UNIVERSIDAD AUTÓNOMA DE CHIAPAS

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN
CAMPUS 1

ING. EN DESARROLLO Y TECNOLOGÍAS DE SOFTWARE

7 “M”

OPT.2 - ANÁLISIS DE VULNERABILIDADES

SUB2 - HUELLAS DIGITALES Y RECONOCIMIENTO

ACT. 2.3 REALIZAR LOS SIGUIENTE ATAQUES SQLMAP AL DVWA EN EQUIPO

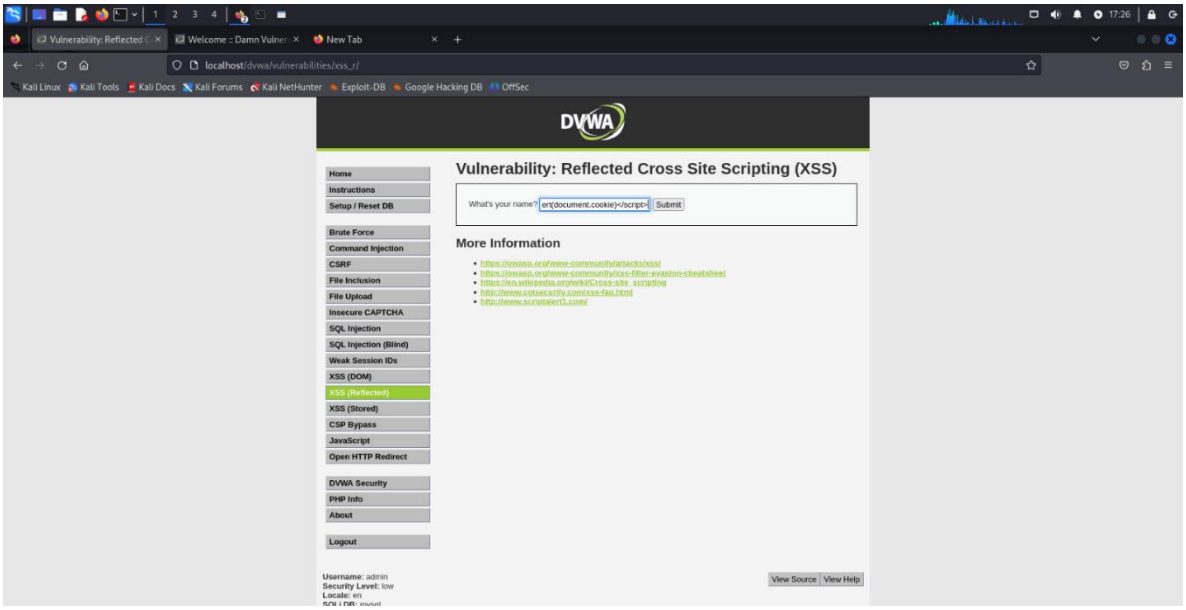
ALUMNOS:
GABRIEL OMAR FUENTES CHACÓN – A211120
LUIS EDUARDO GONZÁLEZ GUILLÉN – A211397
STEVEN DE DIOS MONTOYA HERNÁNDEZ – A211387
MARCO ANTONIO ZÚÑIGA MORALES – A211121

