with servers, particularly in data retrieval processes.

As for this question I used notes from the module to retrieve answer as indicated below.


kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.10.15.87
18:57
Hack The Box - Academy — Mozilla Firefox
Kali Linux
YouTube
Hack The Box - Academy
94.237.56.188:51302/downl
https://academy.hackthebox.com/module/35/section/220
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Life Left: 110m
Integrated Terminal
Right Ctrl

The first line of any HTTP request contains three main fields 'separated by spaces':

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.

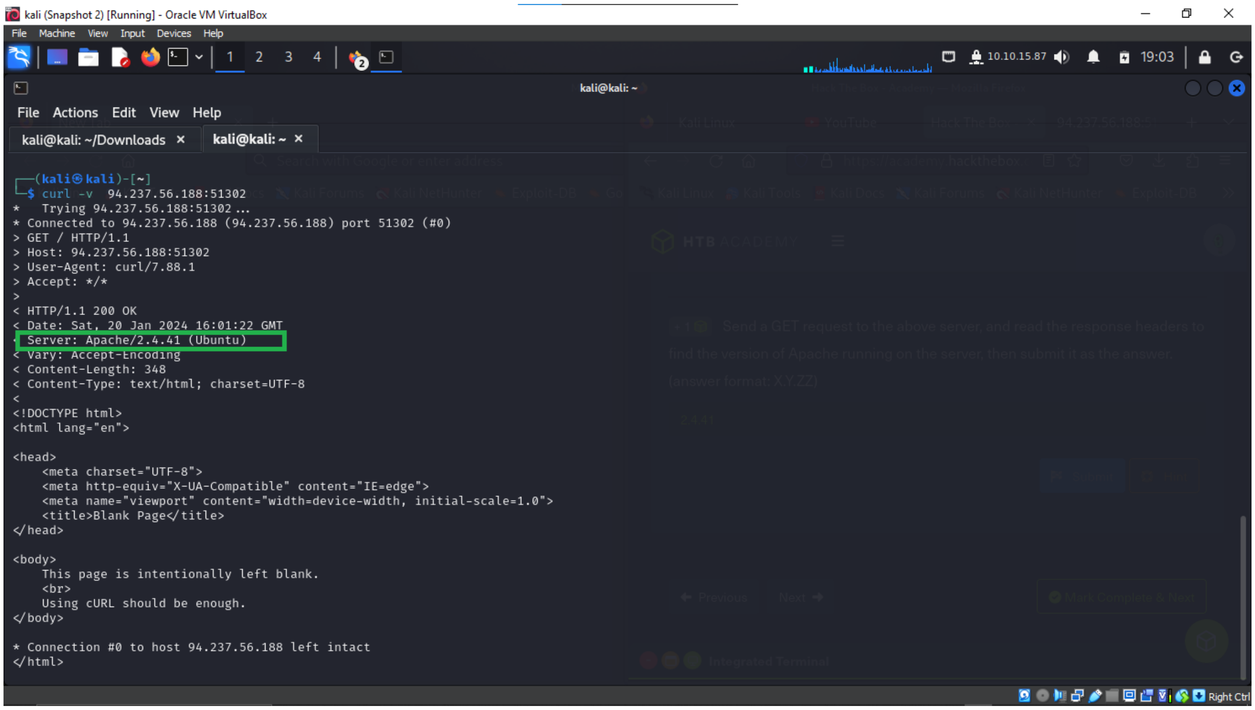
The next set of lines contain HTTP header value pairs, like Host, User-Agent, Cookie, and many other possible headers. These headers are used to specify various attributes of a request. The headers are terminated with a new line, which is necessary for the server to validate the request. Finally, a request may end with the request body and data.

Note: HTTP version 1.X sends requests as clear-text, and uses a new-line character to separate different fields and different requests. HTTP version 2.X, on the other hand, sends requests as binary data in a dictionary form

Q3: 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)

A3: 2.4.41

This highlights the importance of inspecting response headers, which can reveal critical information about the server, such as software versions, potentially useful in security assessments. In our case I used ***curl -v***(verbose) which provides more detailed information about the network request and response.


kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.10.15.87
19:03
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~
Right Ctrl

