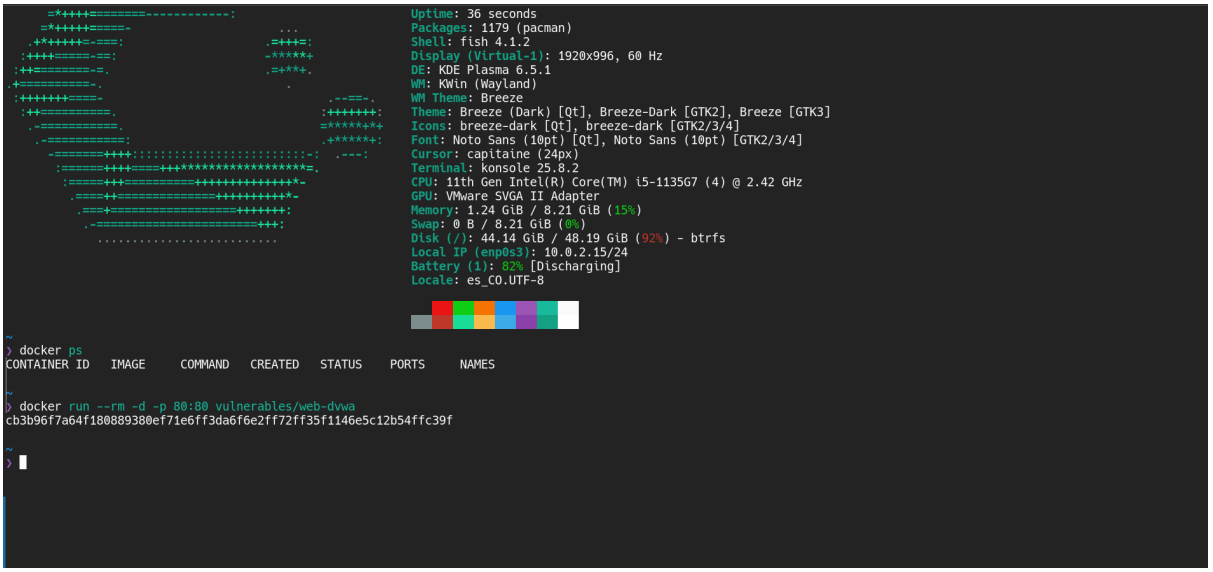
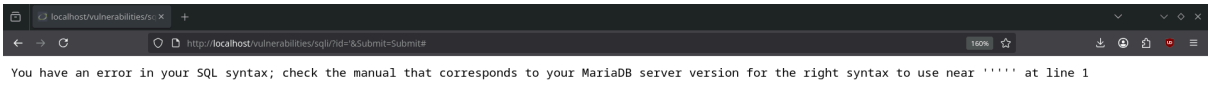
Laboratorio inyeccion SQL con DVWA en docker.

