

hACKING éTICO

Unidad 2. Actividad 16



13 de DICIEMbre de 2023

Carlos DÍAZ MONTES

ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

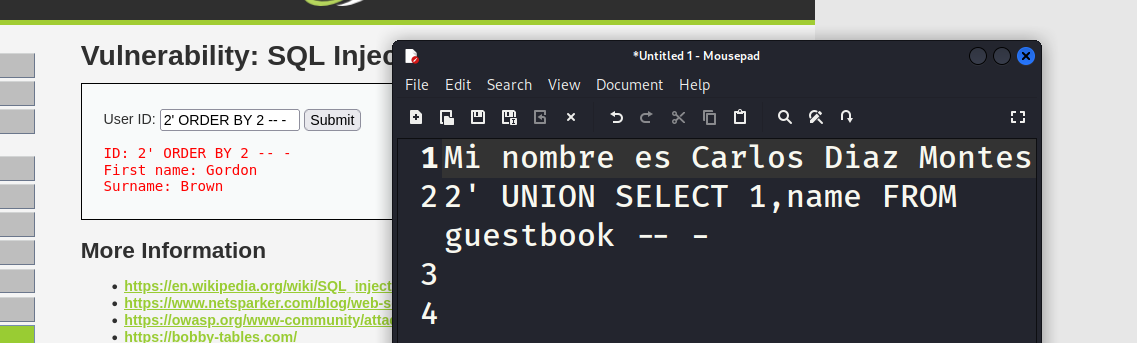
[Ejercicio 1. 2](#_Toc152183703)

# SQL Injection – Descubrimiento de la base de datos.

# Conocer número de columnas

Ejercicio 1: número de columnas de la select

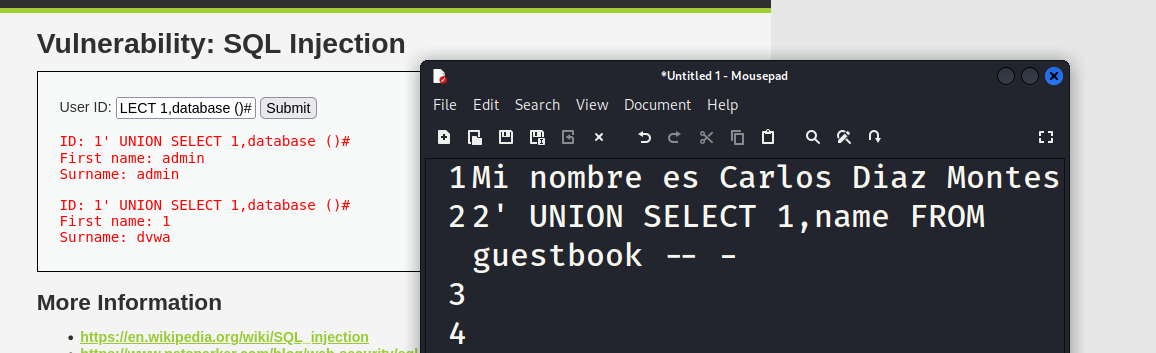
Para ver el número de columnas que tiene la base de datos simplemente vamos incrementando el numero de 2’ ORDER BY **X,** en el momento en el cual deja de funcionar significa que has superado el límite de columnas:



# 2. Conocer el nombre de la base de datos actual.

Ejercicio 2: Nombre de la base de datos y usuario.

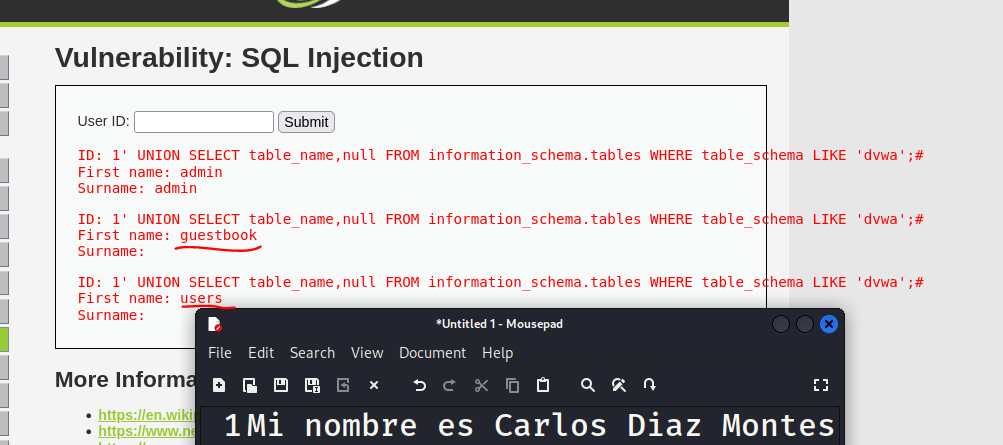
El nombre del usuario es admin y el de la base de datos dvwa. Para esto he puesto 2’ UNION SELECT 1,database ()#



# 3. Consultar tablas en el information\_schema.

Ejercicio 3: Obtén la lista de tablas de la base de datos actual.