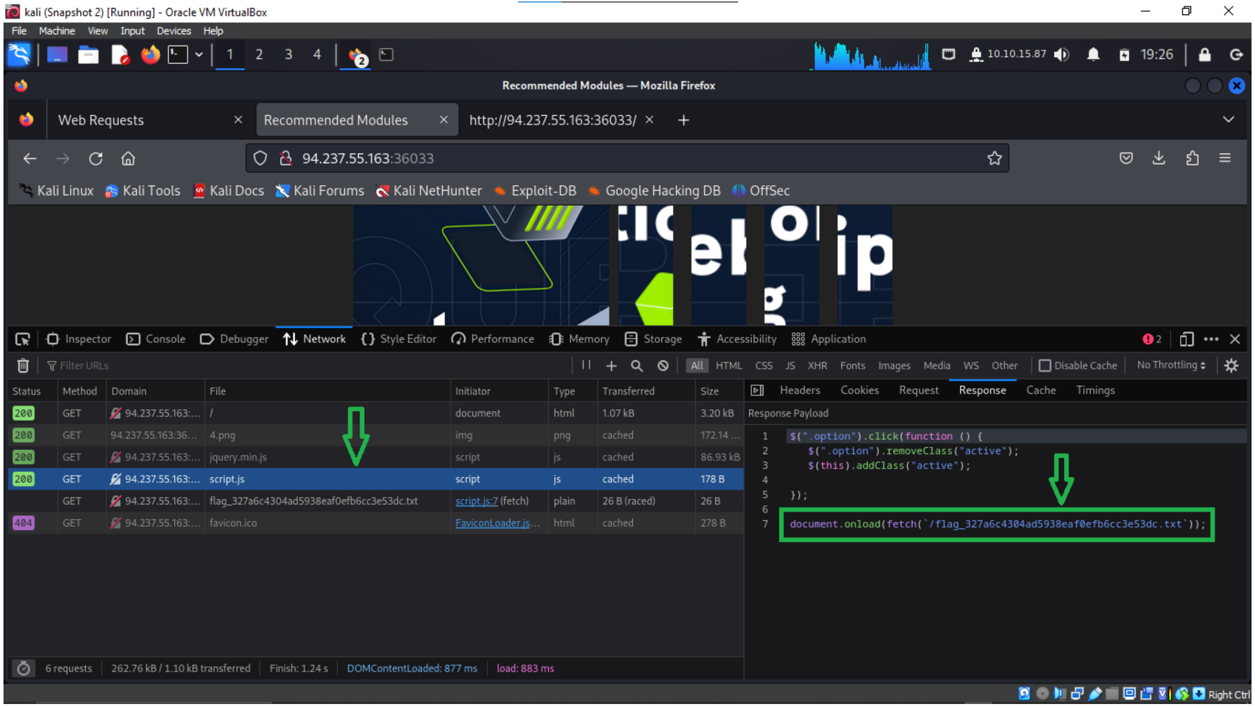
```
┌──(kali㉿kali)-[~]
└─$ curl -v  94.237.56.188:51302
*   Trying 94.237.56.188:51302 ...
* Connected to 94.237.56.188 (94.237.56.188) port 51302 (#0)
> GET / HTTP/1.1
> Host: 94.237.56.188:51302
> User-Agent: curl/7.88.1
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Sat, 20 Jan 2024 16:01:22 GMT
< Server: 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 94.237.56.188 left intact
</html>
```

–

Q4: 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.

A4: HTB {p493_r3qu3$t$_m0n! t0r}

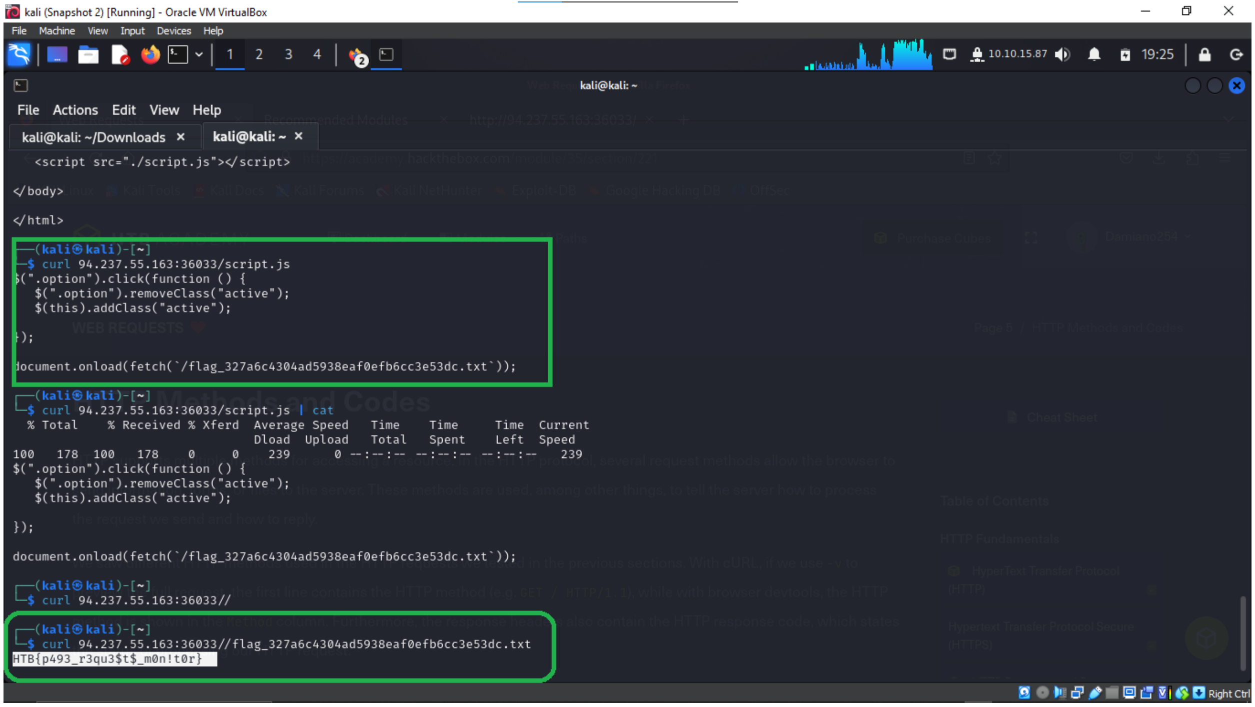
Using browser devtools to monitor network requests is an essential skill in web development and cybersecurity, helping to understand how web pages dynamically load content.



Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	94.237.55.163:...	/	document	html	1.07 kB	3.20 kB
200	GET	94.237.55.163:36...	4.png	img	png	cached	172.14 ...
200	GET	94.237.55.163:...	jquery.min.js	script	js	cached	86.93 kB
200	GET	94.237.55.163:...	script.js	script	js	cached	178 B
	GET	94.237.55.163:...	flag_327a6c4304ad5938eaf0efb6cc3e53dc.txt	script.js:7 (fetch)	plain	26 B (raced)	26 B
404	GET	94.237.55.163:...	favicon.ico	FaviconLoader.js...	html	cached	278 B

```
$(".option").click(function () {
   $(".option").removeClass("active");
   $(this).addClass("active");

});

document.onload(fetch(`/flag_327a6c4304ad5938eaf0efb6cc3e53dc.txt`));
```

6 requests | 262.76 kB / 1.10 kB transferred | Finish: 1.24 s | DOMContentLoaded: 877 ms | load: 883 ms

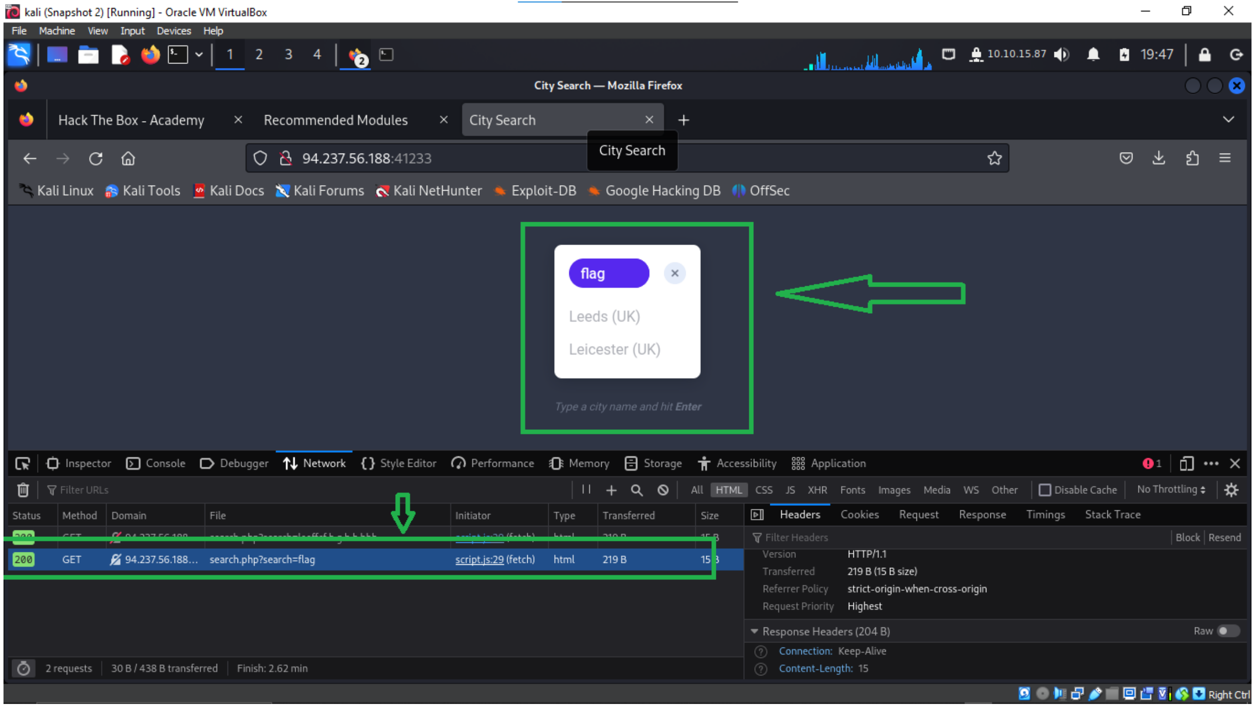

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~

```
  <script src="./script.js"></script>

</body>

</html>

┌──(kali㉿kali)-[~]
└─$ curl 94.237.55.163:36033/script.js
$(".option").click(function () {
   $(".option").removeClass("active");
   $(this).addClass("active");

});

