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

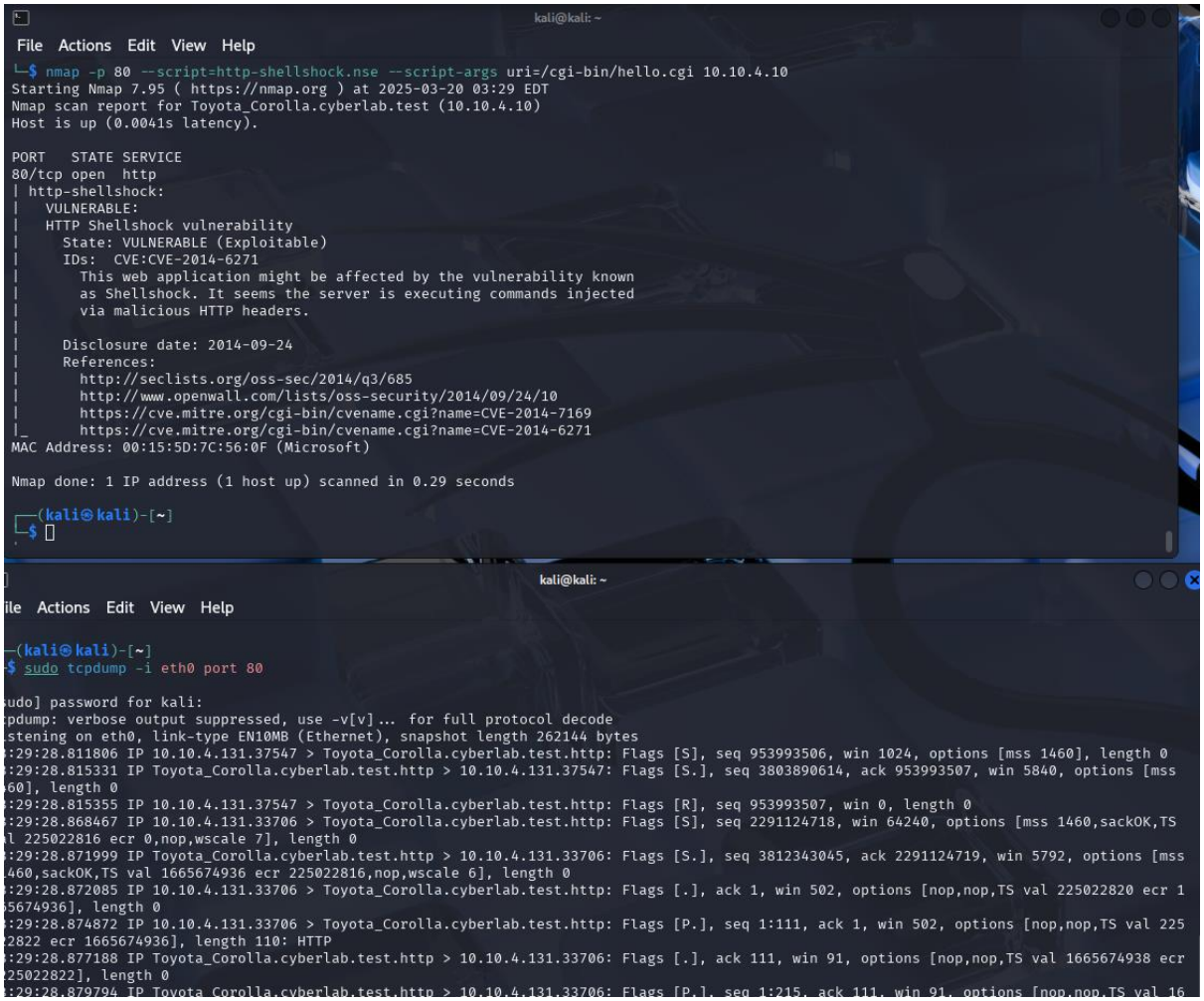
*Untitled 1 - Mousepad

File Edit Search View Document Help

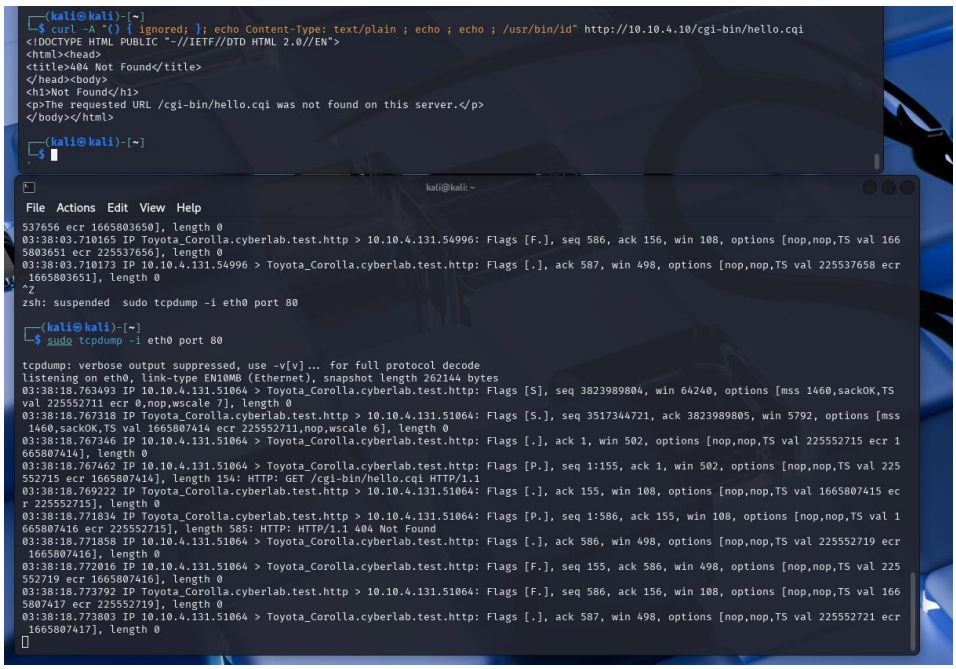
```
1 10.10.4.5-100
2 nmap -p80,443 --script=http-shellshock 10.10.4.20/cgi-bin
3 dirb http://10.10.4.20/cgi-bin/ -x .php,.txt,.html
4 nmap -p80 --script=http-shellshock 10.10.4.10/cgi-bin/
5 http://10.10.4.10/cgi-bin/
6
```

```
┌──(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
```

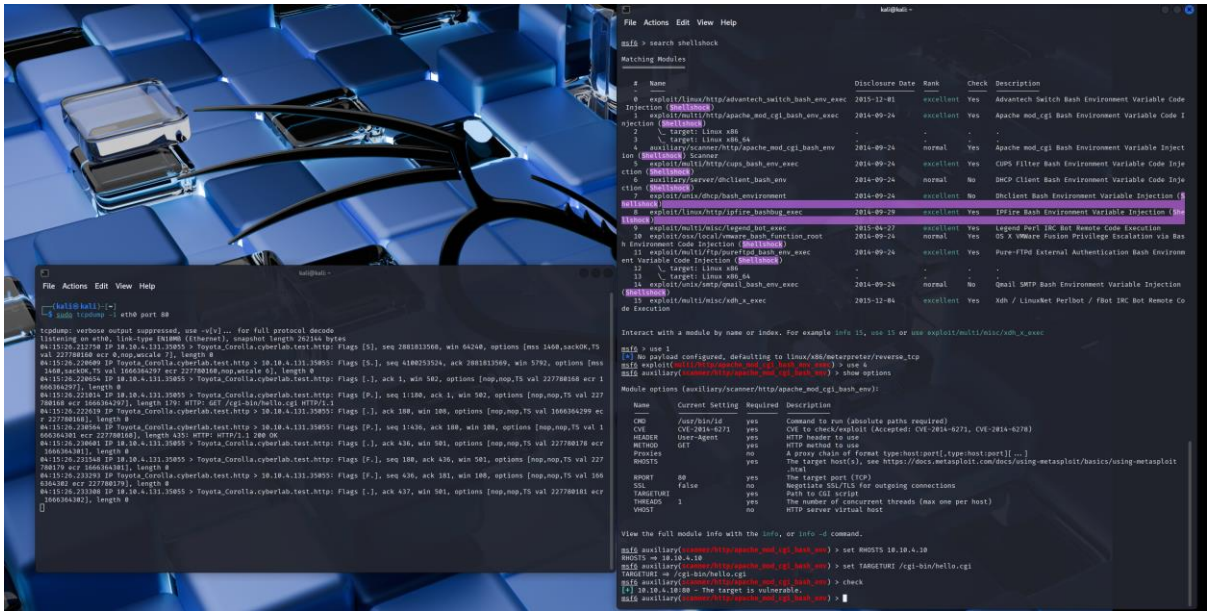
Step 3. Vulnerability Verification



Curl:



Metasploit:


File Actions Edit View Help
msf6 > search shellshock
Matching Modules
File Actions Edit View Help
(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
msf6 > use 1
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > use 4
msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > show options
Module options (auxiliary/scanner/http/apache_mod_cgi_bash_env):
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > set RHOSTS 10.10.4.10
RHOSTS => 10.10.4.10
msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > set TARGETURI /cgi-bin/hello.cgi
TARGETURI => /cgi-bin/hello.cgi
msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > check
[+] 10.10.4.10:80 - The target is vulnerable.
msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) >