DOCENTE: DR. LUIS GUTIÉRREZ ALFARO

TUXTLA GUTIÉRREZ, CHIAPAS
SÁBADO, 13 DE ABRIL DE 2024

1.- Cross Site Scriptiong (XSS) Reflected

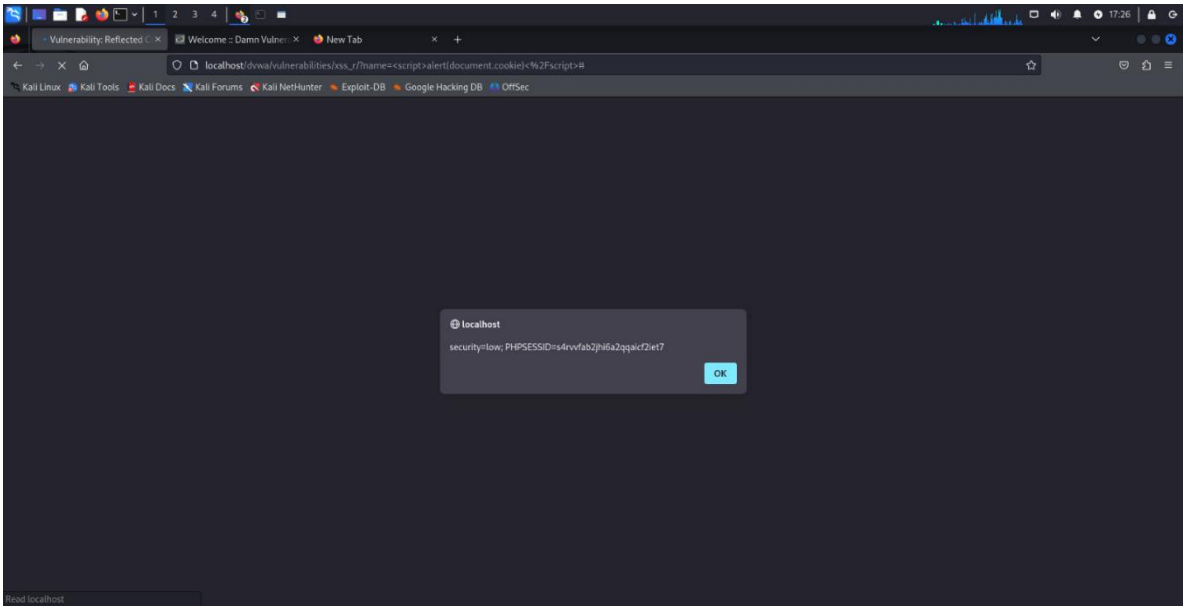
Es básicamente usar inputs de páginas para meter scripts, para esto, sacamos a XSS reflected donde nos pide su nombre



En este caso como podemos usar la vulnerabilidad del input podemos poner scripts de php en este caso lo que quiero obtener son las cookies.

<script>alert(document.cookie)</script>

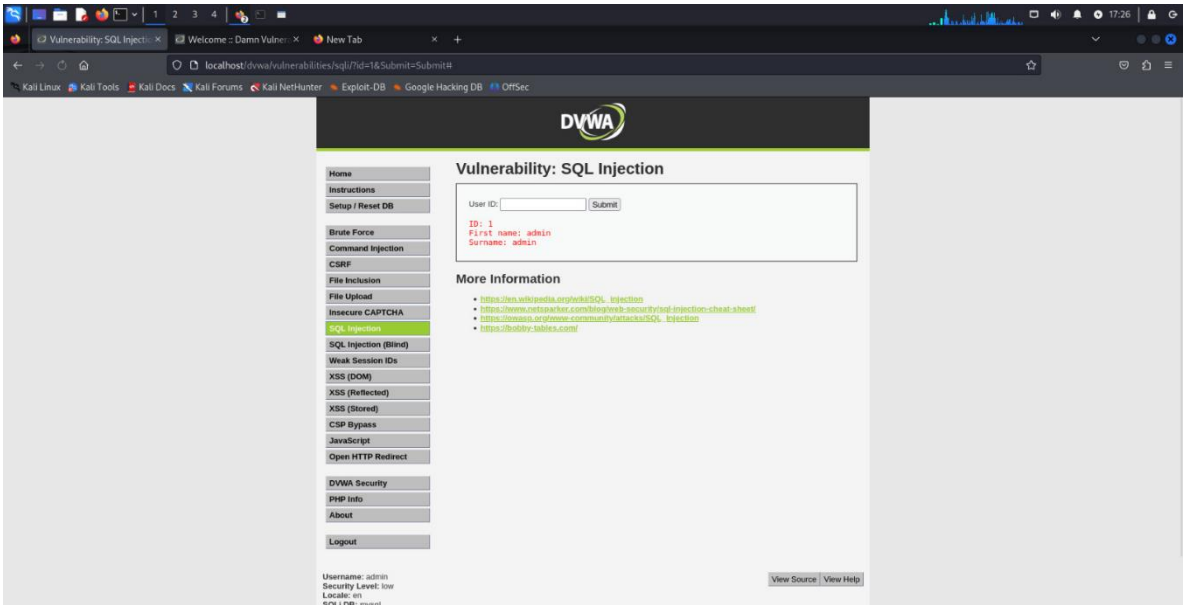
Con esto podemos obtener las cookies y el nivel de seguridad de DVWA



