Todo Management System

JWT Authentication with EJS

Project Overview

This project is a beginner-level backend application built using MERN stack principles. It focuses on Node.js, Express.js, and MongoDB for backend development, while EJS is used for server-side rendering. JWT is implemented to provide secure authentication and authorization.

Objectives

- Implement secure JWT-based authentication
- Develop CRUD functionality for todo management
- Follow professional backend architecture standards

Technology Stack

- Node.js
- Express.js
- MongoDB
- EJS
- JSON Web Tokens (JWT)

Core Features

- User registration and login
- Secure route protection using JWT
- Create, view, update, and delete todos
- User-specific todo access

Authentication Endpoints

POST /auth/register – Register a new user
POST /auth/login – Authenticate user and issue JWT
GET/POST /auth/logout – Logout authenticated user

Todo Endpoints

GET /todos – Retrieve all user todos
POST /todos – Create a new todo
GET /todos/:id – Retrieve a single todo
PUT/POST /todos/:id – Update a todo
DELETE/POST /todos/:id – Delete a todo

Security Considerations

- Password hashing before storage
- JWT expiration handling
- Middleware-based route protection

Deliverables

- Fully functional backend application
- Secure authentication system
- EJS-based server-rendered interface
- Clean and professional project structure