<https://www.dotnettricks.com/learn/angular/token-based-authentication-json-web-token-aspnet-core>

https://www.toptal.com/angular/angular-5-asp-net-core

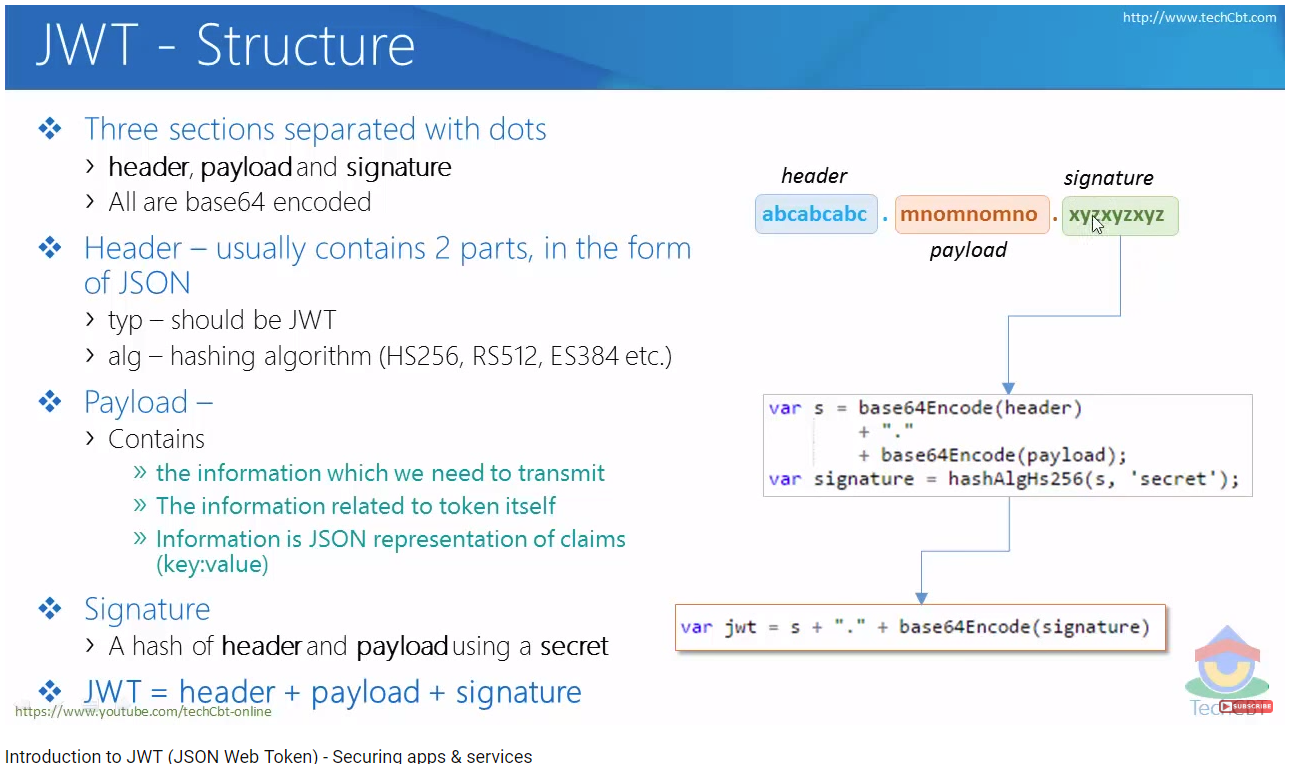
Token-based Authentication in Angular 6 with ASP.NET Core 2.1

