# **NOTLAR**

* Failure: İlgili kullanıcının hesabı kitlensin mi kitlenmesin mi? Yani kullanıcı belirli bir sayıda bilgilerini yanlış girerse, belli bir süre hesabı bloklansın.
* Auto Validate Antiforgery Token: Sunucunun üretmediği x bir yerden belirli istekler yapamaz hale gelir. Her yerden istek gelemez.
* Document.cookie diyerek cookieleri çekebiliriz.
* Http Only true olarak setlenmişse eğer document.cookie desek bile cookielere erişim sağlayamayız, onları çekemeyiz. Yani bir tür güvenlik önlemi.
* Same Site eğer lax olarak geçilmişse bu cookie başka sitelerle veya subdomainlerle paylaşılabilir. Eğer strict olarak setlenmişse ilgili cookie sadece ilgili domainden kullanılabilir. Harici bir domainlerden veya subdomainlerden kullanılamaz.
* Cookielerde ilgili kullanıcının rol bilgisi (admin mi?), id bilgisi, username bilgisi buralarda tutulabilir. Bunları özel bir class aracılığıyla (bu classın adı User ve asp.nette olan özel bir class) bu datalara erişilebilir. Bunun için birtakım konfigürasyonlar yapılmalıdır.
* Bu tür yerlerde ya da db leri direk tutmak doğru değil
* Hani staja başlamadan önce cuma günü bir proje vermiştim
* O proje veriyi encrypt decrypt ediyo
* Bu tür veriler, özellikle ortak erişim alanlarındakiler encrypted şekilde tutulursa, herhangi bir zararlı uygulamanın önemli verilere erişimi kısıtlanmış olur
* Sadece giriş yapmış kullanıcıların erişebilmesini istiyorsak Action Result’ ımızın üzerine [Authorize] komutu yazılır. Aynı zamanda yanında başka kısıtlar da verebiliriz.

Örnek;

metin içeren bir resim

Açıklama otomatik olarak oluşturuldu

Burada sadece Authorize diyip bıraksaydık yalnızca giriş yapan kullanıcı sayfayı görebilirdi. Ama yanına verilen roles komutu ile kişinin giriş yapması yetmez aynı zamanda rollerinde Admin veya Member da olmalıdır.