Laboratorio 17

Imanol Muñiz Ramirez A0170713

*Comentario: Este laboratorio lo implementé en mi proyecto. Los archivos que subo son mi controlador, modelo y cómo hago la conexión con la base de datos para su manejo. En el modelo se muestran como aplico el CRUD.*

¿Qué ventajas tiene escribir el código SQL únicamente en la capa del modelo?

La primera es que mantienes un orden que te permite identificar tanto dónde escribir tú código cómo poder rastrear el flujo de información para rastrear errores. Por ejemplo, de esta forma, si obtenemos un error sobre un query mal escrito, podemos instantáneamente saber en qué archivo está el error.

Por otra parte también nos posibilita poder acceder a las funciones que hacen el CRUD desde distintos controladores lo cual es útil para mantener los archivos y ahorrar líneas de código.

¿Qué es SQL injection y cómo se puede prevenir?

Es una vulnerabilidad de las aplicaciones web que consiste en manipular consultas de la base de datos mediante la inserción de código SQL con el propósito de sustraer información confidencial, controlar la base de datos o dañarla.

Para prevenir estos ataques podemos hacer que nuestras entradas solo permitas ciertos caracteres o valores específicos, evitar construir consultas de SQL concatenando cadenas de texto como valores de entrada, escapar los caracteres especiales y controlar los privilegios de los usuarios.