06-Seguridad y Autenticación

Consignas para el Proyecto e-Commerce:

1. Hashear las contraseñas

Las contraseñas de los usuarios no deben almacenarse en texto plano por motivos de seguridad. Implementa un sistema de hashing usando una biblioteca como bcrypt. El objetivo es que las contraseñas sean irreversibles, es decir, que una vez convertidas a un hash, no puedan revertirse al valor original. Asegúrate de aplicar un "salting" para mejorar la seguridad del hash.

2. Implementar un método de autenticación

Desarrolla un sistema de autenticación para que los usuarios puedan iniciar sesión de forma segura. Usa JSON Web Tokens (JWT) o sesiones. Cuando un usuario intente acceder, verifica sus credenciales (email y contraseña). Si coinciden, genera un token que será enviado al cliente para validar futuras solicitudes. No olvides incluir la validación de los tokens en cada ruta protegida.

3. Implementar un método de autorización

Crea un mecanismo para controlar qué acciones puede realizar cada usuario dependiendo de su rol (admin, cliente, etc.). Usa middlewares para verificar que los usuarios tengan permisos adecuados antes de acceder a rutas sensibles (por ejemplo, solo un administrador debería poder eliminar productos). La autorización debe basarse en los roles asignados y estar bien integrada con el sistema de autenticación.

4. Asegúrate de manejar los errores

Es fundamental que tu sistema maneje correctamente todos los errores que puedan surgir, tanto del lado del cliente como del servidor. Crea middlewares que gestionen errores de autenticación, autorizaciones fallidas, y fallos en las operaciones con la base de datos. El usuario debe recibir mensajes claros y no técnicos sobre lo que salió mal.

5. Subir el proyecto a GitHub

Una vez completadas las implementaciones, asegúrate de subir tu proyecto a GitHub. Incluye un archivo README.md explicando las funcionalidades, instrucciones para ejecutar el proyecto y cualquier configuración adicional que el usuario deba conocer. No olvides agregar un archivo .gitignore para evitar que subas archivos sensibles como las contraseñas del entorno o los tokens privados.