document.onload(fetch(`/flag_327a6c4304ad5938eaf0efb6cc3e53dc.txt`));

┌──(kali㉿kali)-[~]
└─$ curl 94.237.55.163:36033/script.js | cat
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   178  100   178    0     0    239      0 --:--:-- --:--:-- --:--:--   239
$(".option").click(function () {
   $(".option").removeClass("active");
   $(this).addClass("active");

});

document.onload(fetch(`/flag_327a6c4304ad5938eaf0efb6cc3e53dc.txt`));

┌──(kali㉿kali)-[~]
└─$ curl 94.237.55.163:36033//

┌──(kali㉿kali)-[~]
└─$ curl 94.237.55.163:36033//flag_327a6c4304ad5938eaf0efb6cc3e53dc.txt
HTB{p493_r3qu3$t$_m0n!t0r}
```

Q5: 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.

A5: HTB {curl_g3773r}

This showcases how cURL can be used as an alternative to browser-based interactions, offering more control and often revealing underlying issues with web applications.



City Search — Mozilla Firefox

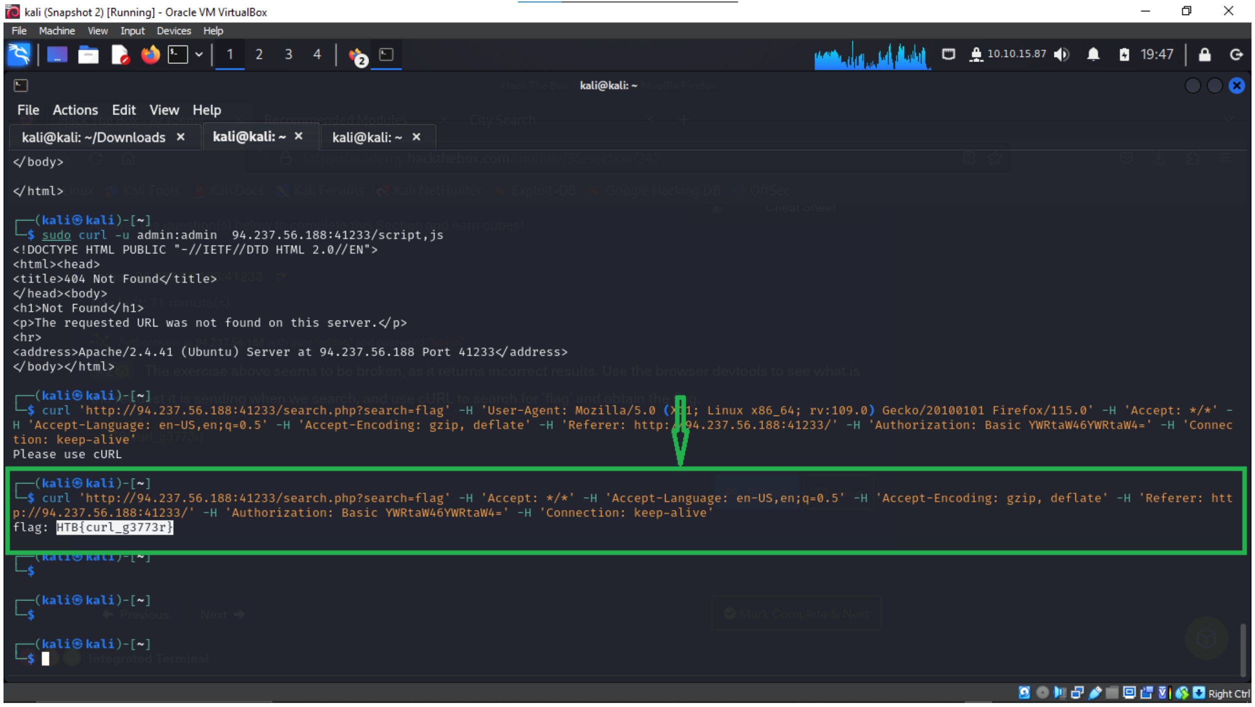
94.237.56.188:41233

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	94.237.56.188…	search.php?search=flag	script.js:29 (fetch)	html	219 B	15 B

