Защита методов WebAPI

Для разграничения доступа будем использовать JSON Web Token(JWT) – токен создается сервером и подписываются секретным ключем и передаются пользователю, который в дальнейшем использует данный токен для подтверждения личности.

Для работы с JWT нужен пакет JWTBearer, если проект .NET 8, то и версию у скачиваемого пакета должна быть 8.

Создали класс сервис TokenService, где выполняется генерация

Для того, чтобы в нем была доступна конфигурация он добавляется в Programm.cs (builder.Services.AddScoped<TokenService, TokenService>();), а в классе добавляем поле

Конфигурация создается в appsettings.json

"JWT": {

"Key": "1111111111111111111111111111111111111111111111111111111111111111", - любой ключ, размер зависит от алгоритма шифрования

"Issuer": "http://localhost:5098",

"Audience": "http://localhost:5098"

}

JWT:

builder.Services.AddAuthentication(JwtBearerDefaults.AuthenticationScheme)

.AddJwtBearer(options =>

options.TokenValidationParameters = new()

{

ValidateIssuer = false, // true

//ValidIssuer = "http://localhost:5098", // кто издатель, например сервер builder.Configuration["JWT:Issuer"]

ValidateAudience = false, // true

//ValidAudience = "http://localhost:5098", // кто ползователь, где применяется токен builder.Configuration["JWT:Audience"]

ValidateLifetime = true,

ValidateIssuerSigningKey = true,

IssuerSigningKey = new SymmetricSecurityKey(Encoding.UTF8.GetBytes(builder.Configuration["JWT:Key"]))

}

);

Информацию можно посмотреть декодировав JWT

Для запрета доступа к классу или методу, можно добавить атрибут [Authorize]