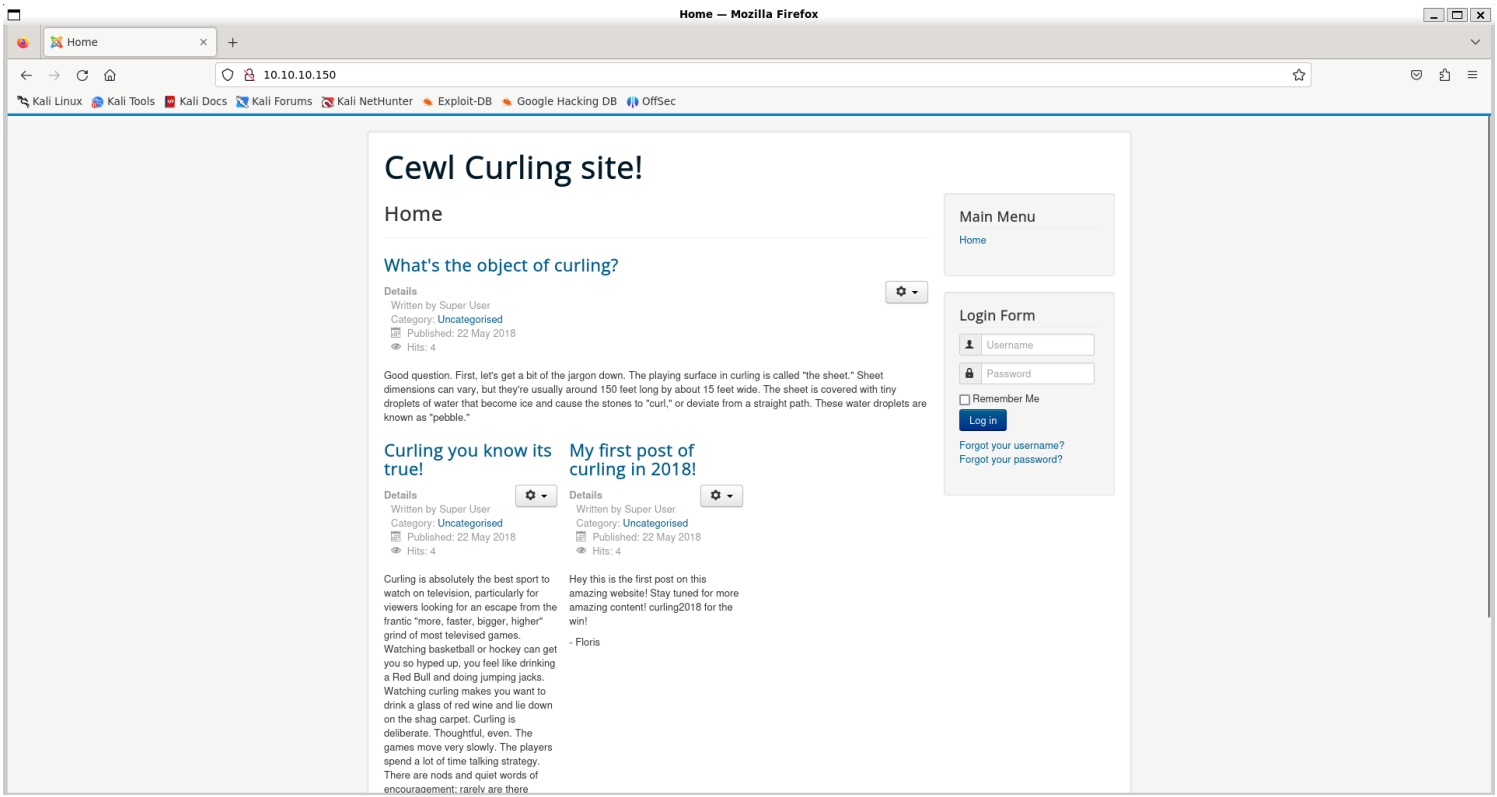
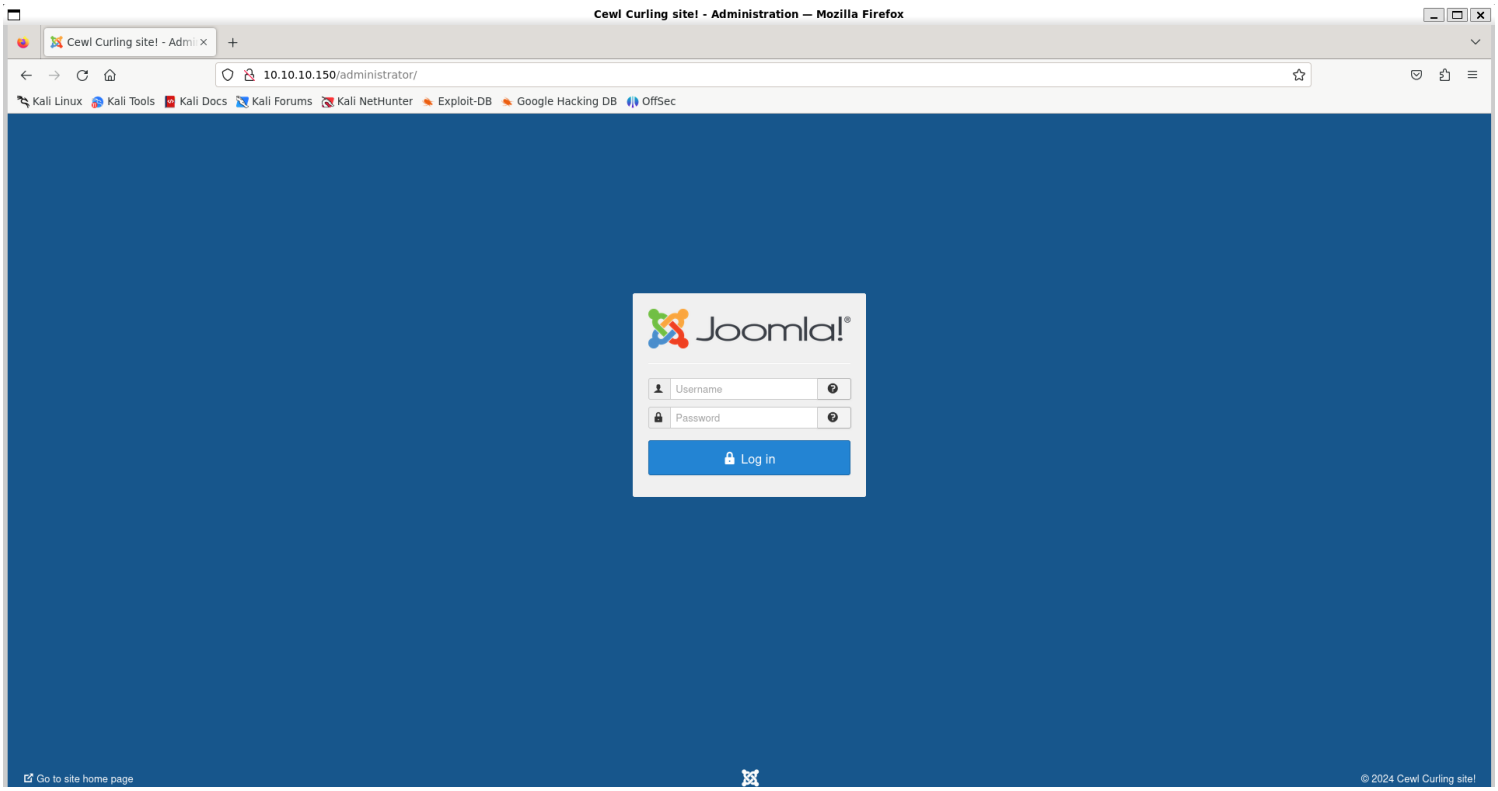
Information Gathering

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

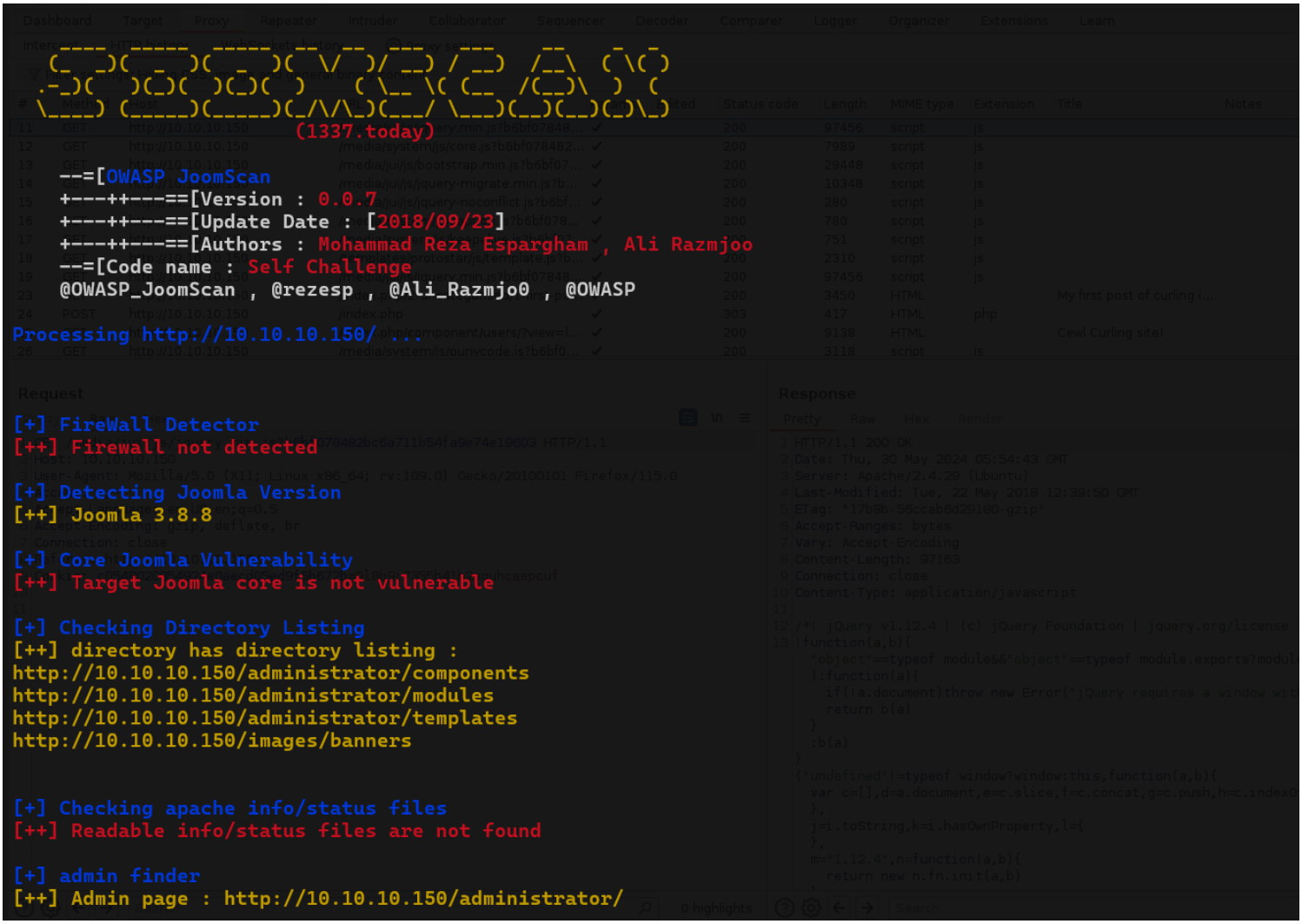




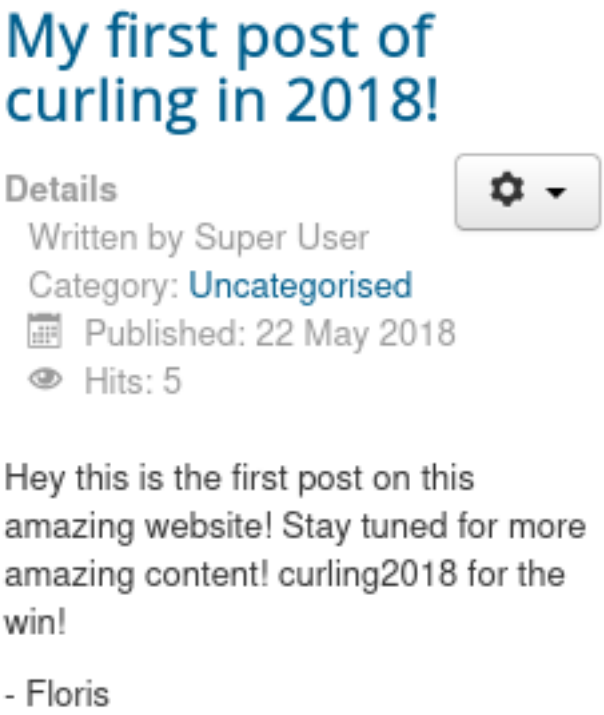
3) Checked pages

```
┌──(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]