Version HTTP/1.1
Transferred 219 B (15 B size)
Referrer Policy strict-origin-when-cross-origin
Request Priority Highest

Response Headers (204 B)
Connection: Keep-Alive
Content-Length: 15

2 requests | 30 B / 438 B transferred | Finish: 2.62 min

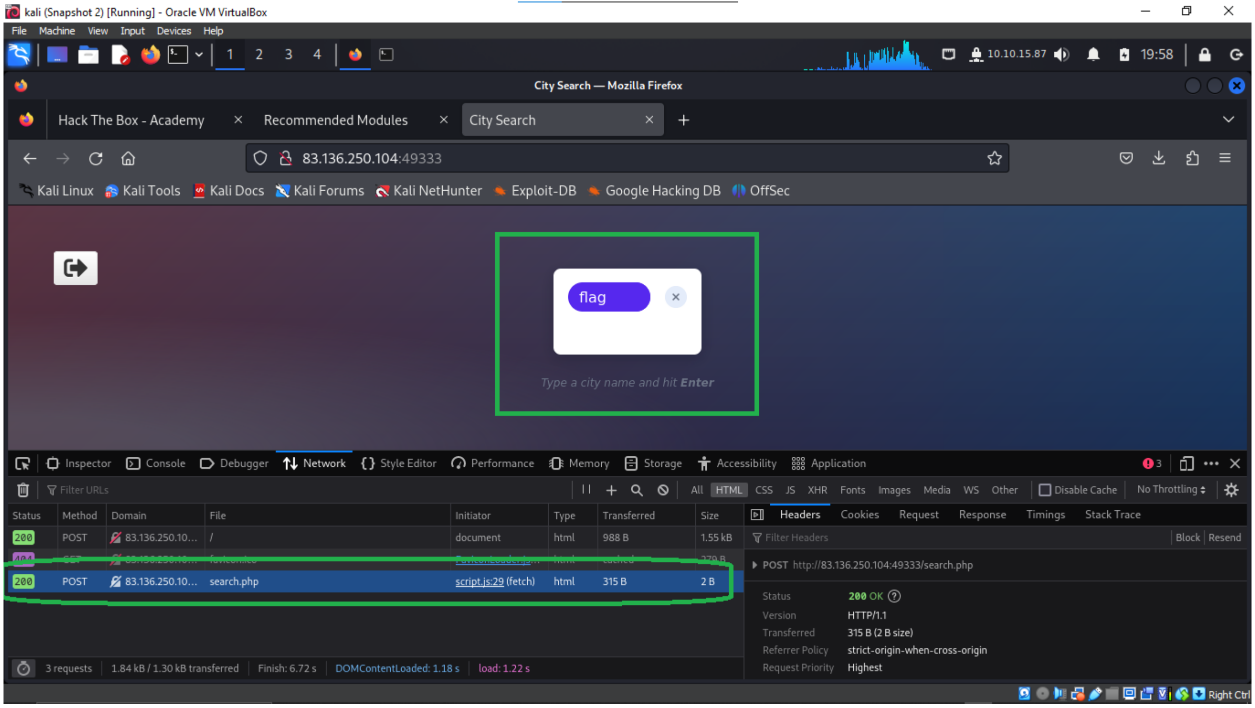


```
</body>

</html>

┌──(kali㉿kali)-[~]
└─$ sudo curl -u admin:admin  94.237.56.188:41233/script,js
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at 94.237.56.188 Port 41233</address>
</body></html>

┌──(kali㉿kali)-[~]
└─$ curl 'http://94.237.56.188:41233/search.php?search=flag' -H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0' -H 'Accept: */*' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'Referer: http://94.237.56.188:41233/' -H 'Authorization: Basic YWRtaW46YWRtaW4=' -H 'Connection: keep-alive'
Please use cURL

┌──(kali㉿kali)-[~]
└─$ curl 'http://94.237.56.188:41233/search.php?search=flag' -H 'Accept: */*' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'Referer: http://94.237.56.188:41233/' -H 'Authorization: Basic YWRtaW46YWRtaW4=' -H 'Connection: keep-alive'
flag: HTB{curl_g3773r}
┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$
```

Q6: 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'

A6: HTB{p0$t_r3p34t3r}

This answer demonstrates how session cookies can be utilized in conjunction with cURL to maintain state and perform authenticated actions, a common requirement in web interactions.