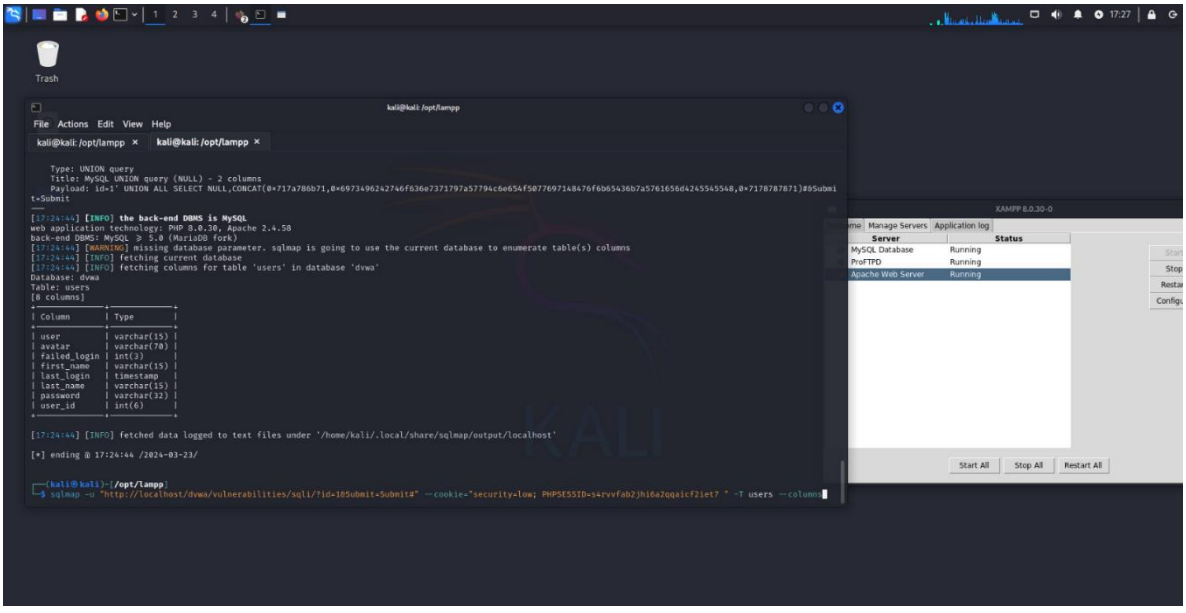
De igual forma podemos ejecutar más scripts en ese input pero en este caso solo usaremos el de cookies.

