



UNIVERSIDAD AUTÓNOMA DE CHIAPAS
LICENCIATURA EN INGENIERIA EN DESARROLLO
Y TECNOLOGIAS DE SOFTWARE



ANALISIS DE VULNERABILIDADES

Reporte: Ataques a DVWA

Nombres de los alumnos: Luis Gerardo Mendoza Gomez | A200004

Bryan Andrew Castro Valencia | A200728

Nombre del catedrático: Dr. Luis Gutiérrez Alfaro

Semestre: 7

Grupo: M

Fecha de entrega: 31/10/23

REPORTE DE ATAQUES AL DVWA EN BUSCA DE VULNERABILIDADES

Compañero atacado: Bryan Andrew

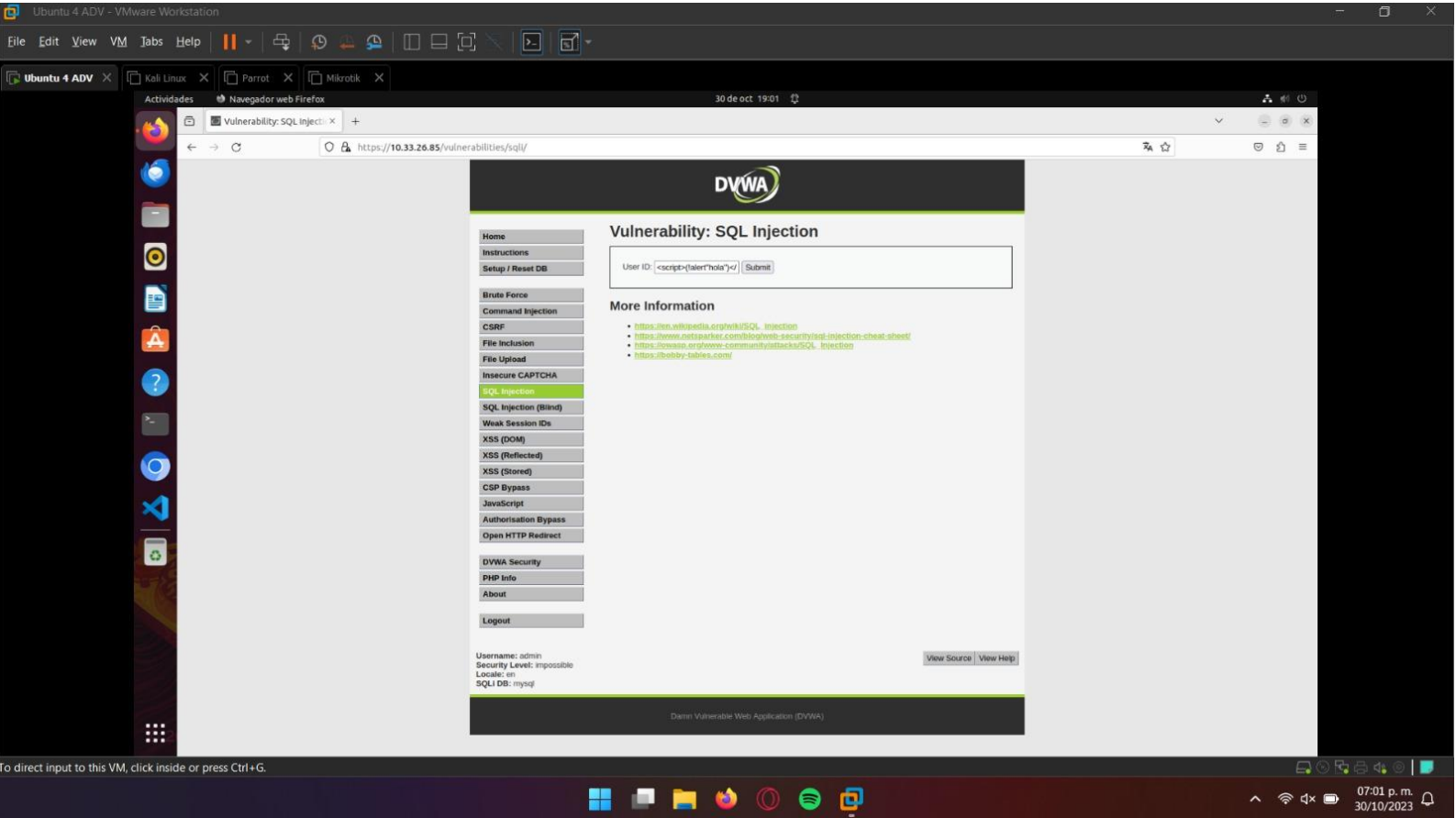
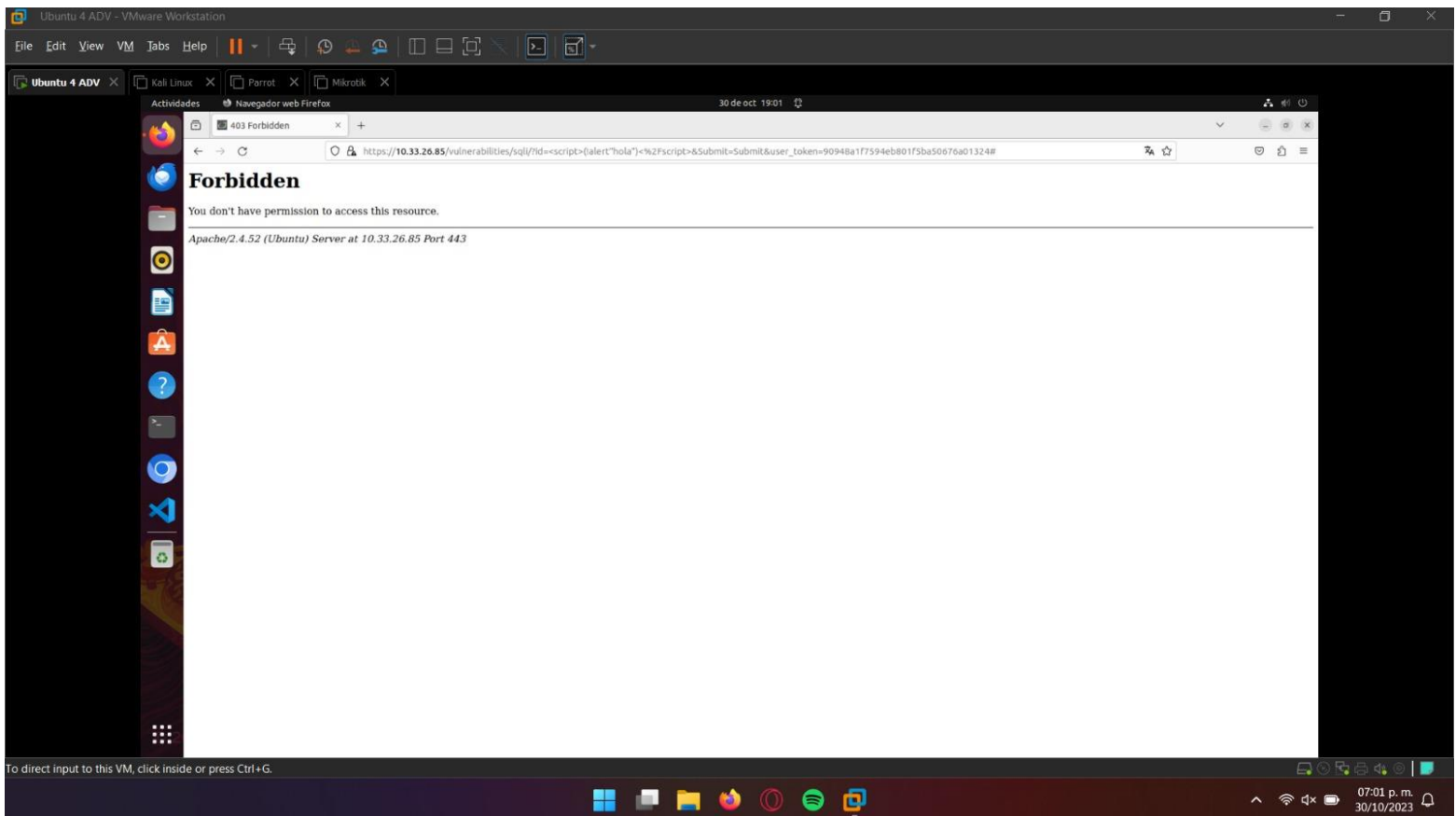