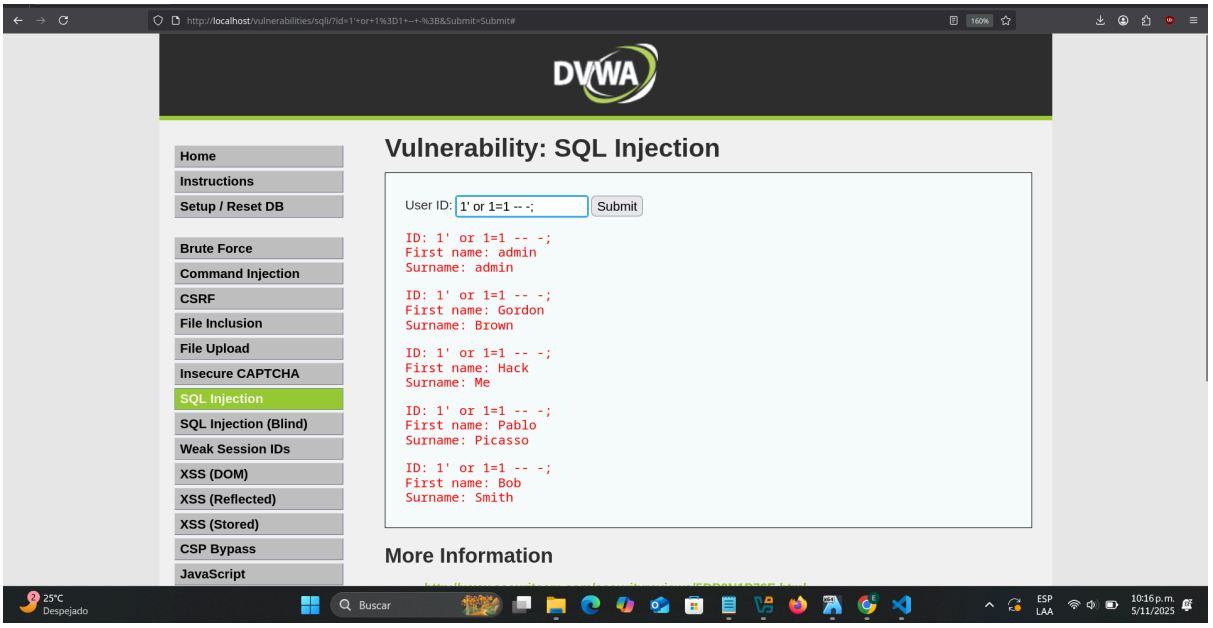


luego de haber arrancado el servicio, iniciado session, crear la database y conocer un poco la interfaz. (readme)

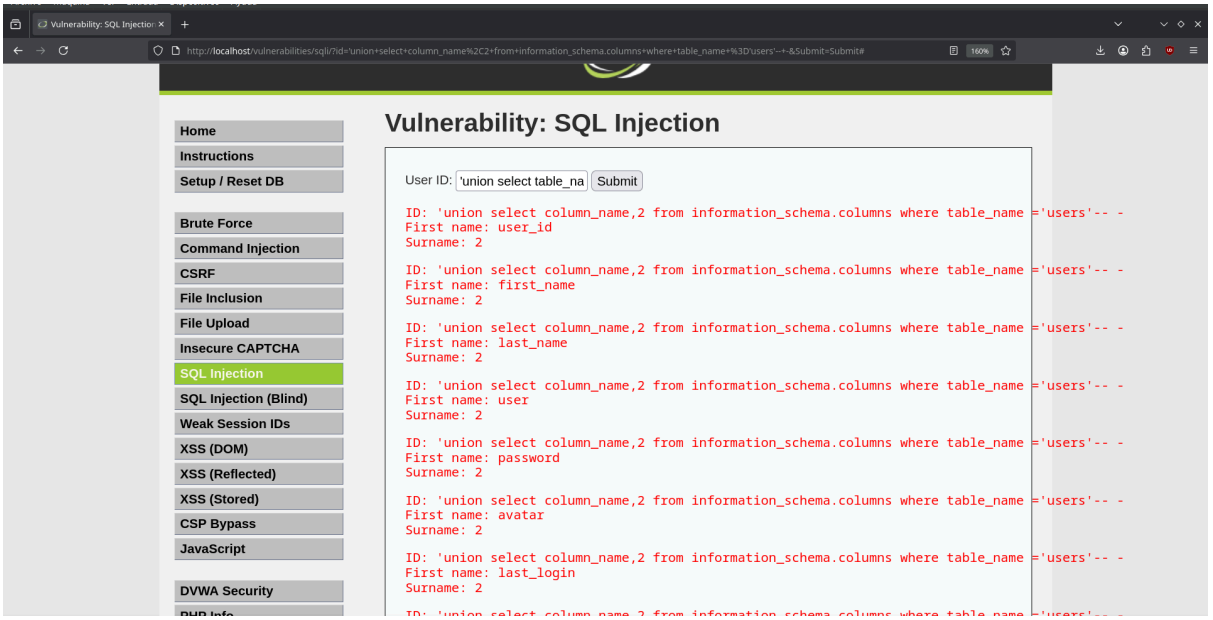
ahora en la dificultad low, probaremos colocar una comilla, veremos que pasa:



como podemos ver nos arroja un error de sintaxis, también nos arroja el servidor que está detrás de la base de datos, esta nueva página que se abrió significa que la base de datos en vulnerable a inyecciones sql de bajo nivel.



