

Enoca .Net Eğitim Task 4

Konu:

ASP.NET Core ile Rate Limit özelliği ekleyerek API güvencesi sağlama

Talimatlar:

ASP .NET Core kullanarak bir API'ye rate limit eklenilmesinin öğrenilmesi hedeflenmektedir. Proje kapsamında birkaç API endpointi oluşturulacak ve bu endpointlere rate limit özelliği eklenerek API'nin güvenliği sağlanacaktır.

Teknolojiler:

Asp.Net web API, **Rate Limit**

Yapılması Beklenenler :

1. ASP.NET Core Web API projesi oluşturma.
2. Proje içinde en az 2 farklı API endpointi oluşturulacaktır. Bu endpointlerin her biri farklı bir HTTP metodu (GET, POST, PUT, DELETE vb.) kullanacak şekilde tasarlanmalıdır.
3. ASP.NET Core'daki "Middleware" yapısını kullanarak bir rate limit mekanizması oluşturması gerekmektedir. Bu mekanizma, API endpointlerine belirli bir süre içinde sınırlı sayıda istek gönderilmesini sağlayacak şekilde tasarlanmalıdır.
4. Rate limit mekanizması, kullanıcılara "429 Too Many Requests" hata kodu göndererek aşırı isteklerin önüne geçmelidir.
5. Projenin bir parçası olarak, Swagger (OpenAPI) desteğini de eklemesi gerekmektedir. (Swagger, API endpointlerinin otomatik olarak belgelenmesini sağlayacak ve API'lerini daha kolay bir şekilde test etmelerine olanak tanıyacaktır.)

Ön Bilgi:

Asp.NET Core API ile tasarlanmış bir endpoint'in normal şartlarda sürekli istek alabilecek şekilde tasarlanması kötü niyetli kişiler tarafından kullanılarak *Denial Of Service Attack(DOS Attack)* ve hatta *Distributed Denial Of Service Attack(DDOS Attack)* denilen saldırılarla karşı karşıya kalınmasına sebebiyet verebilir. Kötü niyetli kişiler tarafından dış dünyaya karşı istek hacmi her daim açık olan bir API tespit edildiği takdirde, bir kaç client veya client görevi görecektir tehlikeli(compromised) yazılım eşliğinde ilgili API'ya aralıksız istek göndererek hedef sunucuyu çökertmek veya servisi hizmet veremez hale getirmek amaçlı yapılan saldırı çeşitidir.

Böylece ilgili sunucu hizmetlere karşılık veremeyecek veya gecikmeli çalışacak hale getirildiği takdirde kullanıcılara ya yavaş sonuç dönülecek ya da kullanıcılar tarafından erişilemeyecektir.

İşte böyle bir senaryoyla karşılaşmamak için API'larımıza dış dünyadan gelecek isteklerin sınırını belirtmemiz gerekmektedir. Bunun için **Rate Limit** belirtilerek bu olası saldırıdan rahatça korunulabilir. Rate Limit; uygulamanıza güvenlik ve ölçeklendirilebilirlik getirecektir.

Rate Limit, API uygulamasına belirli bir süre zarfında ne kadar istek yapılabileceğini, hangi IP'lerin bundan muaf tutulabileceğini vs. belirleyebilmekte ve böylece uygulamamızın istek hacmini kontrol etmemizi sağlayabilmektedir.

Yardımcı Kaynaklar:

<https://www.gencayyildiz.com/blog/asp-net-core-rate-limit-ile-api-guvencesi-saglama/>

<https://www.youtube.com/watch?v=TVrKJD9Tg5A>

<https://github.com/stefanprodan/AspNetCoreRateLimit>