Imagen 1.0.- Ataque mediante uso de un Script



Como resultado del uso del script, el acceso es denegado, por lo cual esta parte se encuentra protegida.

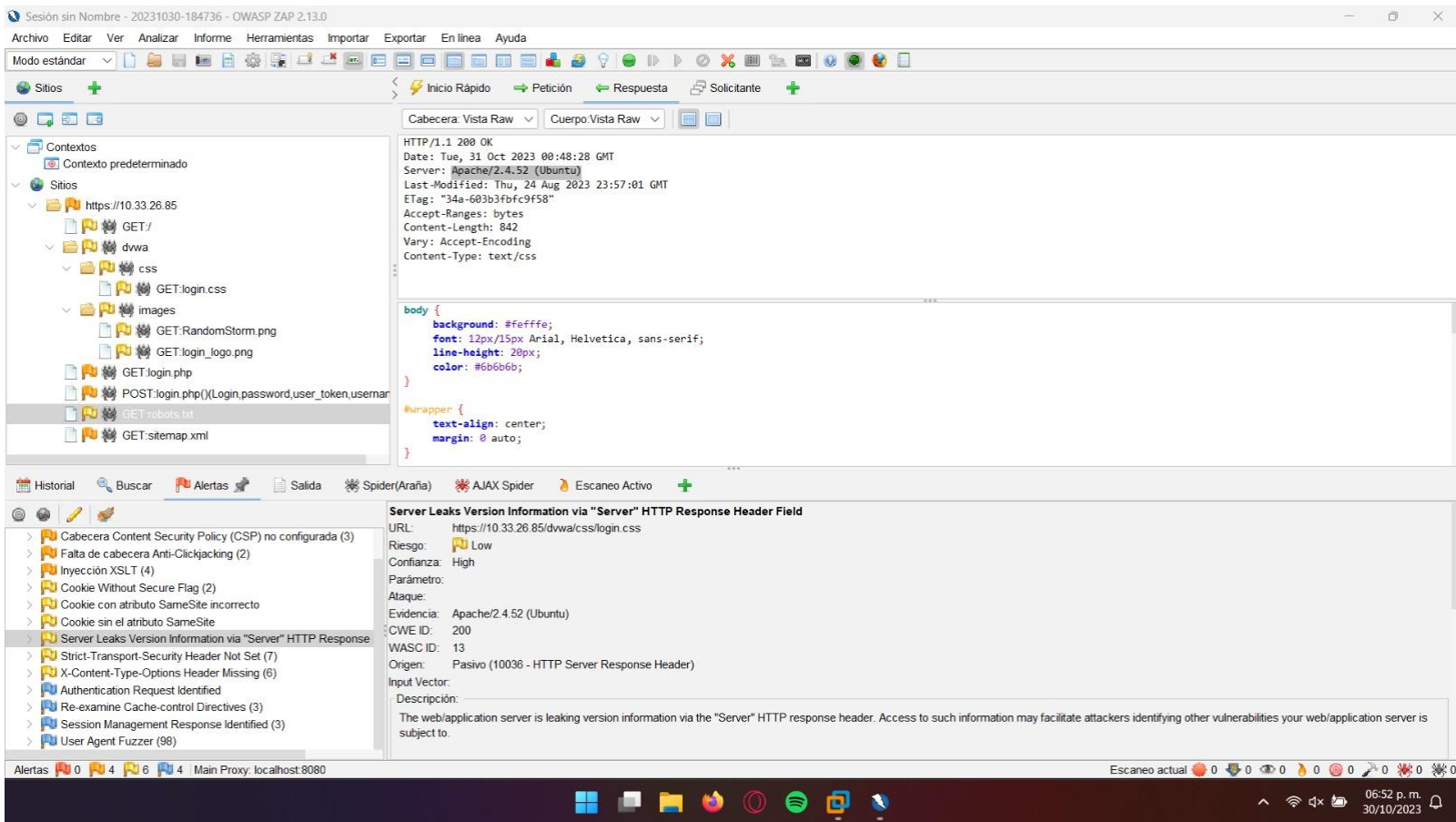
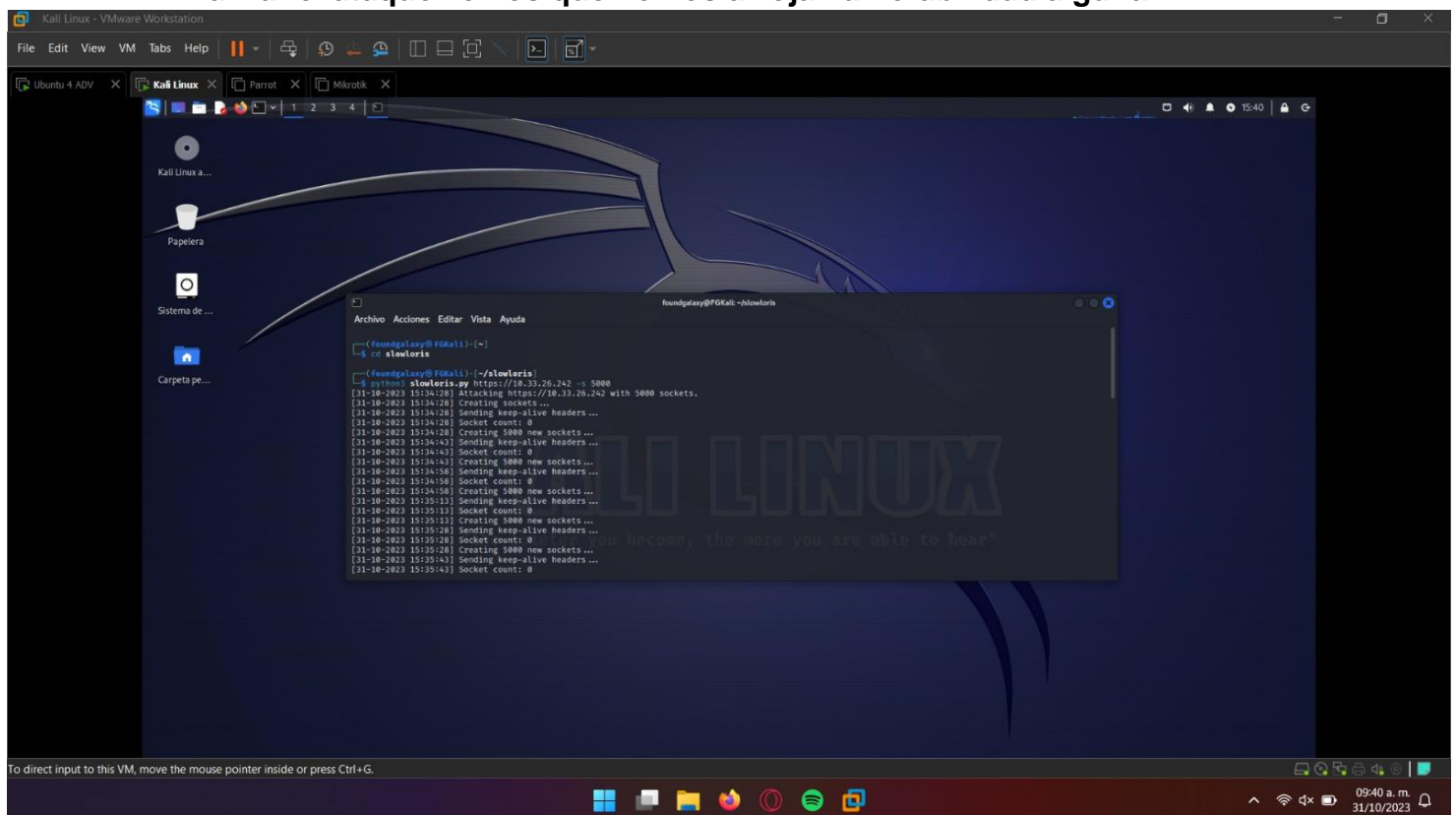
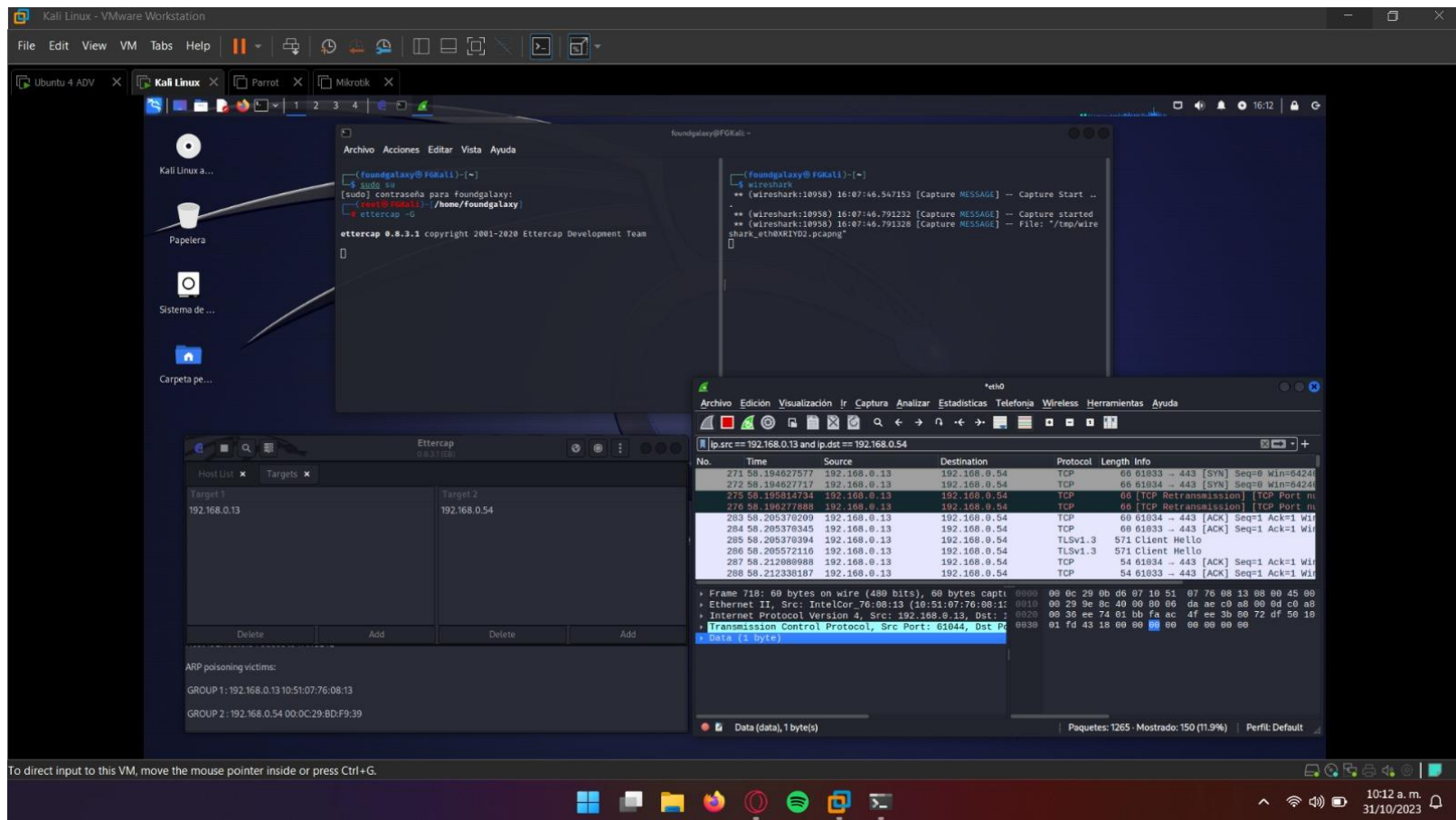