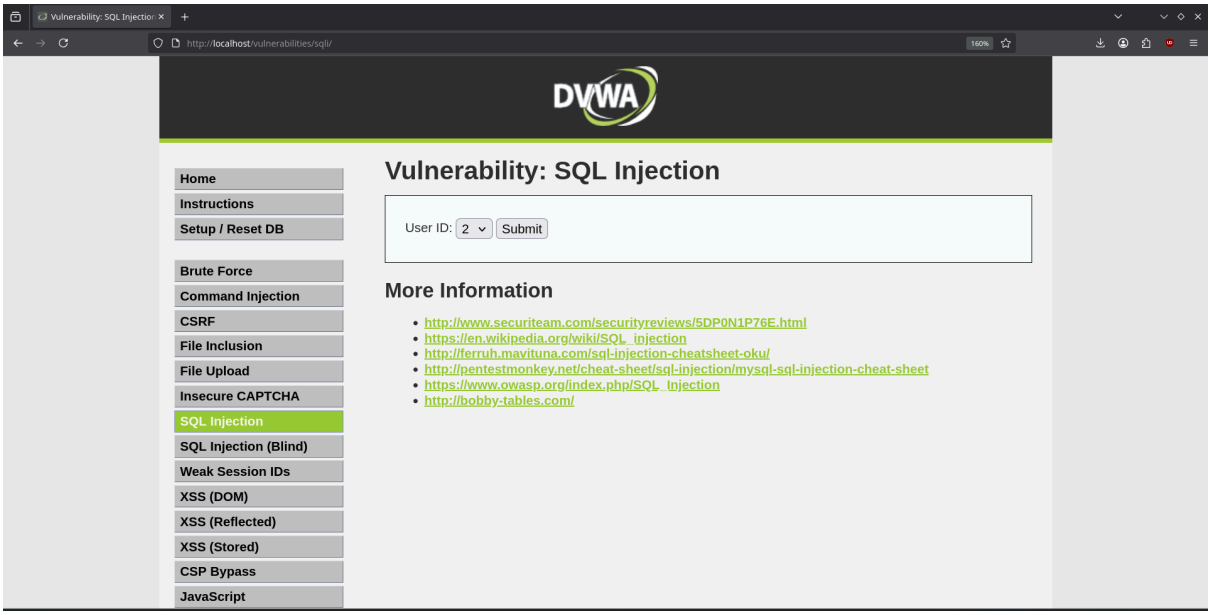
con esta nueva inyeccion le mandamos una petición a la base de datos para que nos muestre todos los usuarios que esta tiene.



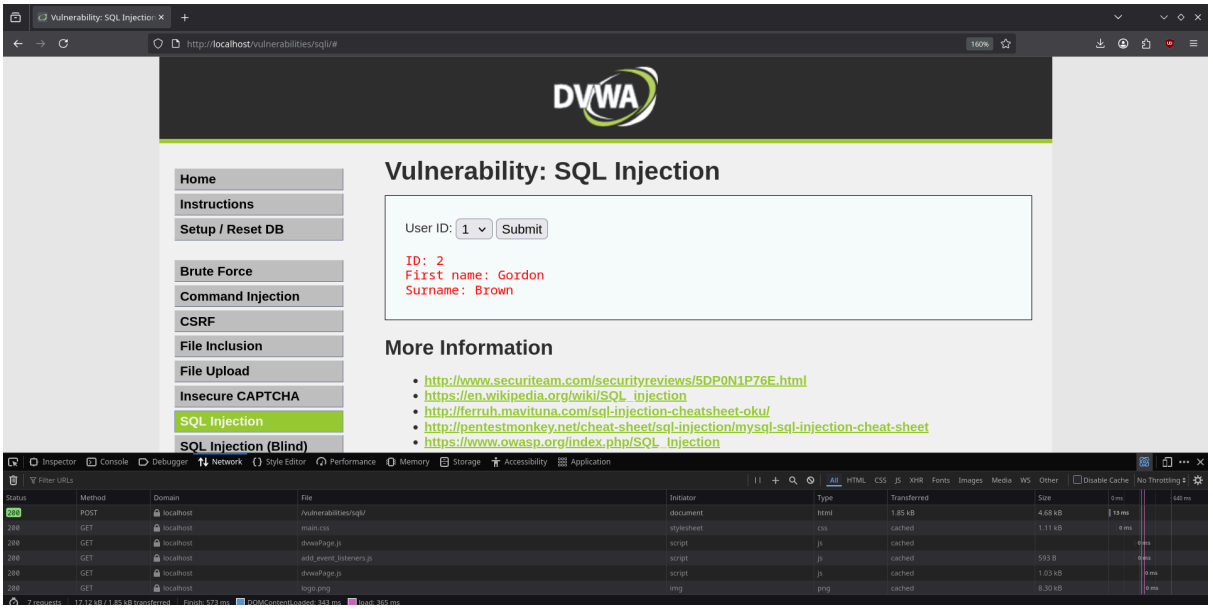
si deseamos ver el nombre de las columnas de la tabla usuario, se aplica la consulta de arriba

