* ¿Por qué es una buena práctica separar el modelo del controlador?

Para repartir la responsabilidad, y separar la información ingresada para validarla antes de que entre a la base de datos y evitar que pueda dañar o corromper la integridad de la base de datos.

* ¿Qué es SQL injection y cómo se puede prevenir?

Es cuando utilizando los inputs se ingresan palabras clave que afectan el funcionamiento interno del sistema. En php se puede prevenir usando el htmlspecial characters para validar que la información ingresada es únicamente en html entities.