Secure ASP NET API with JWT Authentication

* **كل request رايح لأي endpoint عندي بال Api لازم يكون معها ال credentials تبعها ضمن ال header اللي على أساسها بتعامل مع ال request سواء بدو authentication أو allow ananyms**
* **ماهو ال JWT Json Web Token Authentication ؟**

**هو ببساطة عبارة عن token بستخدمه مشان أعمل secure لل api تبعي**

من أشهر ال techniques المستخدمة في apis secure (في معظم ال frameworks وليس فقط مع الدوت نت)

ال token يكون مقسم الى **ثلاثة أقسام** كالتالي:

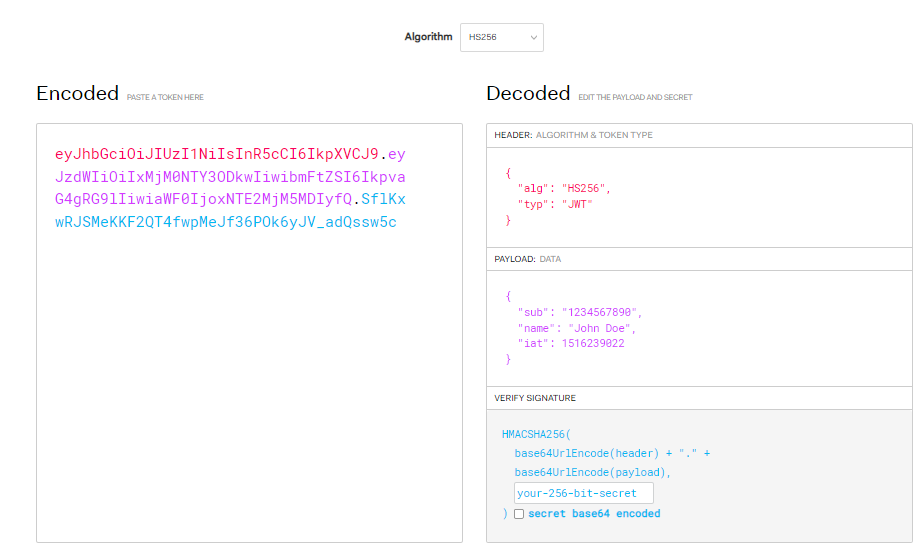
1. Header:

فيه معلومات عن ال algorithm المستخدم بال hashing

1. Payload:

فيه المعلومات تبعك اللي عم تبعتها مع ال token مثل ال (username, email, roles, token expiration date أو أي داتا بدك ياها)

1. VERIFY SIGNATURE



# Prepare JWT Configuration

* طبعا شغلي رح يكون على مشروع من نوع web api وبعدين رح نزل الباكيجات التالية:

Install Needed Packages as below:

Microsoft.AspNetCore.Authentication.JwtBearer

Microsoft.AspNetCore.Identity.EntityFrameworkCore

System.IdentityModel.Tokens.Jwt

Microsoft.EntityFrameworkCore

Microsoft.EntityFrameworkCore.Design

Microsoft.EntityFrameworkCore.SqlServer

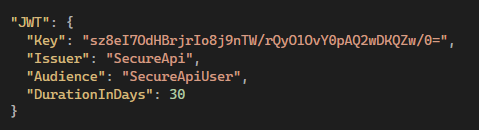
Microsoft.EntityFrameworkCore.Tools

Microsoft.VisualStudio.Web.CodeGeneration.Design

* هلق بدنا نزبط ال configuration كالتالي:

1. appsettings.json:

وضع ال key تبع ال jwt بالإضافة الى معلومات اخرى ضمن ال كالتالي:



* Key:

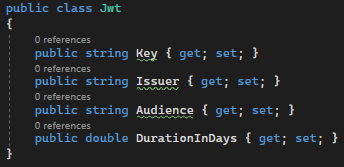
المستخدم في عملية ال encryption مع ال jwt token وطبعا هو لازم يكون secure جدا وماحدا عنده access عليه (ممكن تخزنه بمكان اخر)

* DurationInDays:

المدة اللي رح يكون ال token expired بعدها وهاد الوقت بيختلف من application الى اخر (مثلا ممكن تكون الداتا جدا sensitive فبتخليه expire each half hour)

1. Helpers -> Create Jwt Class:

* فيه نفس المعلومات ضمن ال appsettings.json



1. Program.cs

* بدي أعمل mapping بين المعلومات ضمن ال appsettings والكلاس jwt كالتالي:



# Create Database and Identity Tables + Seeding Roles

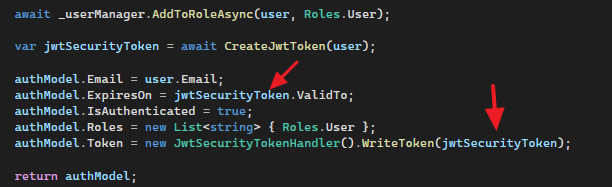
مافي شي مهم كله منعرفه من كورس User Management With Identity وأنشأ Admin + User Roles