                        [Status: 200, Size: 14243, Words: 762, Lines: 362, Duration: 211ms]
bin                     [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 222ms]
plugins                 [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 182ms]
includes                [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 179ms]
media                   [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 6381ms]
language                [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 201ms]
components              [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 280ms]
cache                   [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 614ms]
libraries               [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 205ms]
templates               [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 340ms]
modules                 [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 854ms]
tmp                     [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 179ms]
layouts                 [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 995ms]
administrator           [Status: 301, Size: 320, Words: 20, Lines: 10, Duration: 474ms]
cli                     [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

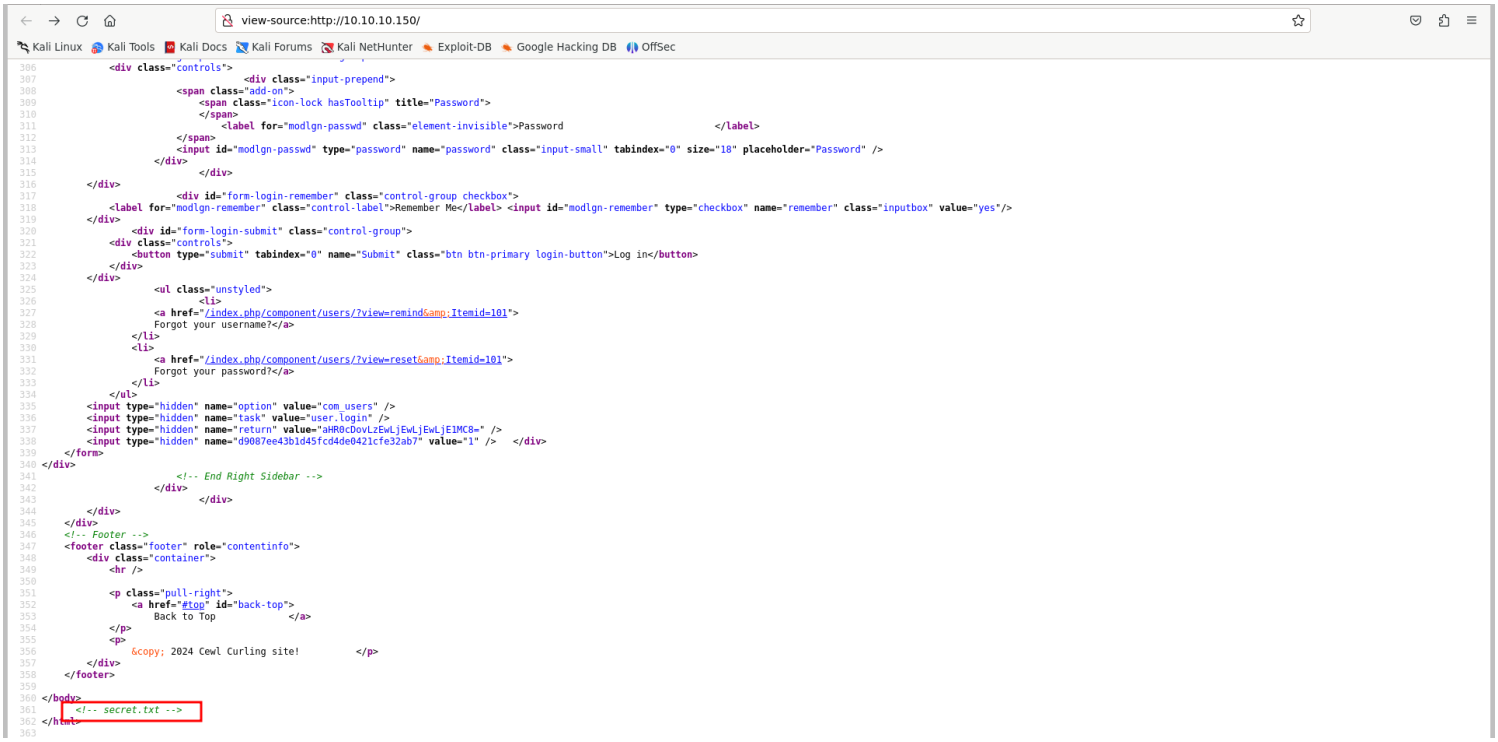


5) The username is Floris

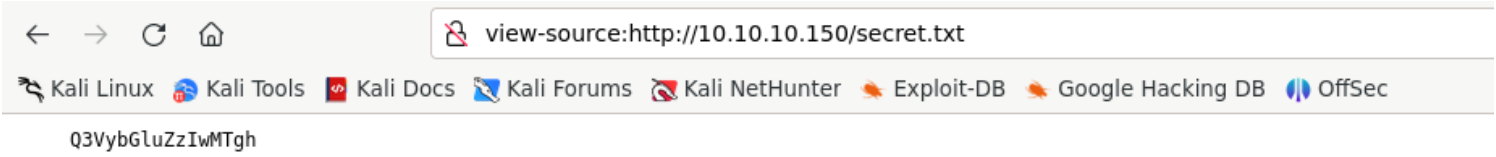


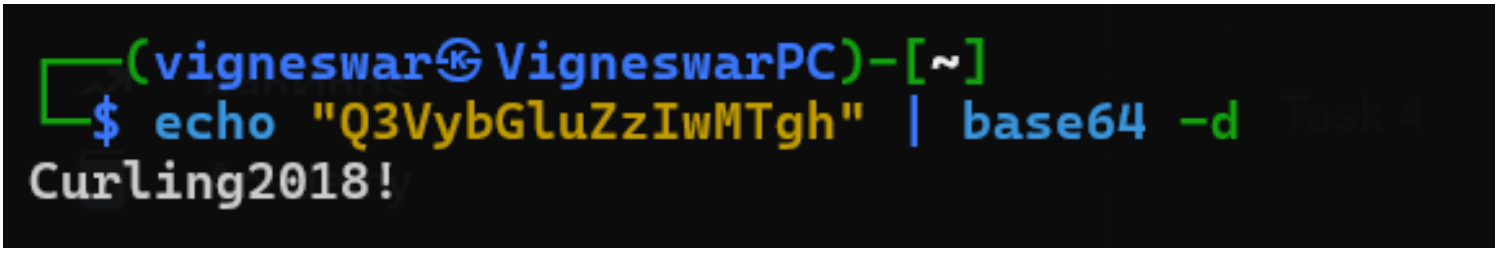
Vulnerability Assessment

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

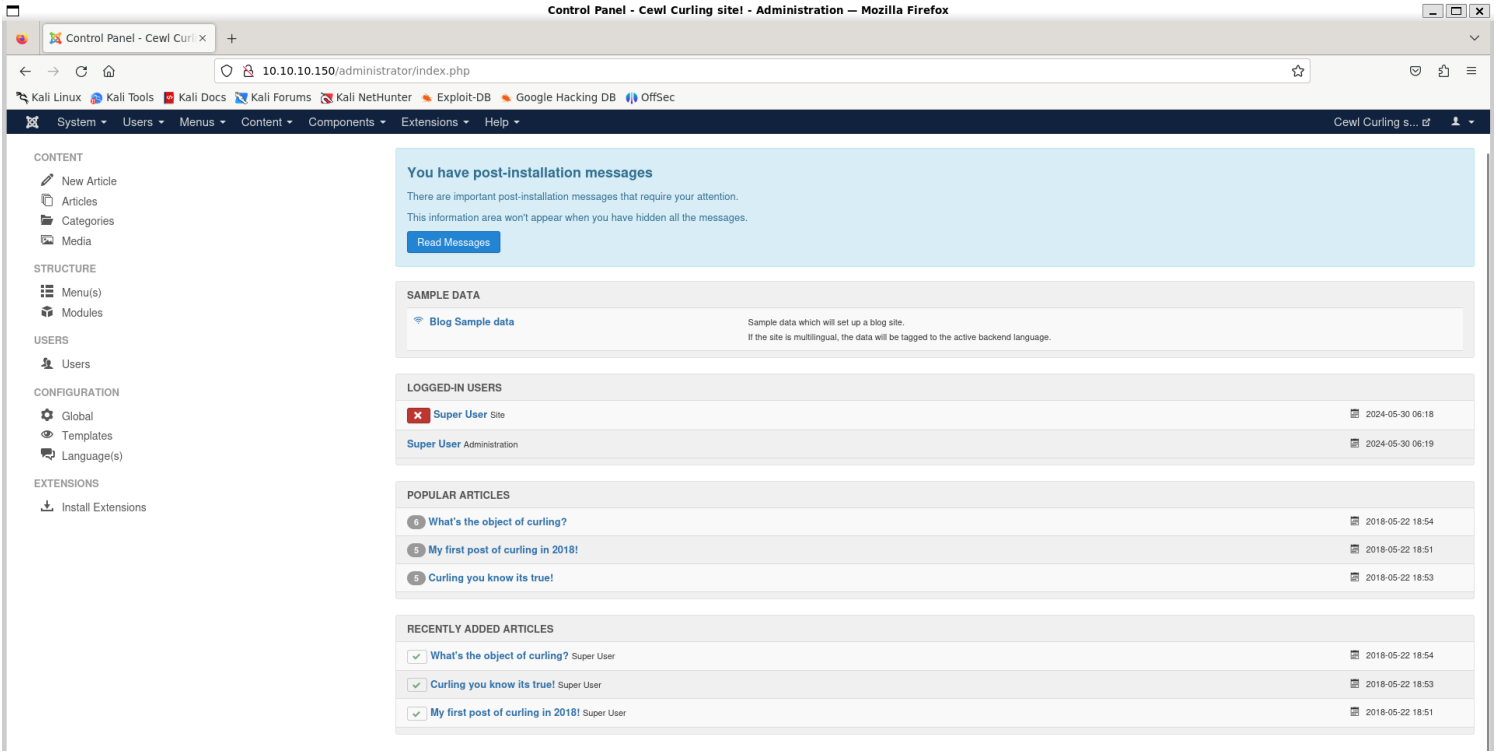


2) Found a password