---

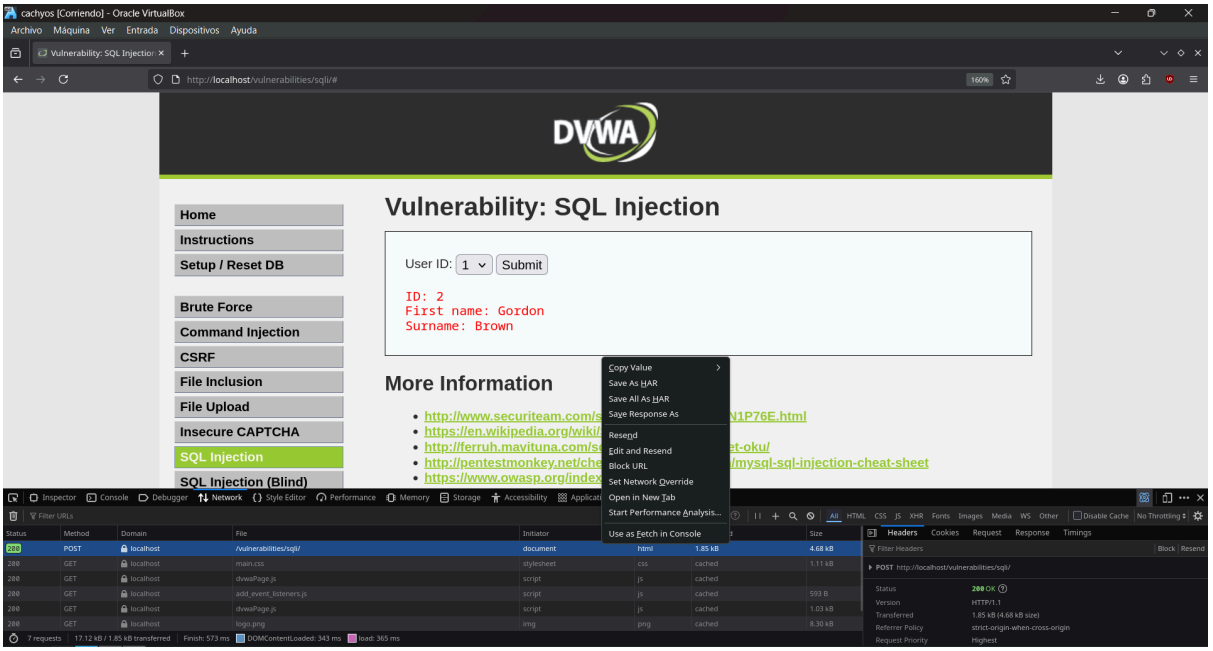
Inyeccion medium



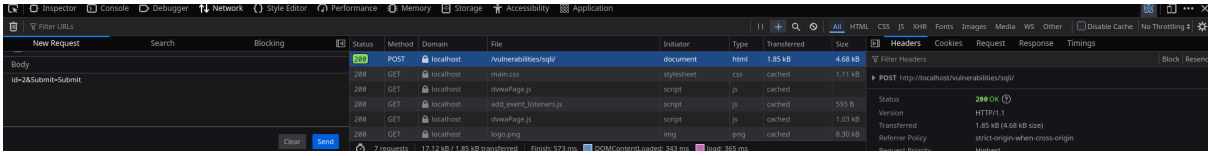
en el siguiente nivel no hay un campo para poder hacer nuestras inyecciones, lo haremos de otra manera.