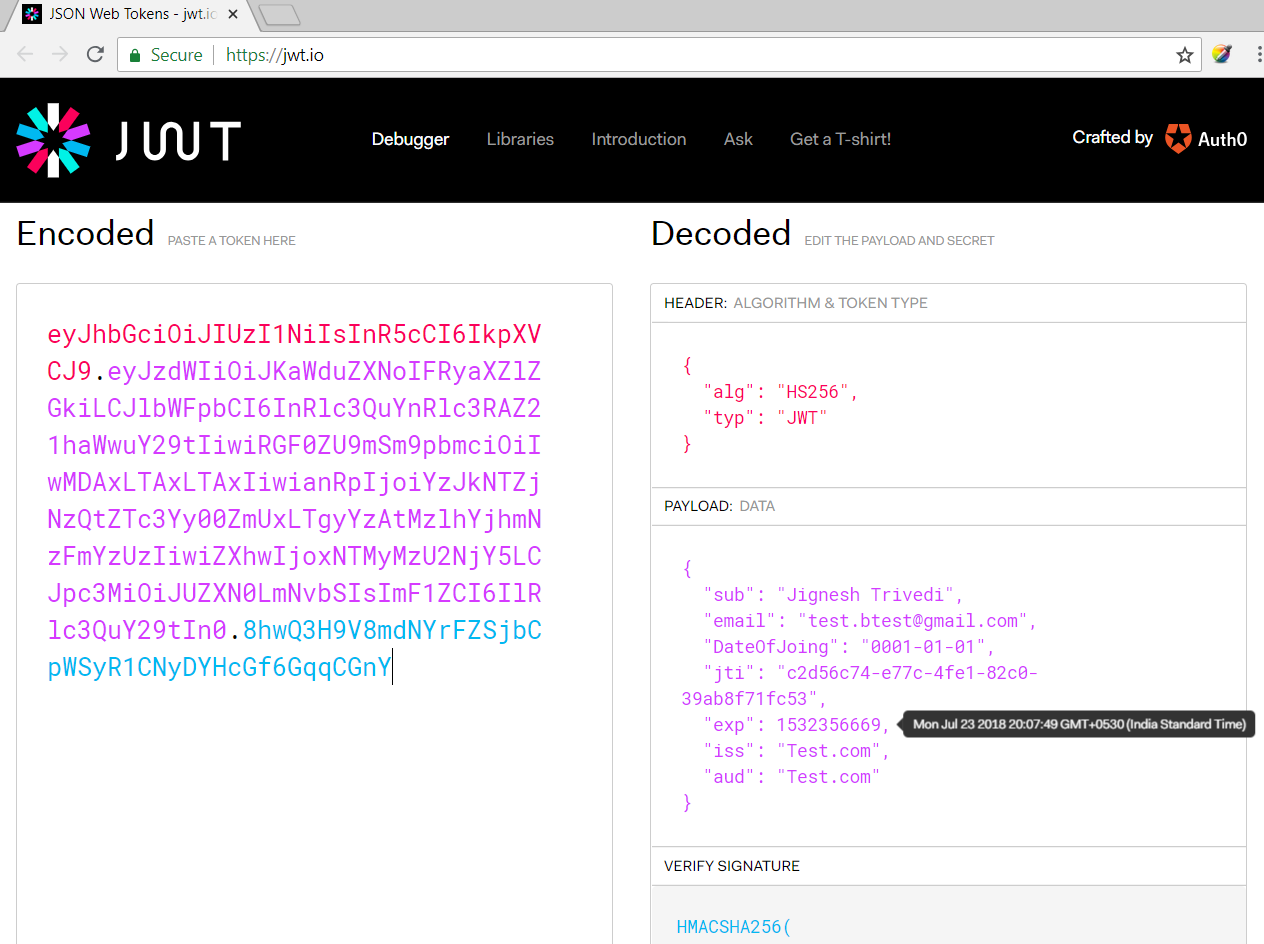
JSON Web Token (JWT) is the most popular and open standard interface that allows communication & data transmitting between parties as JSON. JWT is digitally signed, so the information is trusted and verified.

It consists of three parts: Header, Payload, and Signature; all the parts are separated by the dot (.). It looks like "hhhh.ppppp.sssss" and these parts are Base64Url encoded. The header part of JWT consists of two parts: the hash algorithm that used like RAS or HMAC SHA256, the second part is the type of token (it is always JWT). The Payload part of JWT contains the claims (user information such as Username, email, etc.) and other metadata. The claim can be either Registered, Public or Private.

The signature part of JWT is created by using the base64 encoded value of header and payload, a secret key that used by the algorithm (defined in the Header part of JWT) and signs that. This part is being used to verify the message is same as original i.e. wasn't change in transition.

The jwt.io debugger (https://jwt.io/) is enable us to decode the JWT (not decode signature part) and we can verify or generate new token.





Why Use JWT (JSON Web Token)?

One of the common answers to this question is, JWT is convenient, compact, and secure. The token is simply a based64 encoded string that contains the few header fields and payloads, so it usually contains fewer bytes compare to other tokens. It can be signed using either RSA public/private key-pair encryption or HMAC encryption using a shared secret, so they are more secure. It is open source libraries and readily available libraries with various technologies such as .net, Python, Java, Ruby, Swift etc.

There are many XML based tokens are available such as SAML (Security Assertion Markup Language) token, SWT (Simple Web Token), etc. The JWT is JSON based. The size of encoded JSON smaller compare to the size of encoded XML, so JSON Web Token is more compact than the other token. It is more secure because it uses public/private key in the form of an X.509 certificate for signing.

