نکته:

در webApi نمی توان از cookie استفاده کرد چون stateless است بلکه باید از token استفاده شود.

Json web token

دارای 3 بخش کلی است.

Header

شامل الگوریتم رمزنگاری توکن و نوع توکن

{

“alg”:”hs256”,

“typ”:”jwt”

}

Payload

محتوای است که می خواهیم برای کاربر ست کنیم شامل claim های کاربر که می توانیم خود payload را هم کد گذاری کنیم.

}

“name”:”ali”,

“id”:2

}

verify signature

کلید مربوط به توکن است که اگر محتوای نوکن تغییر کند این امضا غیر معتبر می شود در واقع حاصل هش دو قسمت قبلی است و در صورت تغییر قسمت محتوا غیر معتبر می شود

فوق العاده امن است

تنظیمات اولیه :

IssuerSigningKey یک رشته می گیرد هر چیزی و آن را به عنوان کلید رمز نگاری در نظر گرفته بهتر است رشته غیر قابل حدس باشد.

ValidIssuer یک رشته می گیرد و مشخص کننده کسی که رشته را ساخته معمولا اسم سایت

ValidAudience یک رشته است که مشحص کننده کسی است که از کلید می خواهد استفاده کند یک رشته دلخواه به آن پاس می دهیم.

ValidateLifeTIme مدت زمان انقضای کلید را چک کن = true

vaidateIssuer = true بررسی کن issuer درست باشد

validateIssuerSignKey = true بررسی کند کلید درست باشد

ValidateAudience = true بررسی کن مقدار audience نیز درست باشد.

این بررسی ها تضمین می دهد که توکن معتبر است و توسط خود سایت ما درست شده است.