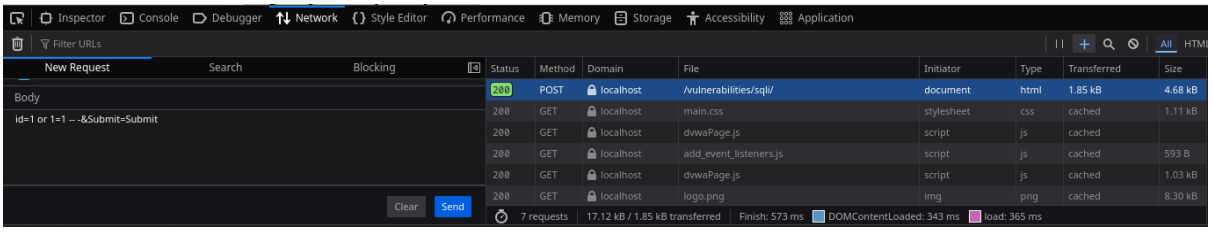
abriremos nuestro modo inspeccionar, nos vamos a network, despues enviamos en submit en la interfaz, esto se hace para poder capturar la peticion que se hace a través del botón



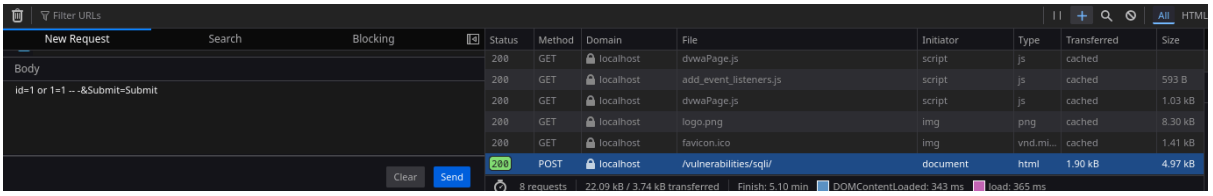
el siguiente paso es darle en “edit and resend” esto para enviar de nuevo la peticion, pero en esa nueva request se pueda editar.



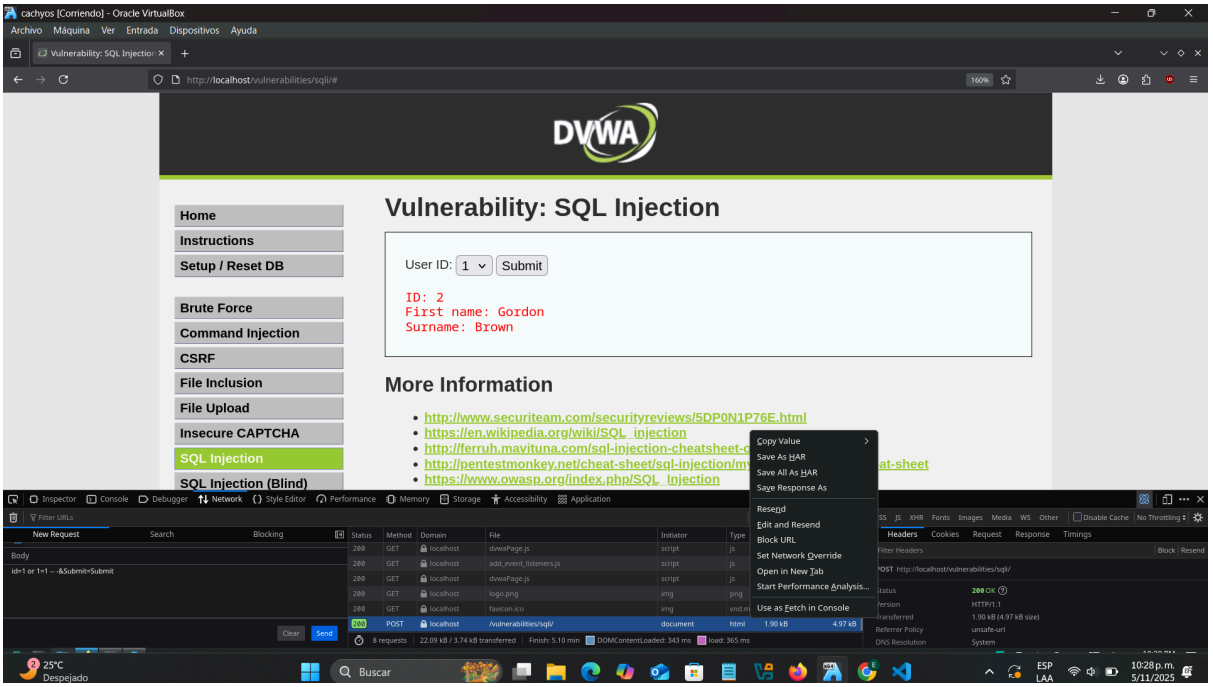
como podemos ver en “body” podemos editar nuestra peticion.