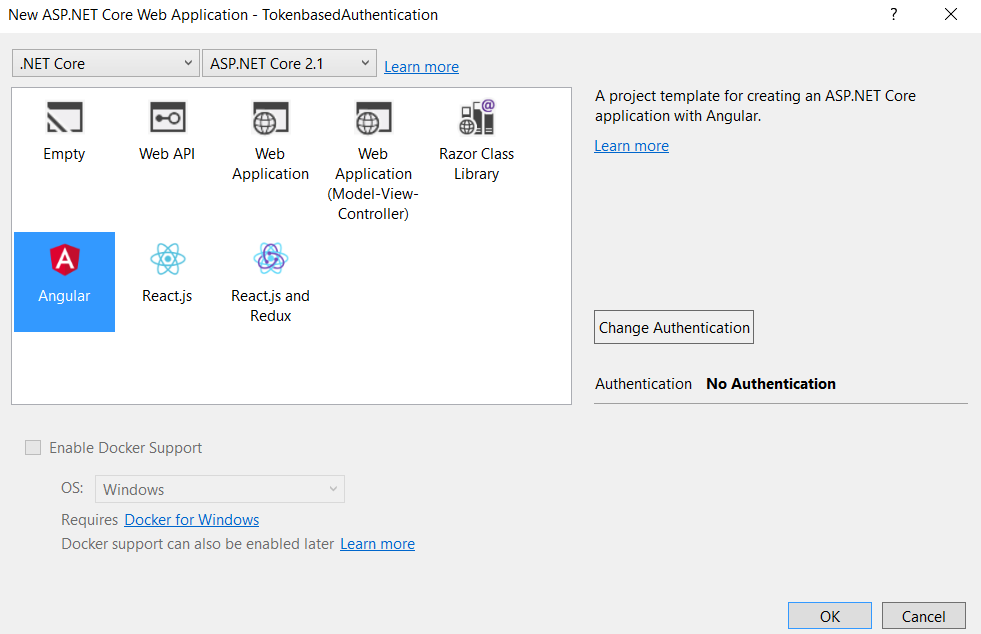
In this post, I will explain how to create application using Angular 6 app with ASP.net core 2.1 and do the token-based authentication using JWT.

Prerequisites

The following software needs to be installed in our system before starting the work.

* .NET Core framework 2.1 or above
* TypeScript 2.5 and above.
* Latest version of Node JS and npm (node package manager)
* Editor such as VS 2017 or VS Code

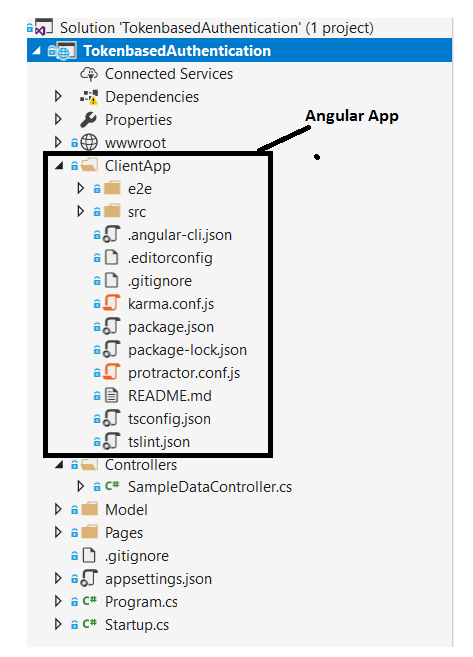
ASP.NET Core comes with many built-in template such as Angular, React, etc. I am using Angular template to demonstrate the concept. We can create an application by using Angular template of Visual Studio (2017 or higher) or using CLI (Command Line Interface).



Following .net core CLI command will create an ASP.NET Web API project with Angular with project name "TokenbasedAuthentication" in the current folder.

1. <dotnet new angular –n TokenbasedAuthentication

In this template, Angular client App and Web API are shipped together in one project, however we can create two separate project: one for Angular and other for web API.



Configure JWT Token based Authentication

To Configure, JWT based authentication, we need to register a JWT authentication schema by using "AddAuthentication" method and specifying JwtBearerDefaults.AuthenticationScheme. Here, we configure the JWT bearer options for authentication schema using AddJwtBearer method.

