Objective:

Learn about how to setup authorization in ASP.NET Core. Learn what a JWT token is and how to setup Bearer scheme authorization in ASP.NET Core.

Theory:

- https://docs.microsoft.com/en-us/aspnet/core/security/authentication/?view=aspnetcore-6.0
- https://docs.microsoft.com/en-us/aspnet/core/security/authorization/introduction?view=aspnetcore-6.0
- https://codepedia.info/jwt-authentication-in-aspnet-core-web-api-token
- https://docs.microsoft.com/en-us/aspnet/identity/overview/getting-started/introduction-to-aspnet-identity

Task:

Deadline: 4-5 days

Requirements:

- Learn about how authorization is configured in ASP.NET Core.
- Learn about JWT token
- Implement JWT authorization in our web application. Authorization is simple, 2 roles: admin and customer. Authorization is based on email and password.
- Decorate all controllers/endpoints with authorize attribute.
- For login and registration create a simple html view with a couple of inputs to submit data. Technologies are up to you.

Answer all of these questions to be prepared:

1. What is authentication and authorization?
2. What is JWT token, what are the main components of this token?
3. Explain JWT flow

a. What access and refresh tokens are responsible for?
b. Can a server have only access tokens without refresh ones? If yes what’s pros and cons of such solution
c. What pros and cons of storing access/refresh tokens in a database compared to not storing it?
d. How does a modern web application understand a client is unauthorized?