Extension Tasks

1. Authentication and Authorization

- Add persistence for users and roles (tables or reuse existing) with unique email constraint.
- Store passwords as hashed + salted values (no plaintext).
- Implement endpoint POST **/api/auth/register** to create a user.
- Implement endpoint POST **/api/auth/login** to return a JWT access token containing user role/claims.
- Implement endpoint POST **/api/auth/change-password** for authenticated users.
- Enforce token expiry and deny access with expired/invalid tokens.
- Define roles: at minimum **Admin, Doctor, Receptionist**.
- Create authorization policies (**e.g., RequireAdmin, RequireDoctorOrAdmin, RequireReceptionistOrAdmin**).
- Protect endpoints using [Authorize] + policies
- Return **401** for unauthenticated and **403** for unauthorized requests.

2. Middlewares

- Implement Exception Handling Middleware that returns JSON ProblemDetails (type, title, status, traceId, optional detail).
- Implement Request Logging + Timing Middleware that records method, path, user (if any), status code, and elapsed ms.

3. Validation (FluentValidation) & Filters:

- Add FluentValidation validators for DTOs used by your endpoints
- Create a Validation Filter that returns 400 with a unified error payload when validation fails.

4. Logging:

- Use Serilog to log error response that are being caught by your exception handling middleware and your general logs on a text file.

NOTE: Deadline of this assignment is **Monday 18th of August, 2025 (Before 10.30 am)**