1. public void ConfigureServices(IServiceCollection services)
2. {
3. services.AddAuthentication(JwtBearerDefaults.AuthenticationScheme)
4. .AddJwtBearer(options =>
5. {
6. options.TokenValidationParameters = new TokenValidationParameters
7. {
8. ValidateIssuer = true,
9. ValidateAudience = true,
10. ValidateLifetime = true,
11. ValidateIssuerSigningKey = true,
12. ValidIssuer = Configuration["Jwt:Issuer"],
13. ValidAudience = Configuration["Jwt:Issuer"],
14. IssuerSigningKey = new SymmetricSecurityKey(Encoding.UTF8.GetBytes(Configuration["Jwt:Key"]))
15. };
16. });
17. services.AddMvc().SetCompatibilityVersion(CompatibilityVersion.Version\_2\_1);
19. *// In production, the Angular files will be served from this directory*
20. services.AddSpaStaticFiles(configuration =>
21. {
22. configuration.RootPath = "ClientApp/dist";
23. });
24. }

In this example, we have specified which parameters must be taken into account to consider JWT as valid. As per code mention in above section, the following items are considered to validate the token

* Validate the server information that generates the JWT ((ValidateIssuer = true)
* Validate the receiver of JWT (client) is authorized to receive (ValidateAudience = true)
* Check JWT expiration (ValidateLifetime = true)
* Check signature of the JWT (ValidateIssuerSigningKey = true)
* In this example, I have specify the values for the issuer, audience, signing key that are stored in appsettings.json file.

AppSetting.Json

1. {
2. "Jwt": {
3. "Key": "ThisismyPrivateSecretKey",
4. "Issuer": "abc.com"
5. }
6. }

After configuring JWT based authentication service, the next step is to make it is available to the application. Using app.UseAuthentication() method, we can add the service to the application. This method defines in the "Configure" method of startup class. The UseAuthentication method must called before UseMvc method otherwise .net framework does not recognize authentication service.

1. public void Configure(IApplicationBuilder app, IHostingEnvironment env)
2. {
3. ….
4. app.UseAuthentication();
5. app.UseMvc();
6. }

Generate JWT

To Generate JSON Web Token, I have created Login method under the LoginController that is responsible to generate the JWT. To bypass the authentication, I have marked this controller with "AllowAnonymous" attribute. Using UserModel, I have passed the username and password to this method. The AuthenticateUser method is responsible to validate User credential and returns to the UserModel. In this method, we have to write our custom code to validate user credential. For demonstration, I have only allowed “Jignesh” user i.e. I am checking hardcode value for username, if username is "Jignesh" then this method return user model and Web API generates the token by using GenerateJSONWebToken method.

With the help of JwtSecurityToken class object, we can create JWT. Here I have pass some parameters to constructor of the class while creating object of this class such as issuer, audience, expiration, claims, and signature. Finally using JwtSecurityTokenHandler.WriteToken method, we can generate the token based on the JwtSecurityToken class.

1. using System;
2. using System.IdentityModel.Tokens.Jwt;
3. using System.Security.Claims;
4. using System.Text;
5. using Microsoft.AspNetCore.Authorization;
6. using Microsoft.AspNetCore.Mvc;
7. using Microsoft.Extensions.Configuration;
8. using Microsoft.IdentityModel.Tokens;
9. using TokenbasedAuthentication.Model;
11. namespace TokenbasedAuthentication.Controllers
12. {
13. [Route("api/[controller]")]
14. [ApiController]
15. [AllowAnonymous]
16. public class LoginController : ControllerBase
17. {
18. private IConfiguration \_config;
20. public LoginController(IConfiguration config)
21. {
22. \_config = config;
23. }
24. [HttpPost]
25. public IActionResult Login([FromBody]UserModel login)
26. {
27. IActionResult response = Unauthorized();
28. var user = AuthenticateUser(login);
30. if (user != null)
31. {
32. var tokenString = GenerateJSONWebToken(user);
33. response = Ok(new { token = tokenString });
34. }
36. return response;
37. }
39. private string GenerateJSONWebToken(UserModel userInfo)
40. {
41. var securityKey = new SymmetricSecurityKey(Encoding.UTF8.GetBytes(\_config["Jwt:Key"]));
42. var credentials = new SigningCredentials(securityKey, SecurityAlgorithms.HmacSha256);
44. var claims = new[] {
45. new Claim(JwtRegisteredClaimNames.Sub, userInfo.Username),
46. new Claim(JwtRegisteredClaimNames.Email, userInfo.EmailAddress),
47. new Claim("DateOfJoing", userInfo.DateOfJoing.ToString("yyyy-MM-dd")),
48. new Claim(JwtRegisteredClaimNames.Jti, Guid.NewGuid().ToString())
49. };
51. var token = new JwtSecurityToken(\_config["Jwt:Issuer"],
52. \_config["Jwt:Issuer"],
53. claims,
54. expires: DateTime.Now.AddMinutes(120),
55. signingCredentials: credentials);
57. return new JwtSecurityTokenHandler().WriteToken(token);
58. }
60. private UserModel AuthenticateUser(UserModel login)
61. {
62. UserModel user = null;
64. *//Validate the User Credentials*
65. *//Demo Purpose, I have Passed HardCoded User Information*
66. if (login.Username == "Jignesh")
67. {
68. user = new UserModel { Username = "Jignesh Trivedi", EmailAddress = "test.btest@gmail.com" };
69. }
70. return user;
71. }
72. }
73. }