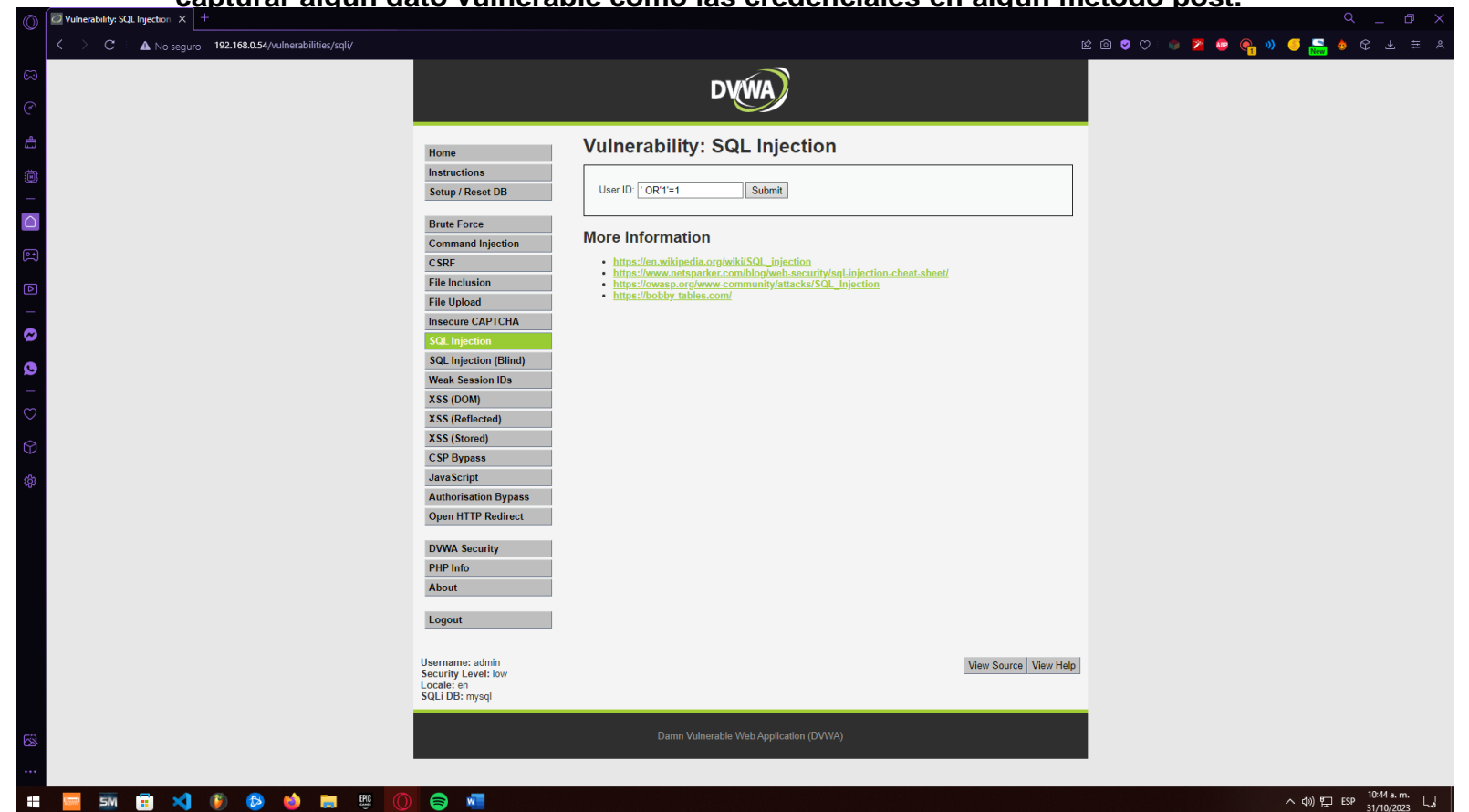
Imagen 2.0 .- Ataque mediante Zap de OWASP.
Al finalizar el ataque vemos que no nos arroja vulnerabilidad alguna.