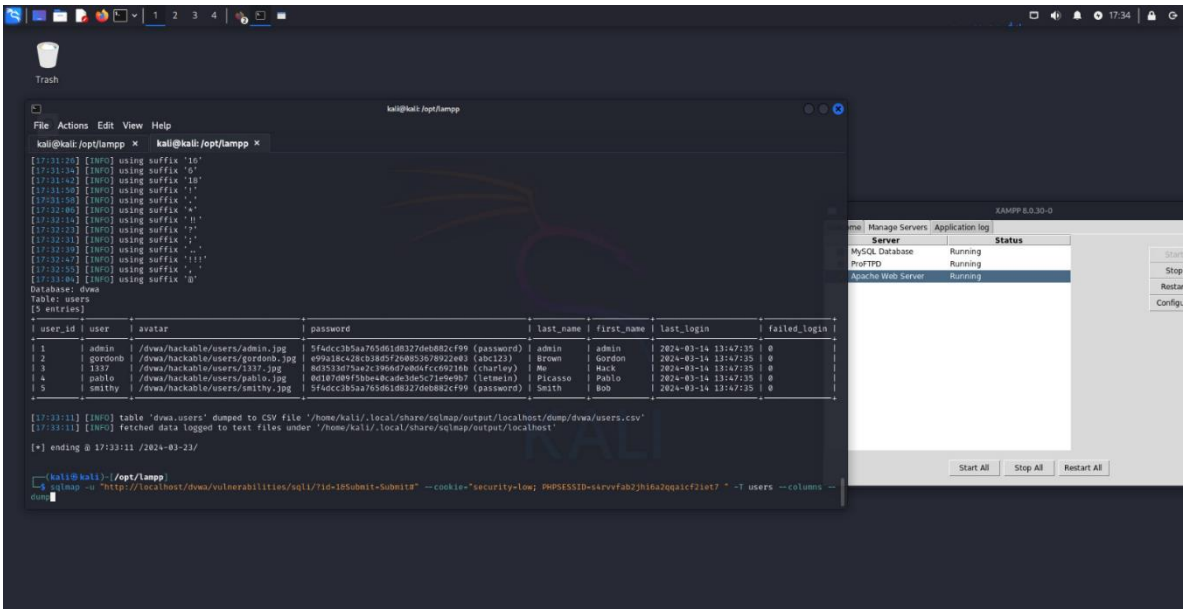
2. SQLMap

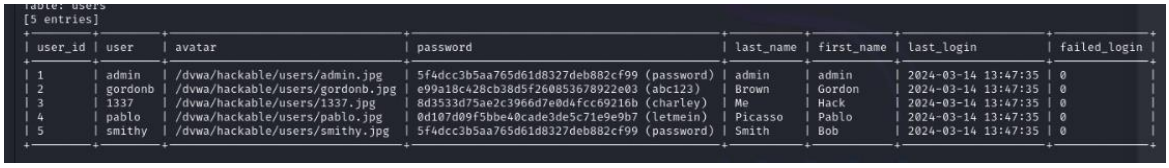
Ya es cosa de solo usar SQLMap para poder ver la base de datos para ver los usuarios y contraseñas haciendo de ayuda el SQL INJECTION



Tomamos el link ya que tiene un submit para obtener una persona de la base de datos.







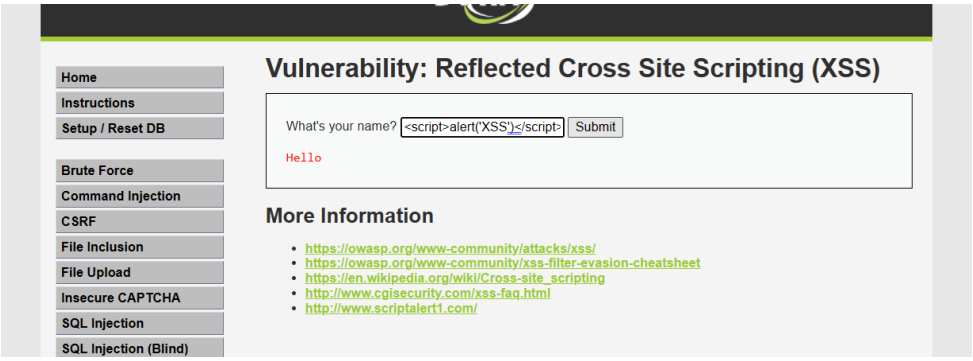
[5 entries]

user_id	user	avatar	password	last_name	first_name	last_login	failed_login
1	admin	/dvwa/hackable/users/admin.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin	2024-03-14 13:47:35	0
2	gordonb	/dvwa/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon	2024-03-14 13:47:35	0
3	1337	/dvwa/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack	2024-03-14 13:47:35	0
4	pablo	/dvwa/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo	2024-03-14 13:47:35	0
5	smithy	/dvwa/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob	2024-03-14 13:47:35	0

Y finalmente pudimos obtener los usuarios y contraseñas con SQL Injection (SQLMAP) y XSS Reflected.

3. Otras vulnerabilidades con XSS Reflected

<script>alert('XSS')</script>



<script>alert('hola esto es una alerta')</script>