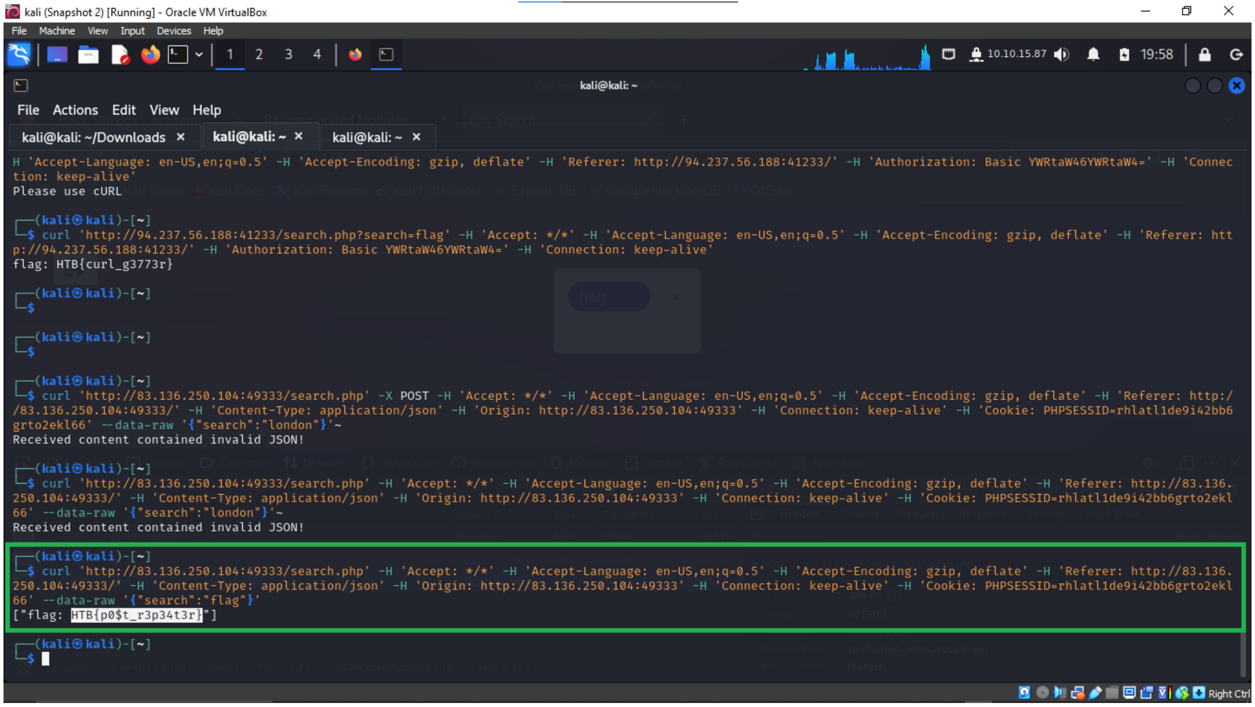


Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	POST	83.136.250.10...	/	document	html	988 B	1.55 kB
404	GET	83.136.250.10...	favicon.ico	FaviconLoader.js...	html	cached	279 B
200	POST	83.136.250.10...	search.php	script.js:29 (fetch)	html	315 B	2 B

3 requests | 1.84 kB / 1.30 kB transferred | Finish: 6.72 s | DOMContentLoaded: 1.18 s | load: 1.22 s

POST http://83.136.250.104:49333/search.php

Status	200 OK
Version	HTTP/1.1
Transferred	315 B (2 B size)
Referrer Policy	strict-origin-when-cross-origin
Request Priority	Highest