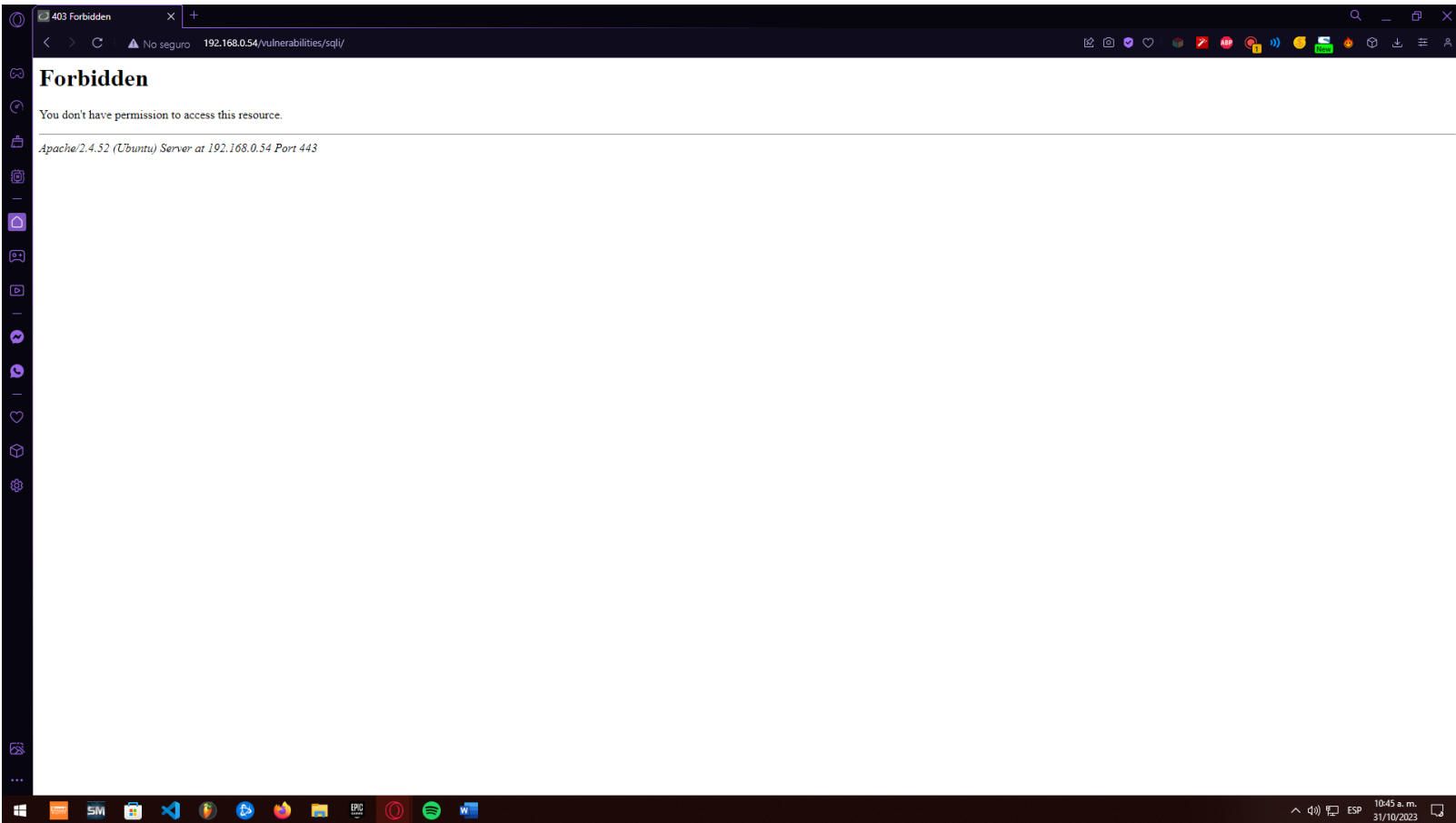
El ataque mediante Slowloris no logra “tirar” al dvwa, únicamente lo ralentiza.