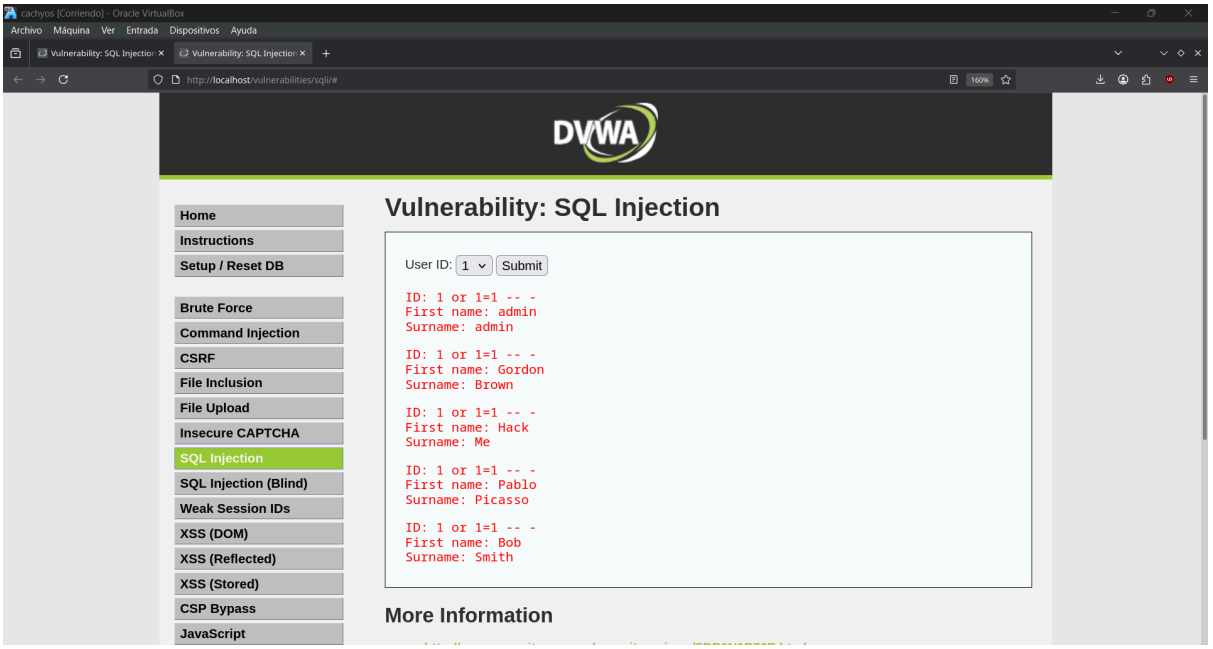
esto para que nos muestre todo lo que contiene la base de datos, dar en “send”.



se nos creó una nueva request, lo que sigue es abrir esa nueva request en una nueva pestaña para poder ver los cambios aplicados.



open in new tab



asi nos mostrará todos los usuarios de esa tabla.