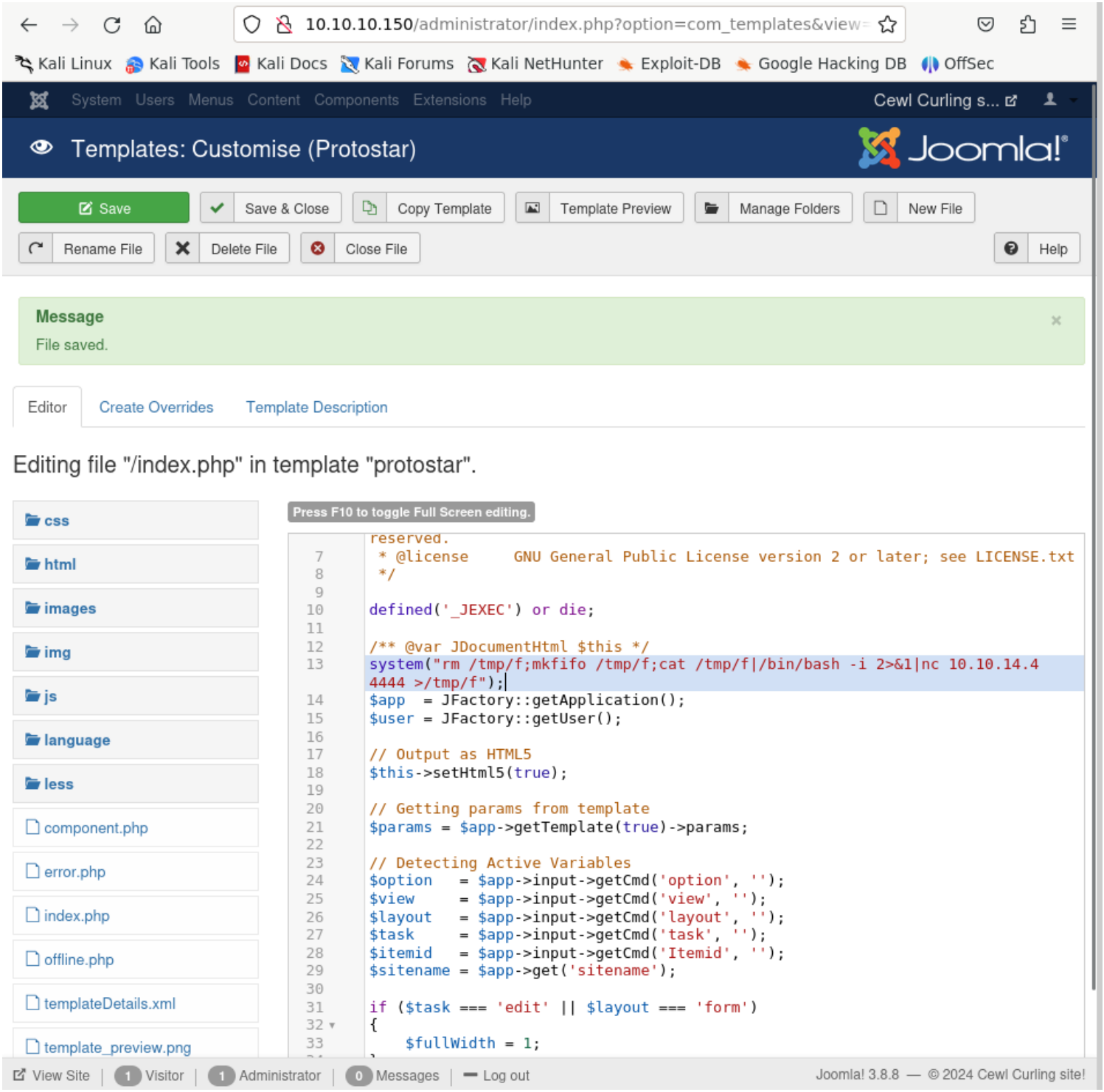


3) Logged in with credentials
Floris:Curling2018!

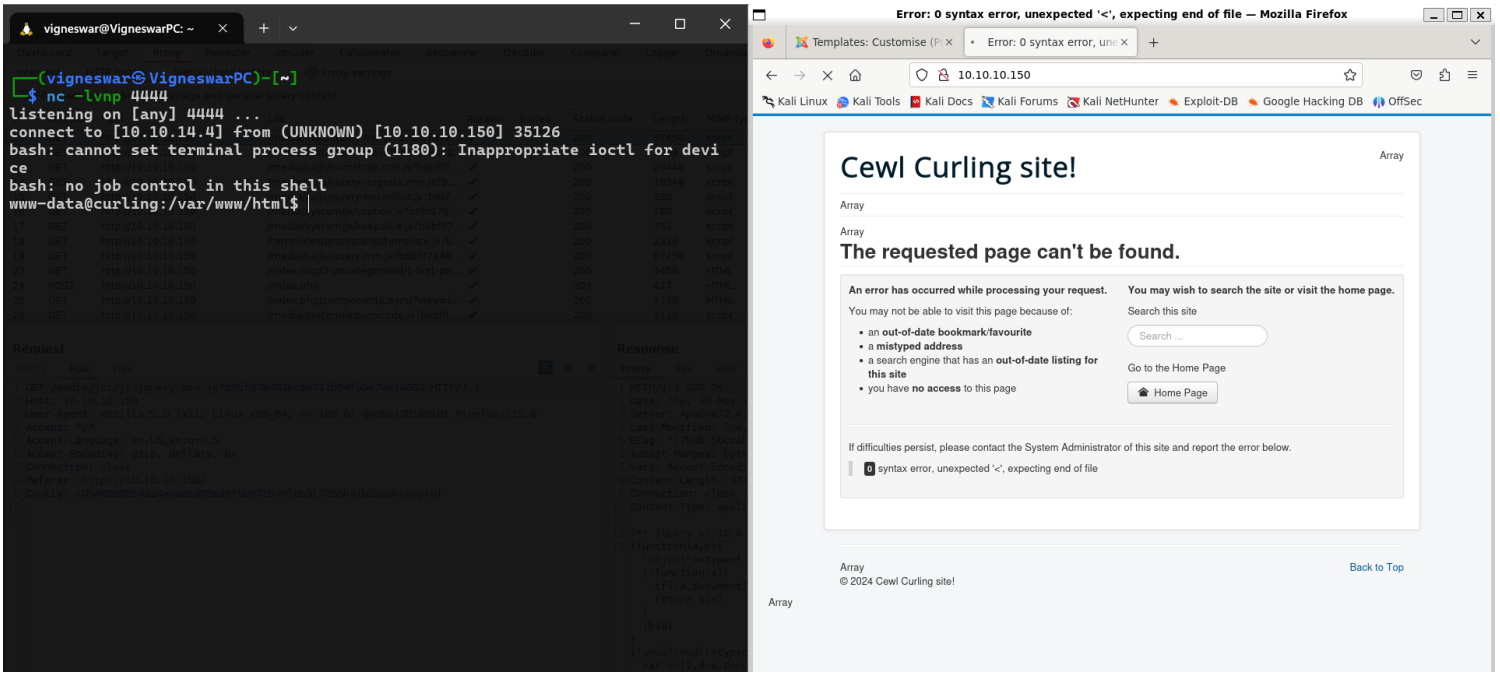


Exploitation

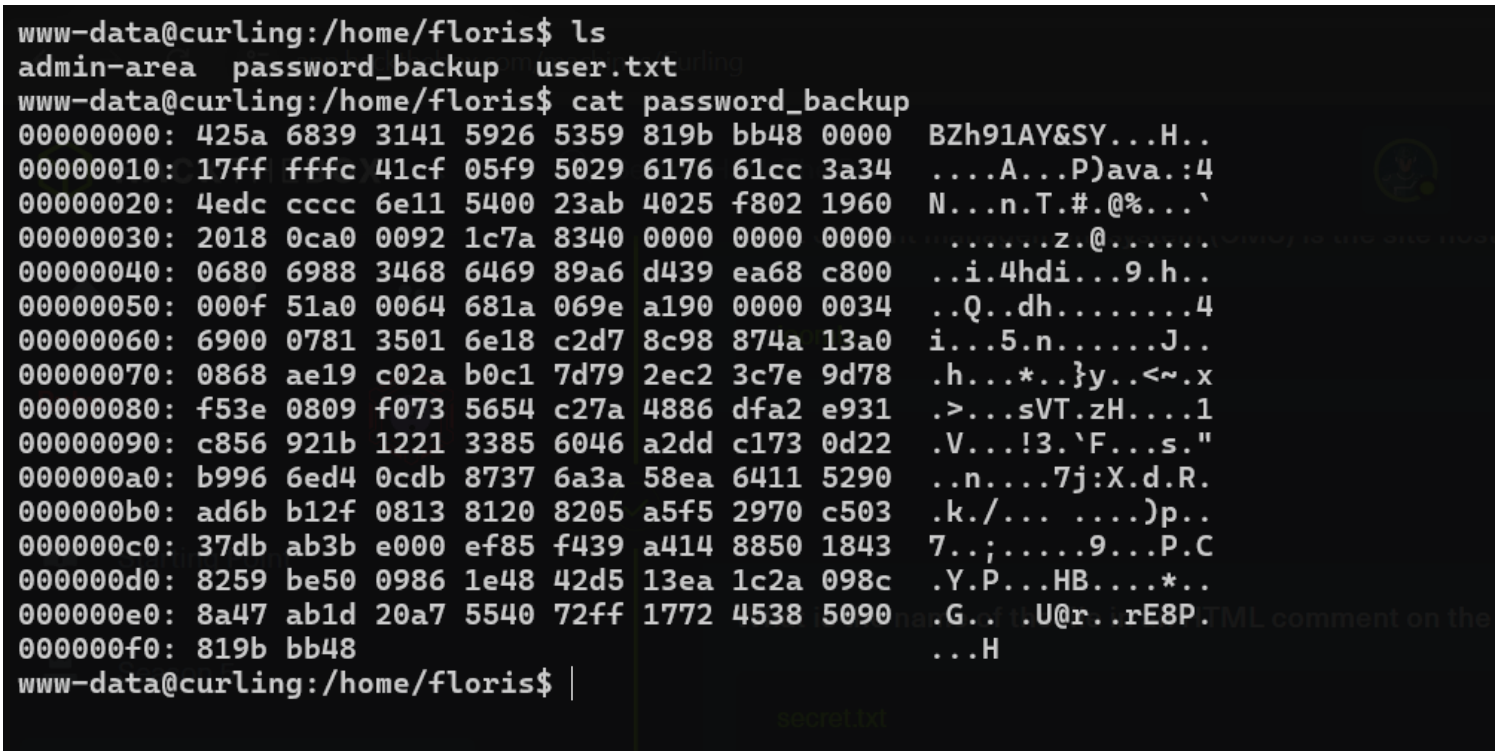
1) Injected reverse shell payload in template



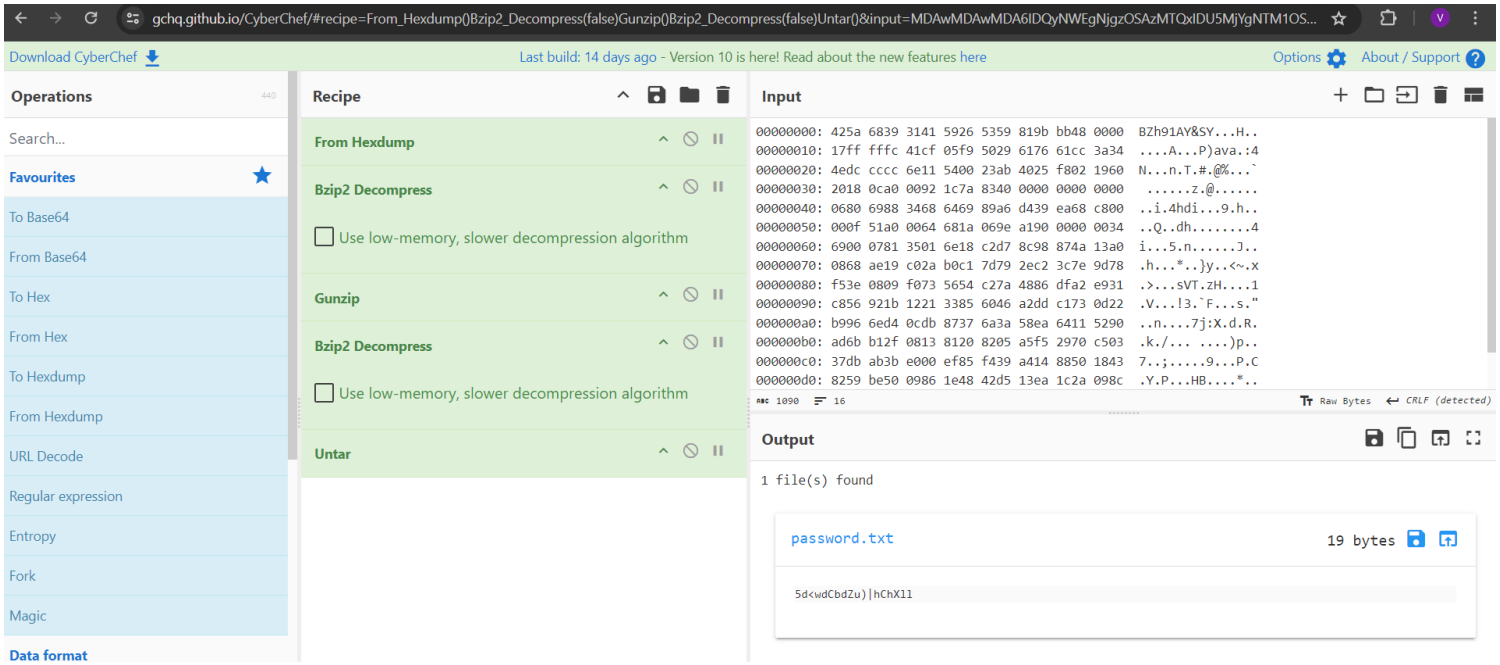
2) Got reverse shell