Ataque haciendo uso de Ettercap y Wireshark, con este ataque tampoco se logra capturar algun dato vulnerable como las credenciales en algun método post.



Mediante un ataque de SQLInjection tampoco se encuentra alguna vulnerabilidad ya que nos denega el acceso.



Manual Explore

This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP. The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.

ID	Source	Req. Timestamp	Met...	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
4	Pro...	10/30/23, 8:50:53 PM	GET	https://10.33.26.242/dvwa/css/login.css	200	OK	38...	842 bytes			
10	Pro...	10/30/23, 8:50:57 PM	GET	https://10.33.26.242/	302	Found	30...	0 bytes	Low		SetCookie
11	Pro...	10/30/23, 8:50:57 PM	GET	https://10.33.26.242/login.php	200	OK	51...	1,395 bytes			
12	Pro...	10/30/23, 8:50:58 PM	GET	https://10.33.26.242/dvwa/css/login.css	200	OK	32...	842 bytes	Low		
16	Pro...	10/30/23, 8:51:04 PM	GET	https://10.33.26.242/index.php	200	OK	18...	6,103 bytes			
17	Pro...	10/30/23, 8:51:04 PM	GET	https://10.33.26.242/dvwa/css/main.css	200	OK	24...	4,026 bytes	Low		
18	Pro...	10/30/23, 8:51:04 PM	GET	https://10.33.26.242/dvwa/js/dvwaPage.js	200	OK	13...	1,030 bytes			
21	Pro...	10/30/23, 8:51:04 PM	GET	https://10.33.26.242/dvwa/js/add_event_list...	200	OK	12...	593 bytes			
22	Pro...	10/30/23, 8:51:07 PM	GET	https://10.33.26.242/vulnerabilities/sql_blind/	200	OK	16...	4,322 bytes	Medium		Form, Hidden, S...
25	Pro...	10/30/23, 8:51:10 PM	GET	https://10.33.26.242/vulnerabilities/sql_blind...	200	OK	24...	4,364 bytes	Medium		Form, Hidden, S...
15	Pro...	10/30/23, 8:51:04 PM	POST	https://10.33.26.242/login.php	302	Found	68...	0 bytes	Low		

NO SALE METODO POST PARA HACER SLQ INYECCION

NO SE PUEDE METER SCRIPTS

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

More Information

403 Forbidden

https://10.33.26.242/vulnerabilities/xss_r/?n

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

Forbidden

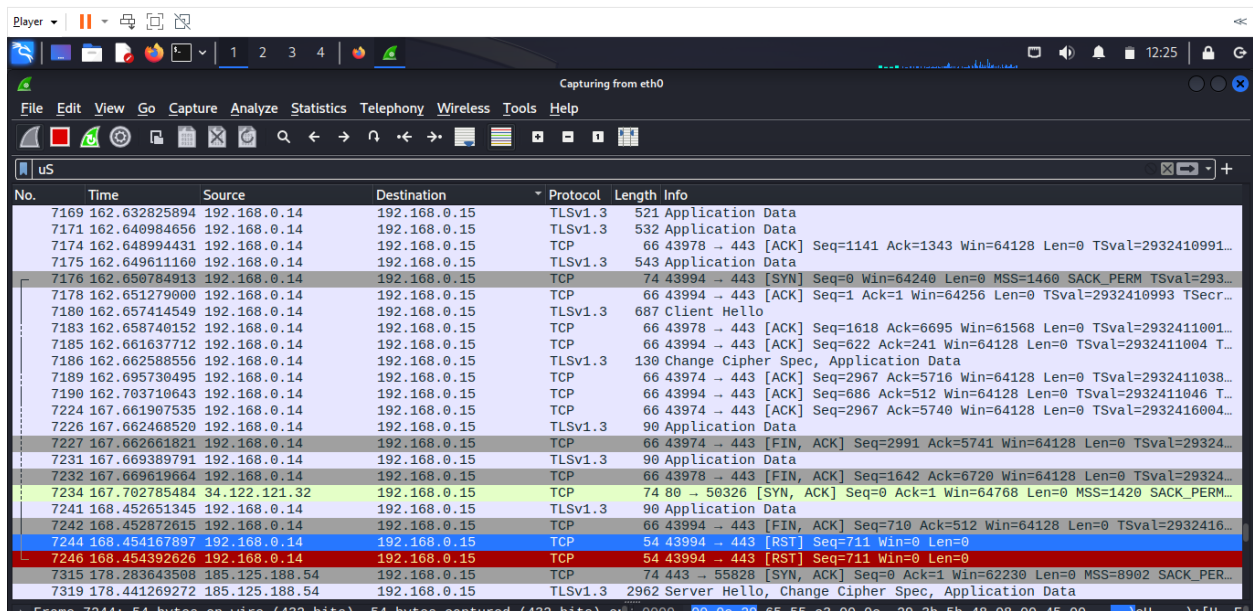
You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at 10.33.26.242 Port 443

