**Giáo Án Tuần 4: Authentication & Authorization với JWT**

📌 **Mục tiêu**:

* Hiểu và triển khai **JWT Authentication trong ASP.NET Core**
* Thực hiện **đăng ký, đăng nhập, xác thực người dùng**
* Phân quyền API theo **Role-Based Authorization**

**Buổi 1: Giới Thiệu Authentication & JWT**

⏱ **Thời lượng**: 2h  
🔹 **Nội dung**:

1. **Authentication & Authorization là gì?**
   * Authentication (Xác thực) vs Authorization (Phân quyền)
   * Các phương thức Authentication phổ biến (Cookie, JWT, OAuth)
2. **Tại sao dùng JWT?**
   * Cấu trúc JWT: **Header, Payload, Signature**
   * Cách hoạt động của JWT trong API
3. **Cài đặt JWT Authentication trong ASP.NET Core**
   * Cấu hình JwtBearerAuthentication
   * Tạo secret key & signing credentials
   * Middleware xử lý JWT

🔹 **Thực hành**:

* Cài đặt **Microsoft.AspNetCore.Authentication.JwtBearer**
* Cấu hình JWT trong Program.cs

**Buổi 2: Xây Dựng API Đăng Nhập & Đăng Ký**

⏱ **Thời lượng**: 2h  
🔹 **Nội dung**:

1. **Tạo API Đăng Ký Người Dùng**
   * Cấu trúc **User Entity**
   * Lưu trữ mật khẩu với **Password Hashing**
   * Thêm User vào **Database**
2. **Tạo API Đăng Nhập và Phát JWT**
   * Kiểm tra thông tin đăng nhập
   * Tạo JWT Token với Claims
   * Trả token về client

🔹 **Thực hành**:

* Tạo API POST /register và POST /login
* Kiểm tra đăng nhập và nhận token

**Buổi 3: Role-Based Authorization & Claims**

⏱ **Thời lượng**: 2h  
🔹 **Nội dung**:

1. **Thêm Role cho User & Phân quyền API**
   * Định nghĩa **UserRoles** (Admin, User)
   * Thêm Claims vào JWT
   * Middleware kiểm tra **[Authorize] với Role**
2. **Sử dụng Authorization Policy trong ASP.NET Core**
   * Cấu hình AddAuthorization()
   * Tạo Custom Policy

🔹 **Thực hành**:

* Chỉnh sửa API để chỉ Admin có thể **thêm/xóa sản phẩm**
* Chỉ User có thể **mua hàng**

**Buổi 4: Bảo Mật API & Refresh Token**

⏱ **Thời lượng**: 2h  
🔹 **Nội dung**:

1. **Bảo mật API bằng Refresh Token**
   * Hạn chế **JWT Expired sớm**
   * Cấu trúc **Access Token + Refresh Token**
   * Tạo API **làm mới Access Token**
2. **Triển khai Middleware Custom JWT Authentication**
   * Kiểm tra JWT hợp lệ
   * Chặn request nếu không có token

🔹 **Thực hành**:

* Cài đặt **Refresh Token**
* Viết Middleware kiểm tra JWT

**Bài Tập Cuối Tuần 4**

✅ **Yêu cầu**: Xây dựng API **quản lý người dùng với JWT Authentication**  
✅ **Các tính năng yêu cầu**:

* Đăng ký, đăng nhập **(User, Admin)**
* Phân quyền API (Admin, User)
* Middleware kiểm tra JWT
* Hỗ trợ **Refresh Token**