Actividad 4

Abish Abril Santana García

Desarrollo full stack

Universidad Tecmilenio

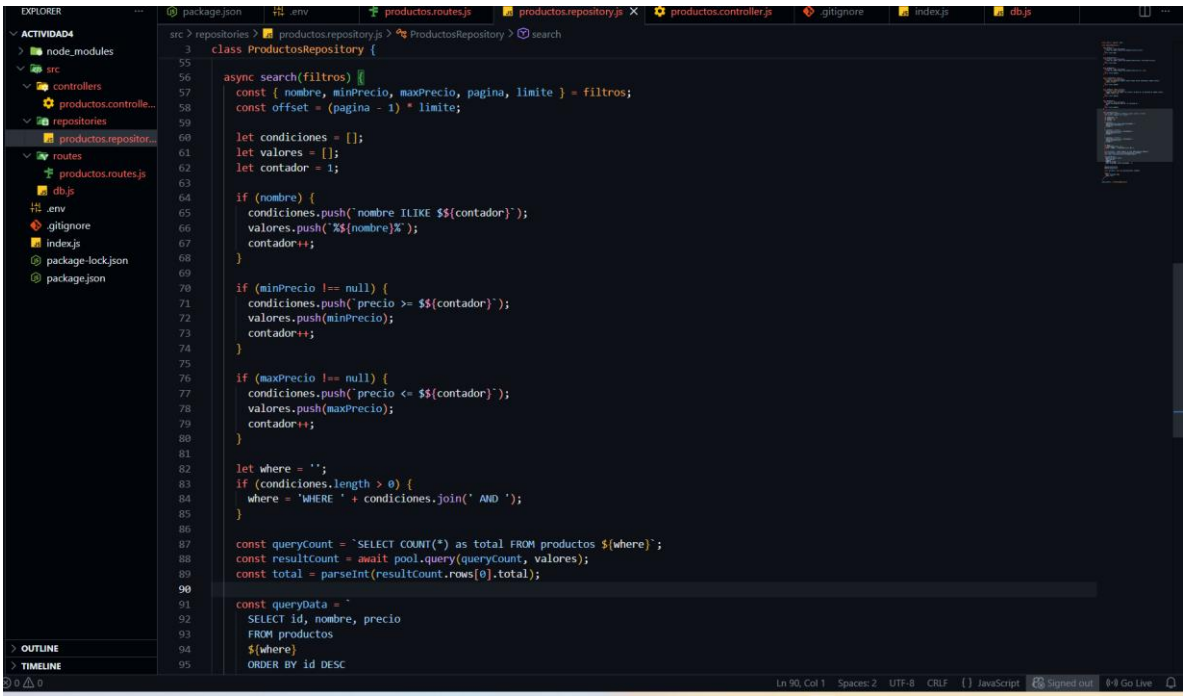
Cómo construiste la query dinámica

En mi archivo productos.repository.js, dentro de la función search:

- Primero, creé un array que se llama condiciones. Ahí voy guardando cada filtro que el usuario pide en la url.
- Segundo, creé otro array que se llama valores. Aquí guardo los datos reales que el usuario escribió.
- Tercero, usé un contador que empieza en 1 y va aumentando cada vez que agrego un filtro.
- Cuarto, al final reviso si hay algo en condiciones. Si tiene, las junto con AND para formar el WHERE. Si no hay filtros, no pongo WHERE.

1. Para la paginación, recibo page y limit, calculo OFFSET y los uso en la consulta.

Así mi consulta funciona con cualquier combinación de filtros que el usuario quiera usar.



Cómo evitaste SQL Injection

En mi archivo productos.repository.js, dentro de la función search:

• Primero, nunca concatené los datos directamente en la consulta.

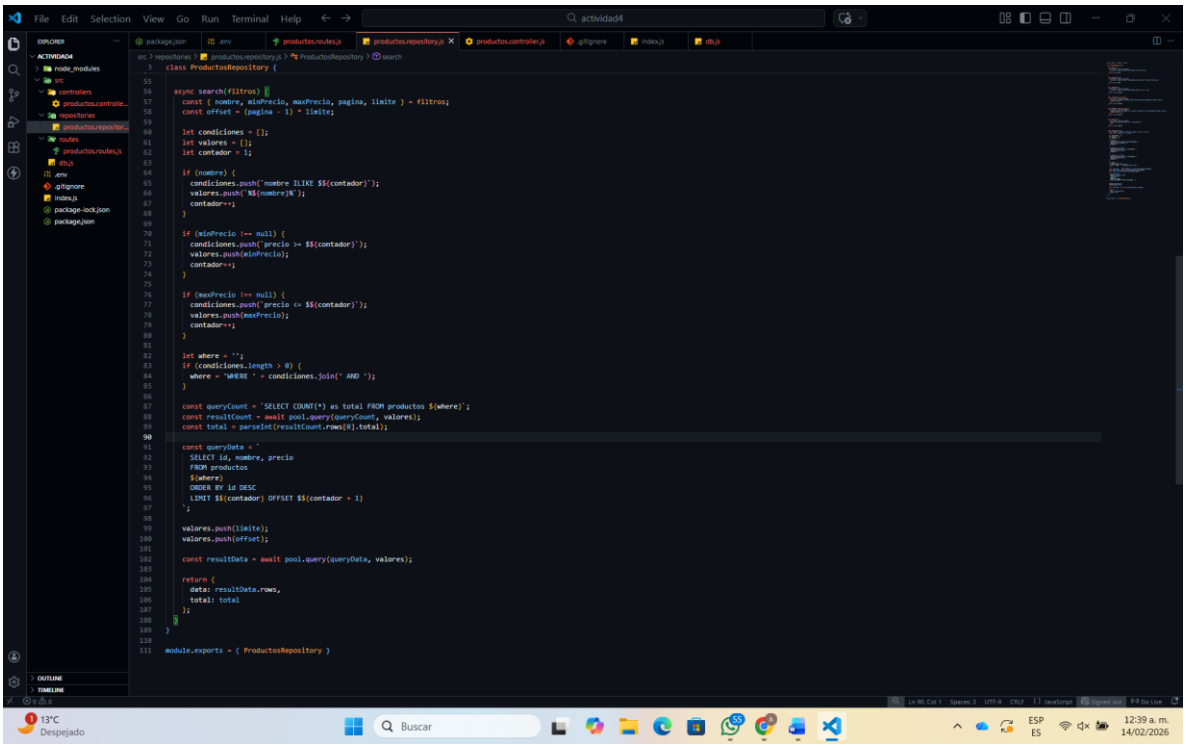
• Segundo, utilicé los parámetros $1 para recibir valores de forma segura. Por ejemplo, en lugar de pegar el texto, escribo "WHERE nombre ILIKE $1".

• Tercero, todos los datos que el usuario escribe los guardé en el array valores. Así la consulta queda limpia y los datos van aparte.

• Cuarto, la librería pg que usamos para conectar con la base de datos se encarga automáticamente de escapar cualquier carácter especial.

• Quinto, en mi controlador también validé que page y limit sean números antes de usarlos.

De esta forma, aunque alguien intente meter código malicioso en la búsqueda, la base de datos lo interpreta solo como texto normal y no como parte de la consulta.



Link de postman https://documenter.getpostman.com/view/51907016/2sBXcBnheh