Si es vulnerable a SLOWLORIS

```
(kali@kali)-[~/Desktop/slowloris/slowloris]
$ python3 slowloris.py 10.33.26.242 -s 5000
[30-10-2023 20:57:07] Attacking 10.33.26.242 with 5000 sockets.
[30-10-2023 20:57:07] Creating sockets ...
[30-10-2023 20:57:22] Sending keep-alive headers ...
[30-10-2023 20:57:22] Socket count: 662
[30-10-2023 20:57:22] Creating 4338 new sockets ...
30/10/23, 8:51:04 PM POST https://10.33.26.242/login.php
5 Main Proxy: localhost:8080
```

NO HAY VULNERABILIDADES EN WIRESHARK



No.	Time	Source	Destination	Protocol	Length	Info
7169	162.632825894	192.168.0.14	192.168.0.15	TLSv1.3	521	Application Data
7171	162.640984656	192.168.0.14	192.168.0.15	TLSv1.3	532	Application Data
7174	162.648994431	192.168.0.14	192.168.0.15	TCP	66	43978 → 443 [ACK] Seq=1141 Ack=1343 Win=64128 Len=0 TSval=2932410991...
7175	162.649611160	192.168.0.14	192.168.0.15	TLSv1.3	543	Application Data
7176	162.650784913	192.168.0.14	192.168.0.15	TCP	74	43994 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=293...
7178	162.651279000	192.168.0.14	192.168.0.15	TCP	66	43994 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2932410993 TSecr...
7180	162.657414549	192.168.0.14	192.168.0.15	TLSv1.3	687	Client Hello
7183	162.658740152	192.168.0.14	192.168.0.15	TCP	66	43978 → 443 [ACK] Seq=1618 Ack=6695 Win=61568 Len=0 TSval=2932411001...
7185	162.661637712	192.168.0.14	192.168.0.15	TCP	66	43994 → 443 [ACK] Seq=622 Ack=241 Win=64128 Len=0 TSval=2932411004 T...
7186	162.662588556	192.168.0.14	192.168.0.15	TLSv1.3	130	Change Cipher Spec, Application Data
7189	162.695730495	192.168.0.14	192.168.0.15	TCP	66	43974 → 443 [ACK] Seq=2967 Ack=5716 Win=64128 Len=0 TSval=2932411038...
7190	162.703710643	192.168.0.14	192.168.0.15	TCP	66	43994 → 443 [ACK] Seq=686 Ack=512 Win=64128 Len=0 TSval=2932411046 T...
7224	167.661907535	192.168.0.14	192.168.0.15	TCP	66	43974 → 443 [ACK] Seq=2967 Ack=5740 Win=64128 Len=0 TSval=2932416004...
7226	167.662468520	192.168.0.14	192.168.0.15	TLSv1.3	90	Application Data
7227	167.662661821	192.168.0.14	192.168.0.15	TCP	66	43974 → 443 [FIN, ACK] Seq=2991 Ack=5741 Win=64128 Len=0 TSval=29324...
7231	167.669389791	192.168.0.14	192.168.0.15	TLSv1.3	90	Application Data
7232	167.669619664	192.168.0.14	192.168.0.15	TCP	66	43978 → 443 [FIN, ACK] Seq=1642 Ack=6720 Win=64128 Len=0 TSval=29324...
7234	167.702785484	34.122.121.32	192.168.0.15	TCP	74	80 → 50326 [SYN, ACK] Seq=0 Ack=1 Win=64768 Len=0 MSS=1420 SACK_PERM...
7241	168.452651345	192.168.0.14	192.168.0.15	TLSv1.3	90	Application Data
7242	168.452872615	192.168.0.14	192.168.0.15	TCP	66	43994 → 443 [FIN, ACK] Seq=710 Ack=512 Win=64128 Len=0 TSval=2932416...
7244	168.454167897	192.168.0.14	192.168.0.15	TCP	54	43994 → 443 [RST] Seq=711 Win=0 Len=0
7246	168.454392626	192.168.0.14	192.168.0.15	TCP	54	43994 → 443 [RST] Seq=711 Win=0 Len=0
7315	178.283643508	185.125.188.54	192.168.0.15	TCP	74	443 → 55828 [SYN, ACK] Seq=0 Ack=1 Win=62230 Len=0 MSS=8902 SACK_PER...
7319	178.441269272	185.125.188.54	192.168.0.15	TLSv1.3	2962	Server Hello, Change Cipher Spec, Application Data

NO ES VULNERABLE A SQL INYECCION

Vulnerability: SQL Injection

User ID:

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

Forbidden

You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at 192.168.0.15 Port 443