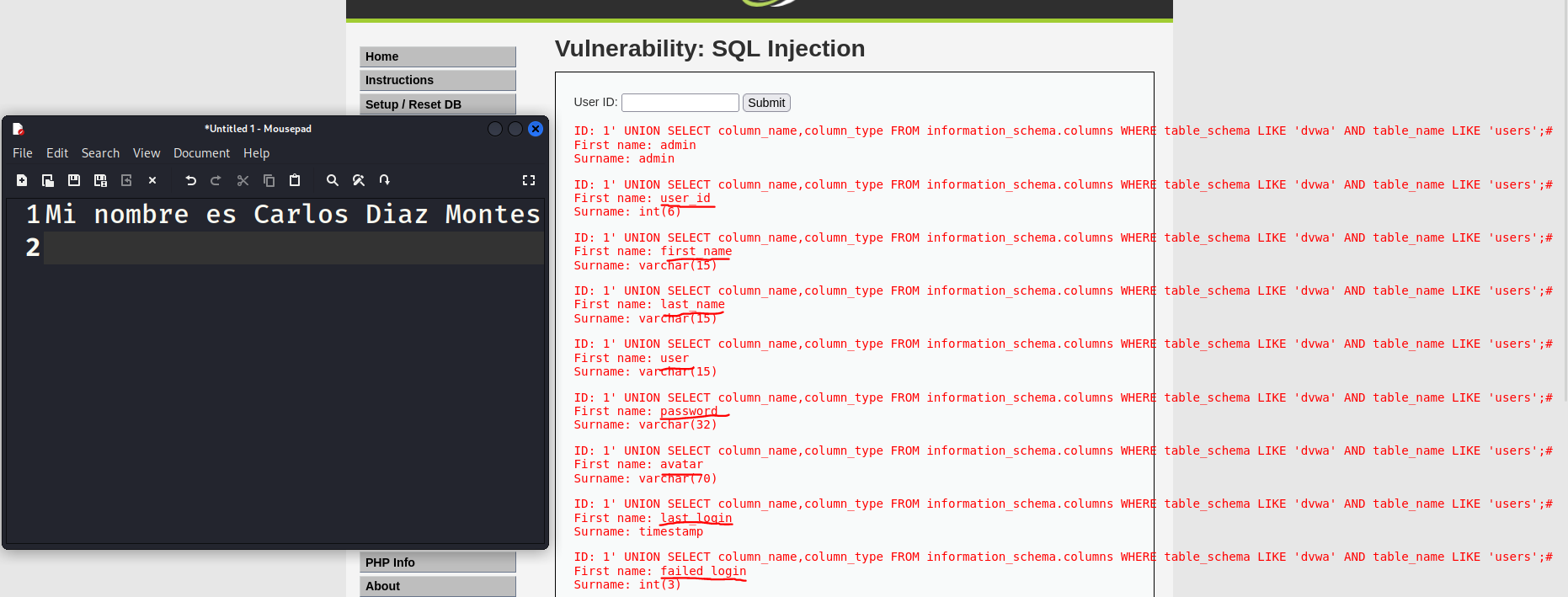
Las tablas son:



# 4. Consultar nombres de columnas de una tabla.

Ejercicio 4: Estructura de la tabla de usuarios

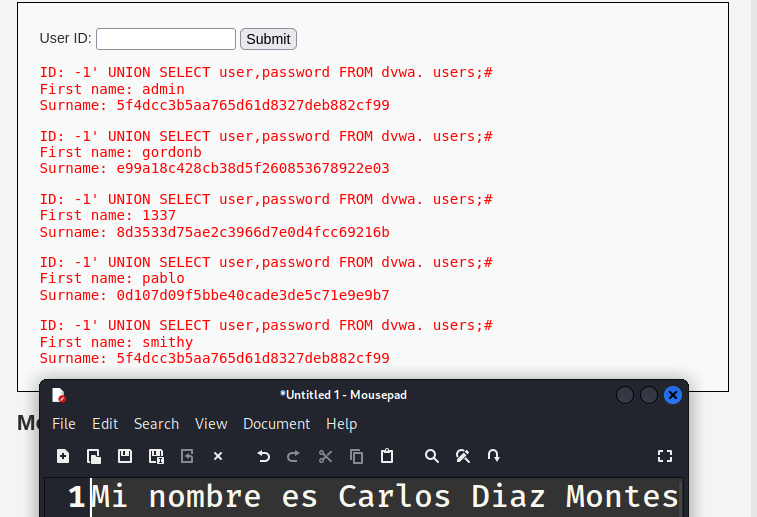
La estructura de la columna de usuario es:



# 5. Consultar datos de la tabla.

Ejercicio 5: Usuarios y contraseñas de la tabla users

Como anteriormente hemos sabido el nombre de la columna user y password, simplemente vamos a pedirla (el comando usado es 1’ UNION SELECT user,password FROM dvwa.users;#):



Ejercicio 6: Obtén las contraseñas con John The Ripper

Nos creamos un documento txt con el nombre hashes y metemos ahí todos los nombres de usuarios con sus respectivas contraseñas: