Universidad autónoma de Sinaloa

Lic. en informática

Desarrollo web del lado del servidor

Docente: José Manuel Cazarez Alderete

Alumno: Sauceda Soto Jesús Alonso

Actividad en línea Modelos

La seguridad implementada en la API con JWT y bcrypt permite que solo usuarios autenticados accedan a las rutas protegidas. Se añade un nuevo modelo Usuario para almacenar nombres de usuario y contraseñas que son automáticamente hasheadas con bcrypt antes de guardarse en la base de datos. Se crean dos nuevas rutas: /registro para que los usuarios creen una cuenta (validando unicidad de nombre de usuario) y /login para que los usuarios existentes inicien sesión proporcionando su nombre de usuario y contraseña. Al iniciar sesión exitosamente, se compara la contraseña proporcionada con el hash almacenado y si coincide, se genera un JSON Web Token (JWT) que contiene el ID y nombre de usuario del usuario, este token expira en una hora y se envía de vuelta al cliente. Luego, un middleware de autenticación llamado authenticateJWT intercepta las solicitudes a rutas protegidas verificando la presencia y validez de este token en el encabezado Authorization (en formato Bearer TOKEN). Si el token es válido, la solicitud procede a la ruta solicitada; de lo contrario, se deniega el acceso con errores 401 (no autorizado) o 403 (prohibido). Este sistema protege las rutas CRUD de Clientes y puede extenderse a otros modelos como Proveedores Artículos y Empleados garantizando que solo usuarios con un token válido puedan realizar operaciones.