MB

################################################################

Securing ASP.NET Core 3 with OAuth2 and OpenID Connect

----------------------------------

ابتدينا الشغل النضيف شغل الويب API بقه و جماله بيقولك عشان اخلى كل الريكويستات محميه و كده ففى طريقه لعمل الكلام ده و هو انى اخلى المستخدم عشان يقدر يعمل ريكويست للسيرفيس انه يحصله فحص و يتشاف اذا كان ده مستخدم ليه تصريح عمل الخدمه دى ولا لأ لو ليه يدخل يعملها عادى و لو ملوش ميخش يعملها فعلى سبيل المثال انا شخص مسجل فى موقع و فى شخص تانى مش مسجل فى الموقع ففى وظايف معينه هتلاقيها بتشتغل معايا عشان انا شخص مسجل دخول فى الموقع و الوظايف دى بتشتغلش مع ناس تانيه و ده لانهم مش مسجلين دخول   
طيب ايه الى يفرق بين ان البنى اد الى داخل يعمل الخدمه دى ليه تصريح او ملوش ؟؟

الى يفرق بينهم انه لو مبعوت مع السيرفيس دى username/password يبقى كده الراجل ده مسجل دخول و يخش يعمل الوظيفه عادى

طب دلوقتى منا كده انا مضطر ابعت فى كل ريكويست ال username/password طب ده كده انا هبعتهم كتير اوى و كده مش حاجه حلوه خالص ده ممكن هاكر ملوش لازمه يعرف يجيبهم من اى ريكويست و اتبهدل انا   
فقالك طب الحل ايه ؟؟

الحل انى اعمل Token التوكين ده يبقى شايل بينات المستخدم فيه و بيبقى متشفر فكده هيبقى موجود معايا فى كل الموقع و ببعته فى كل الريكويست بس كده بقه متشفر ياباشا محدش يعرف يفك شفرته بالتالى كده ذى العسل الدنيا اصبحت دلوقتى ان بيناتات المستخدم هتتعان فى token متشفر و فى الباك اند وقت ما هحتاج بيانات المستخدم عشان يعرف يعمل سيرفيس معينه هروح باعته ال Token و بالتالى كده خلاص هو هيشوف التوكين جاى و فيه البيانات الى انا عوزاها هيروح مشغل السيرفيس عادى و لو ملقاش التوكين او كان فى بيانات غلط فى التوكين هيقفل السيرفيس و مش هيشغلها و كان التوكين اصبح مفتاح اخش بيه للسيرفيسيس المقفوله

MB

################################################################

OAuth2

-------------------

دى طريقه فى السيكيورتى بتسمح بحمايه الداتا و السيرفيس بحيث ان اى سيرفيس هقوم بيها داخل المشروع تبقى محتاجه عشان تشتغل اليوزر و الباسورد على هيئه توكين متخزن فى ال localStorage مع كل Login بحيث انه بعج كده و انا داخل على اى سيرفيس انفذها الكود هيشوف هاه الشخص ده بالبيانات الى فى التوكين دى ليه تصريح يخش يعمل السيرفيس ولا ميعملهش لو التوكين قال يعملها يبقى يعملها لو قال ان دى بيانات غلط يبىقى خلاص ميخشش يعمل حاجه و يفضل ذى الكلب لحد ما نشوف مشكلته ايه بالظبط

و نحلها و بعد كده نجرب تانى و نشوف الى هيحصل و بالتالى كده التوكين و ال OAuth2 دى طرق لحمايه الشغل و الخدمات الى فى الموقع من ان اى حد داخل يهبد فيه