Final Project - Production Web Application

Week 10

Objective

By the end of the Final Project, students should be able to:
• demonstrate a complete, production-ready web application
• apply backend and security concepts covered during the course
• implement authentication, authorization, and roles
• secure API endpoints and user data
• clearly explain architectural and security decisions

How to relate this project to previous assignments

The Final Project builds directly on Assignment 4.

The same project must be used. Creating a new project is NOT allowed.

By this stage, the project should already:
• be deployed
• have a working Web UI
• support CRUD operations
• use authentication and sessions

The goal of the Final Project is to finalize and secure the existing application.

Technical Requirements

1. Project base
• Node.js + Express backend
• MongoDB database
• Modular project structure (routes, controllers, models, middleware, config)
• Same project from Assignment 4

2. Database logic & domain data
• Minimum of TWO related collections
• Realistic domain-based data (not generic entities)
• Logical relations between entities

• Correct data handling for large datasets (pagination)

3. Authentication
• Authentication implemented using sessions or JWT
• Login and logout functionality
• Password hashing using bcrypt

4. Authorization & roles
• At least TWO roles: user and admin
• Role-based access control implemented via middleware
• Users can modify only their own data
• Admin has extended permissions

5. API endpoint security
• All write endpoints are protected
• No public update or delete operations
• Safe error handling and validation

6. Deployment & environment setup
• Application deployed with public URL
• Environment variables used for secrets
• No hardcoded secrets in the codebase

Defense

During the defense, the student must:
• Open the deployed public URL
• Demonstrate CRUD via Web UI
• Demonstrate authentication and authorization
• Show role differences (user vs admin)
• Explain database design and security decisions
• Answer questions from Weeks 1–10

Grading Criteria (100%)

Category	Description	Weight
Core Functionality & UI CRUD	Stable UI CRUD and user flows	10%
Authentication + bcrypt	Login/logout and password security	10%
Authorization (Owner access)	Users modify only their own data	10%
Role-Based Access Control	Admin vs user permissions	10%
Database Logic & Domain Data	Relations, real data, pagination/filtering	15%
API Endpoint Security	Protected endpoints and validation	10%
Deployment & Environment Setup	Public URL and env variables	5%
Defense	Demo and explanation	30%