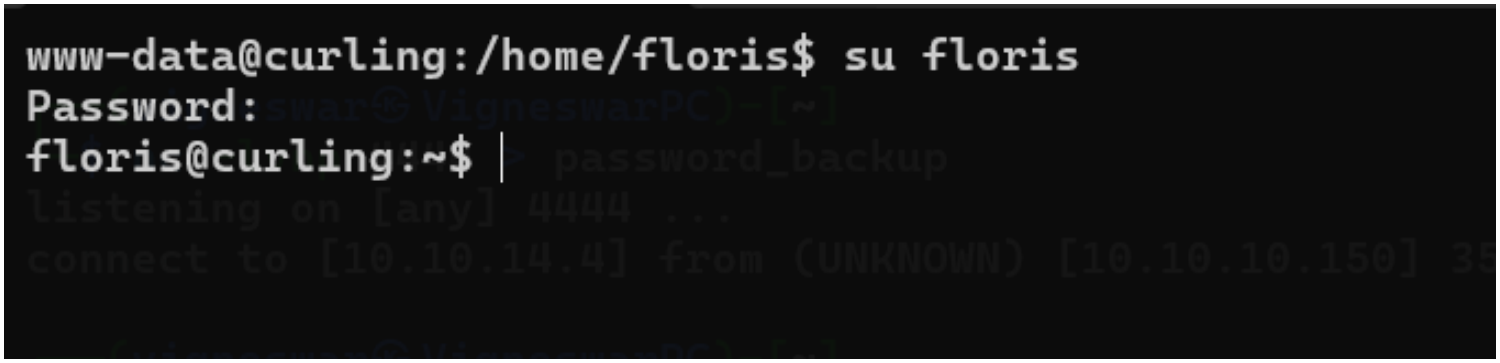


3) Found a strange file



4) Got the password

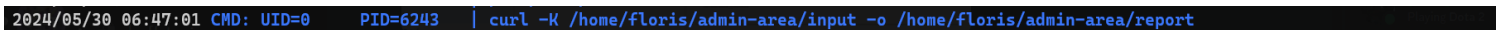


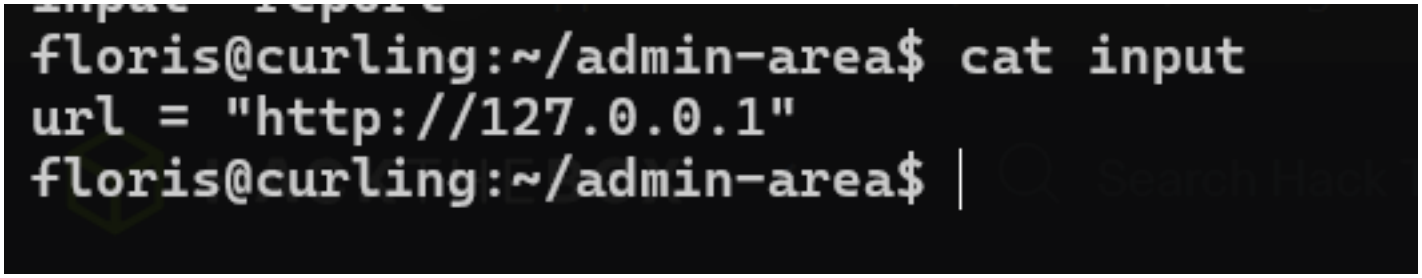


floris:5d<wdCbdZu)|hChXll

Privilege Escalation

1) There is a cron job running that runs curl





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$
```