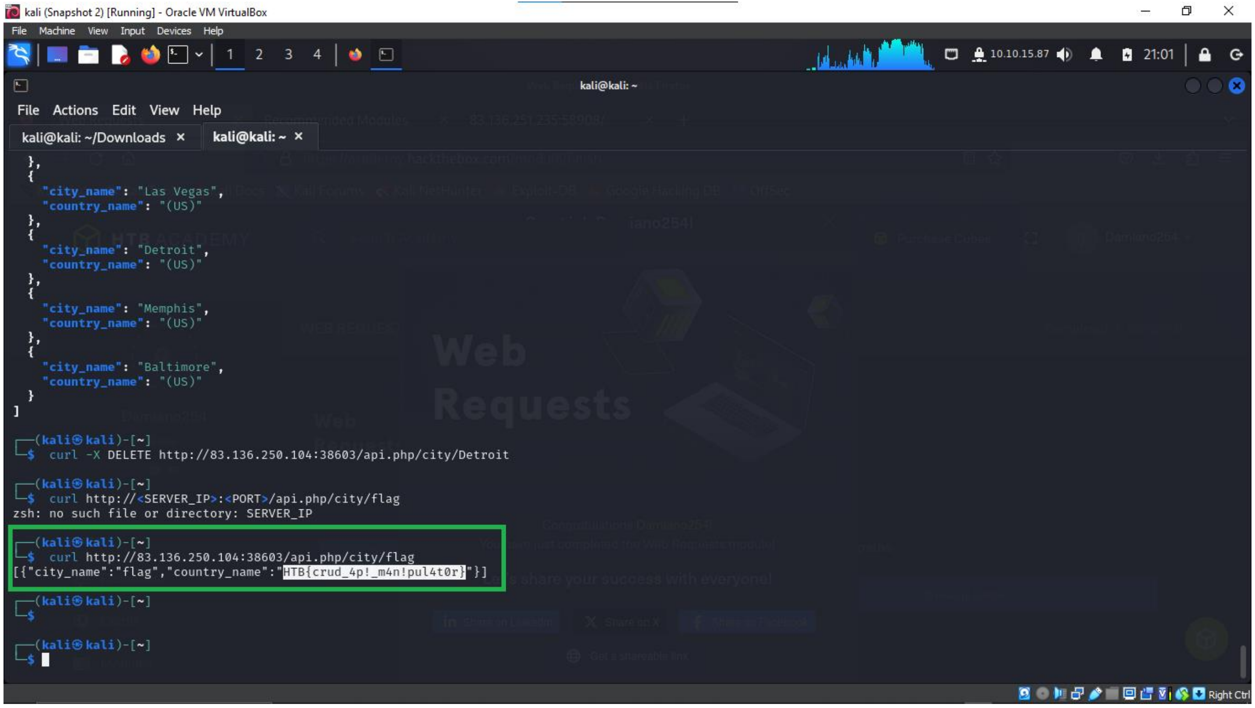


```
H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'Referer: http://94.237.56.188:41233/' -H 'Authorization: Basic YWRtaW46YWRtaW4=' -H 'Connec
tion: keep-alive'
Please use cURL

┌──(kali㉿kali)-[~]
└─$ curl 'http://94.237.56.188:41233/search.php?search=flag' -H 'Accept: */*' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'Referer: htt
p://94.237.56.188:41233/' -H 'Authorization: Basic YWRtaW46YWRtaW4=' -H 'Connection: keep-alive'
flag: HTB{curl_g3773r}

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$ curl 'http://83.136.250.104:49333/search.php' -X POST -H 'Accept: */*' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'Referer: http:/
/83.136.250.104:49333/' -H 'Content-Type: application/json' -H 'Origin: http://83.136.250.104:49333' -H 'Connection: keep-alive' -H 'Cookie: PHPSESSID=rhlatl1de9i42bb6
grto2ekl66' --data-raw '{"search":"london"}'~
Received content contained invalid JSON!

┌──(kali㉿kali)-[~]
└─$ curl 'http://83.136.250.104:49333/search.php' -H 'Accept: */*' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'Referer: http://83.136.
250.104:49333/' -H 'Content-Type: application/json' -H 'Origin: http://83.136.250.104:49333' -H 'Connection: keep-alive' -H 'Cookie: PHPSESSID=rhlatl1de9i42bb6grto2ekl
66' --data-raw '{"search":"london"}'~
Received content contained invalid JSON!

┌──(kali㉿kali)-[~]
└─$ curl 'http://83.136.250.104:49333/search.php' -H 'Accept: */*' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'Referer: http://83.136.
250.104:49333/' -H 'Content-Type: application/json' -H 'Origin: http://83.136.250.104:49333' -H 'Connection: keep-alive' -H 'Cookie: PHPSESSID=rhlatl1de9i42bb6grto2ekl
66' --data-raw '{"search":"flag"}'
["flag: HTB{p0$t_r3p34t3r}"]

┌──(kali㉿kali)-[~]
└─$ 
```

Q7: 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.

A7: HTB {crud_4p! _m4n! pul4t0r}

This reflects on CRUD (Create, Read, Update, Delete) operations in web applications, emphasizing the importance of understanding how data manipulation occurs over the network.