# Add JWT Configuration And Add Auth Service

Register

1. Services -> IAuthService + AuthService

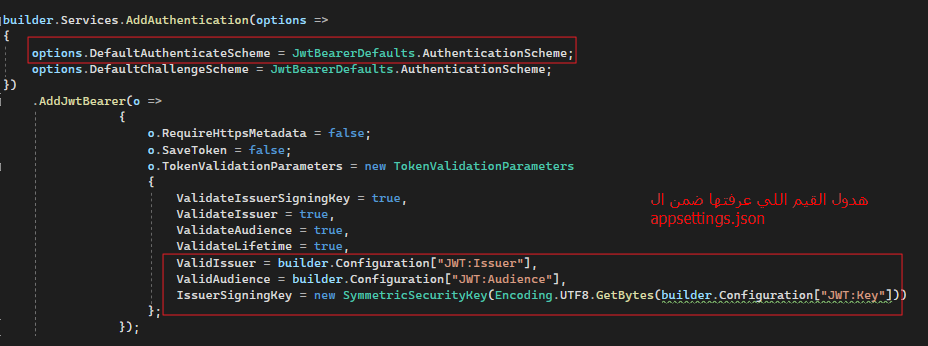
* رح نضيف service اللي رح تكون مسؤولة عن عمليات ال Register, Login,…. (بنفس الطريقة اللي منعرفها ) سهلة جدا وبسند للمستخدم الجديد User role by default
* الفكرة الرئيسية هي بعد اتمام عملية ال Register بنجاح بدي رجع ال Token ومعلومات إضافية لل
* endUser
* قام بإستخدام ميثود جاهز CreateJwtToken وشرحه سريعا ضمن الدرس التالي:



<https://www.youtube.com/watch?v=PXKrGK4zjuM&list=PL62tSREI9C-eYNE1Pyw0yv1tETs5V8WGd&index=7&ab_channel=DevCreed>

1. الان بسجلها ضمن ال programs.cs

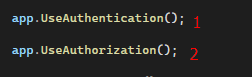
* اضافة ال Jwt Configuration كالتالي:



* حددتله ال default schema الخاصة بال Jwt وهي ال **Bearer** مشان ماحطها عند كل controller (خلص بعرفها مرة واحدة وبمجرد ماحطله Authorize فقط لحاله بيفهم) كالتالي:

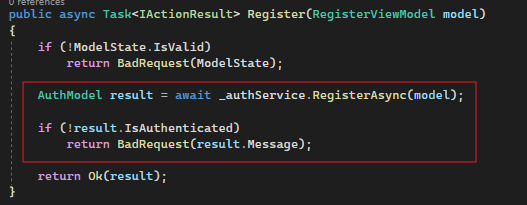


* لازم تنتبه لشغلة انك لازم تضيف ال UseAuthentication() قبل ال UseAuthorization() كالتالي:

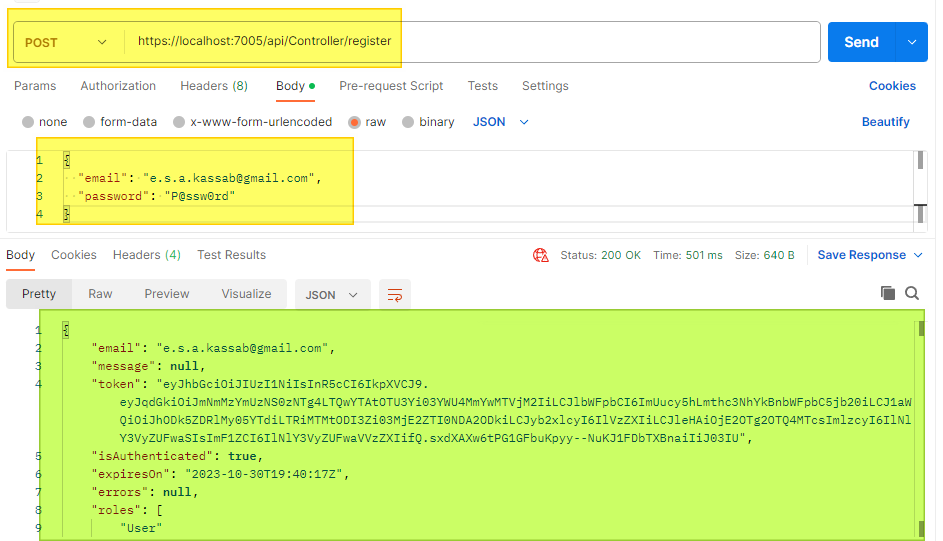


1. Controllers -> AuthController:

* طبعا رح يكون Allow anonymous كالتالي:

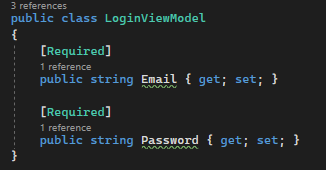


1. وهيك منكون خالصين وبعد ال Register بنجاح منلاحظ أنه رجعلنا ال Token وكامل المعلومات الأخرى بشكل صحيح كالتالي:



