Enoca .Net Eğitim Task 3

Konu: Jwt token yapısı ve Jwt ile Authorization

Talimatlar: Jwt kullanarak .NetApi ile birlikte kullanıcı olarak sisteme giriş ve authorization işlemlerini yapmanız beklenmektedir. Sayfa altında belirtilen kaynaklardan yararlanabilirsiniz.

Teknolojiler: Asp.Net web Api, Microsoft.AspNetCore.Authentication.JwtBearer

Yapılması Beklenenler:

1) Temel Jwt yapısının kurulması
2) Farklı bir Controller üzerinde Authorize gerektirerek erişim sağlanması
3) Kurulan Jwt ile Authorization işlemi yapılması
4) Authorize gerektiren controller a erişim sağlanması
5) Appsettings dosyası içerisinde Jwtconfig adında bir alan açılması ve Issuer, Audience, SıgnınKey vb alanlarının Appsettings dosyası üzerinden alınması

Ön Bilgi:

JWT, kullanıcının doğrulanması, web servis güvenliği, bilgi güvenliği gibi birçok konuda kullanılabilen içerisindeki verileri şifrelenmiş bir biçimde tutan ve sadece doğru key değeri ile içerisindeki verilere ulaşılabilen bir web servis güvenlik aracıdır. Jwt 3 kısımdan oluşur bunlar;

Header:

Header içerisinde şifreleme algoritmasını ve imzalama için kullanılan algoritmayı tutar.

Payload:

Bu kısım claimleri içerir. Bu kısımda tutulan veriler ile token istemci ve sunucu arasında eşsiz olur. Bu tutulan claim bilgileri de bu eşsizliği sağlar. Bu kısımda 3 tip claim bulunmaktadır.

Registered(Kayıtlı) Claims: JWT tarafından önceden reserve edilmiş 3 harf uzunluğunda claimlerdir. Yani bu ayarlanmış belli claim isimlerini diğer claimlerde kullanamazsınız. Bu bilgilerin kullanılması zorunlu değildir ama önerilmektedir. Bu claimlerden bazıları iss (issuer), exp (expiration time), sub (subject), aud(audience) ve diğerleri. Bunlardan en çok kullanılanı expiration time yani son geçerlilik tarihidir. Örneğin token bilginizin 3 saat sonra geçersiz olmasını isterseniz bu bilgiyi exp alanında gönderirsiniz. 3 saat ardından aynı token ile gelen isteklerde token geçersiz olarak değerlendirilir.

Public (Açık) Claims: İsteğe bağlı, açık yayınlanan claimlerdir.

Private (Gizli) Claims: Tarafların kendi aralarında bilgi taşımak için kullandığı gizli claimlerdir.

Signature:

Bu kısım tokenın son kısmıdır. Bu kısmın oluşturulabilmesi için header, payload ve gizli anahtar(secret) gereklidir. İmza kısmı ile veri bütünlüğü garanti altına alınır. Burada kullandığımız gizli anahtar Header kısmında belirttiğimiz algoritma için kullanılır. Header ve Payload kısımları bu gizli anahtar ile imzalanır.

Enoca .Net Eğitim Task 3

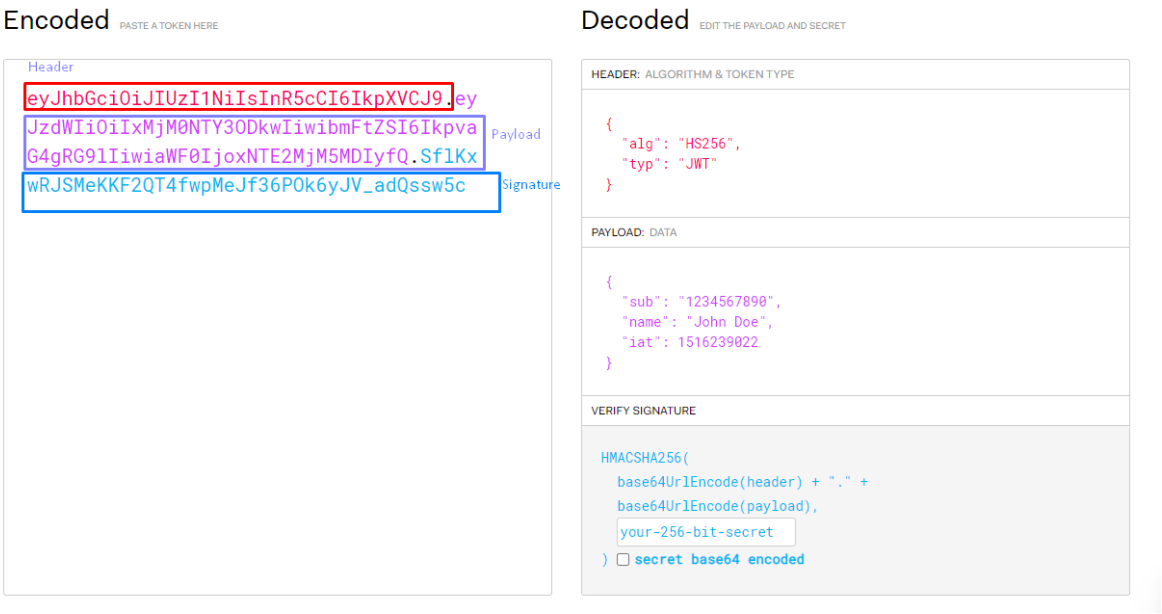

Figure 1Örnek Jwt Token yapısı

Kaynaklar:

https://www.youtube.com/watch?v=062BBfvMB7s

https://www.youtube.com/watch?v=r0OwsLVjKd4

https://www.youtube.com/watch?v=v7q3pEK1EA0

https://www.youtube.com/watch?v=TDY_DtTEkes

https://devnot.com/2017/json-web-token-jwt-standardi/

https://www.gencayyildiz.com/blog/asp-net-mvc-web-api-token-authentication/

https://www.gencayyildiz.com/blog/asp-net-core-angular-7-web-api-token-authentication-kullanimi/