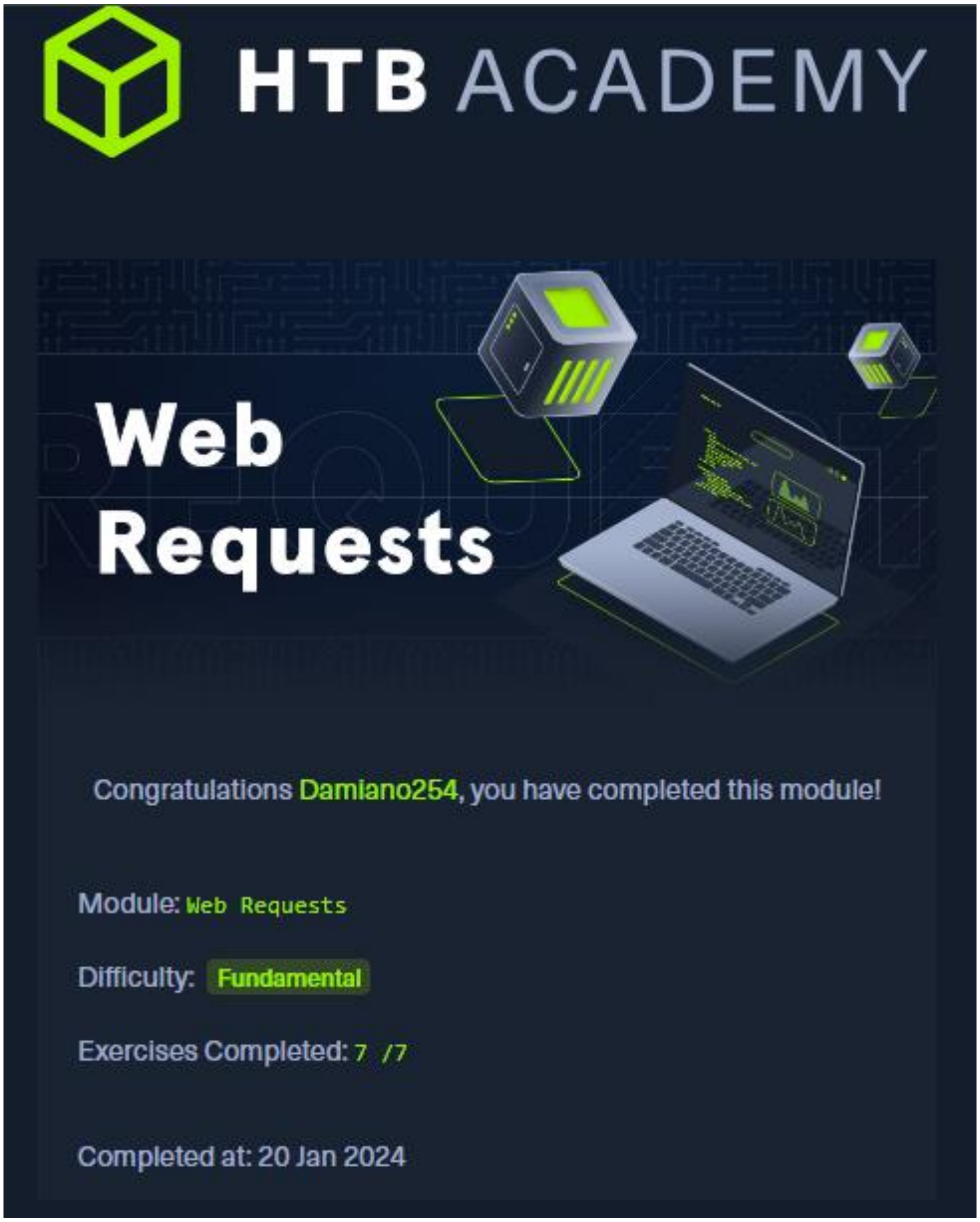

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.10.15.87
21:01
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~
Right Ctrl

```
  },
  {
    "city_name": "Las Vegas",
    "country_name": "(US)"
  },
  {
    "city_name": "Detroit",
    "country_name": "(US)"
  },
  {
    "city_name": "Memphis",
    "country_name": "(US)"
  },
  {
    "city_name": "Baltimore",
    "country_name": "(US)"
  }
]

┌──(kali㉿kali)-[~]
└─$ curl -X DELETE http://83.136.250.104:38603/api.php/city/Detroit

┌──(kali㉿kali)-[~]
└─$ curl http://<SERVER_IP>:<PORT>/api.php/city/flag
zsh: no such file or directory: SERVER_IP

┌──(kali㉿kali)-[~]
└─$ curl http://83.136.250.104:38603/api.php/city/flag
[{"city_name":"flag","country_name":"HTB{crud_4p!_m4n!pul4t0r}"}]

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$
```

Conclusion

The interactions presented in this report offer a sample experience of the diverse and complex nature of web requests. From basic file downloads to advanced manipulation of server responses, these scenarios underscore the critical role of tools and techniques in efficiently navigating and exploiting network environments. For users, whether they are developers, cybersecurity enthusiasts, or just tech-savvy individuals, mastering these concepts is key to understanding and leveraging the full potential of web technologies.

https://academy.hackthebox.com/achievement/949661/35



HTB ACADEMY

Web Requests

Congratulations Damiano254, you have completed this module!

Module: `Web Requests`

Difficulty: Fundamental

Exercises Completed: `7 /7`

Completed at: 20 Jan 2024