Login

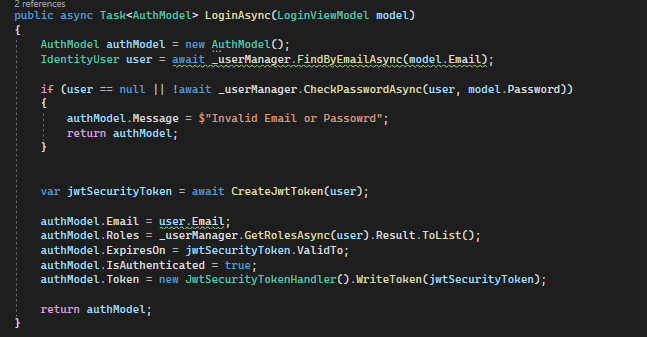
1. ViewModels -> LoginViewModel



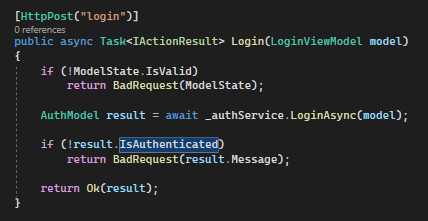
1. IAuthService:



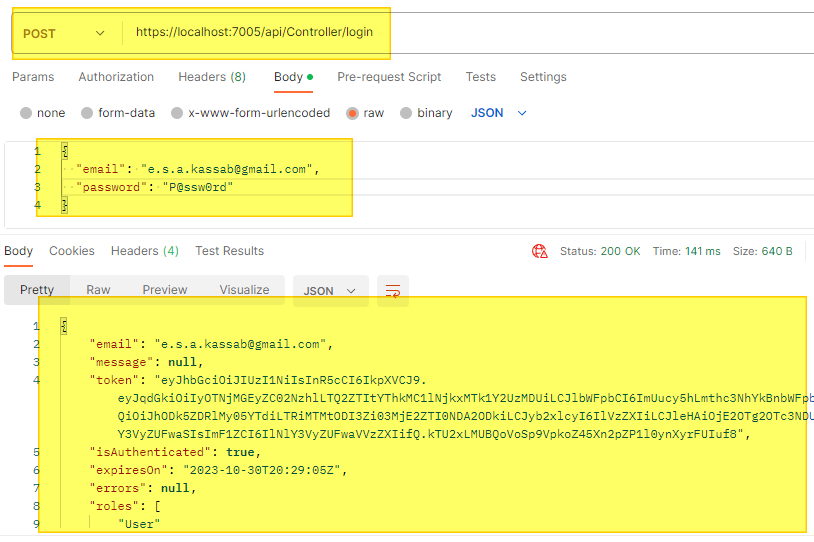
1. AuthService



1. AuthController:

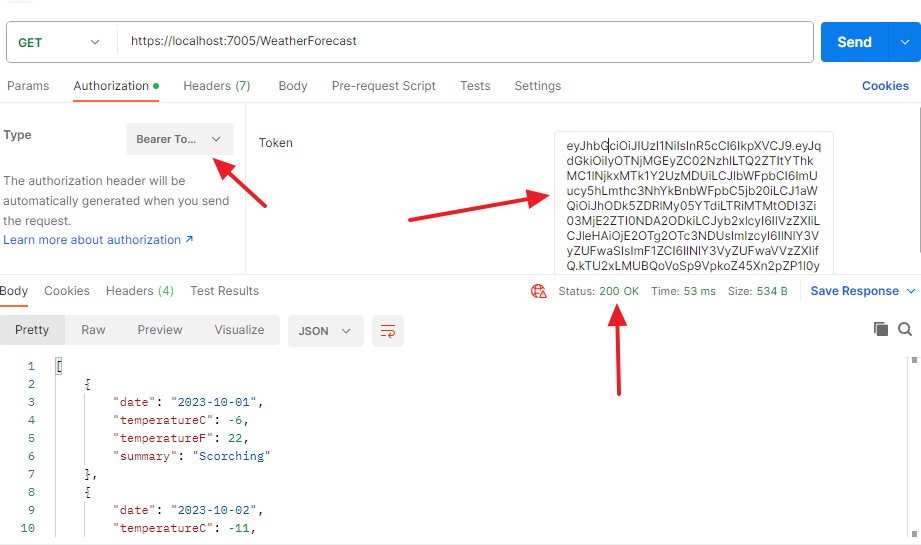


1. وهيك منكون خالصين كالتالي:



# Protect Your Endpoints

* بعد ماخلصت هلق بدي روح أعمل Authorize على ال endpoints تبعي أو على كامل ال controller وهاد الشي بيتحدد من خلال ال business تبعي
* رح جرب على ال WeatherForecastController (في حال ما ارسلت ال token مع ال request تبعي رح يرجعلي Status 401Unauthorized ) كالتالي:



* ملاحظة في حال بدي كانت ال Role=Admin وبعتت بمستخدم User عادي رح يرجع 403 Forbidden

401 Unauthorized

403 Unauthenticated

تم بفضل الله وحمده

Reference:

<https://www.youtube.com/playlist?list=PL62tSREI9C-eYNE1Pyw0yv1tETs5V8WGd>