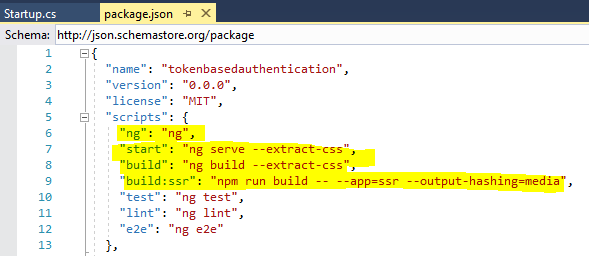
Once, we have enabled the JWT based authentication, we need to pass the token with request header which marked with authorize attribute. If we call a method (that mark with authorize attribute) without token or invalid token, we will get 401 (UnAuthorizedAccess) - HTTP status code as a response. The AllowAnonymous attribute help us to bypass the authentication for any action method or controller(for all action methods within controller).

Client App in Angular 6

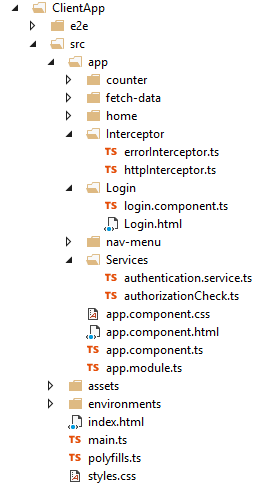
Asp.net core Angular Template creates an Angular app in our project under “ClientApp” folder. Alternatively, we can create an Angular App using Angular CLI (https://cli.angular.io/). To configure SPA (Single Page Application) with angular and ASP.net core web API, we need to register an SPA service in configuring method of startup class and supply source path. Also, during the development, we need to run the angular command to start the angular application. The commands that are used during start app can be defined in the package.json file. Using Following code, we can configure SPA.

Startup.cs

1. public void Configure(IApplicationBuilder app, IHostingEnvironment env)
2. {
3. …..
4. …..
5. app.UseMvc(routes =>
6. {
7. routes.MapRoute(
8. name: "default",
9. template: "{controller}/{action=Index}/{id?}");
10. });
12. app.UseSpa(spa =>
13. {
14. *// To learn more about options for serving an Angular SPA from ASP.NET Core,*
15. *// see https://go.microsoft.com/fwlink/?linkid=864501*
17. spa.Options.SourcePath = "ClientApp";
19. if (env.IsDevelopment())
20. {
21. spa.UseAngularCliServer(npmScript: "start");
22. }
23. });
24. }



I have created following code structure for Angular application. Here, I have created all client code under “scr\app” folder. I have created Login component that take user credential and with help of authorization service, it stored JWT in HTML 5 local storage.



Authentication Service

**Path** \ClientApp\src\app\Services\authentication.service.ts

Authentication Service is responsible to provide login and logout feature to the application. This service post user credential to the web API for Login and check the response. If the response is successful, so response contains the JSON web token and token details are stored in local storage. If the response is not successful, it returns the error which is display by the login component. The local storage shared the data between browser sessions and data also preserve in local storage event if refresh the browser. Alternatively, we can store token information within windows session storage. The session storage cannot share the information between browser sessions. For Logout, it simply removes the token from local storage

1. import { Injectable } from '@angular/core';
2. import { HttpClient } from '@angular/common/http';
3. import { map } from 'rxjs/operators';
5. @Injectable()
6. export class AuthenticationService {
7. constructor(private http: HttpClient) { }
9. login(username: string, password: string) {
10. return this.http.post<any>('/api/login', { username, password })
11. .pipe(map(user => {
12. *// login successful if there's a jwt token in the response*
13. if (user && user.token) {
14. *// store user details and jwt token in local storage to keep user logged in between page refreshes*
15. localStorage.setItem('TokenInfo', JSON.stringify(user));
16. }
18. return user;
19. }));
20. }
22. logout() {
23. *// remove user from local storage to log user out*
24. localStorage.removeItem('TokenInfo');
25. }
26. }

Login Template and component

**Path** \ClientApp\src\app\Login\

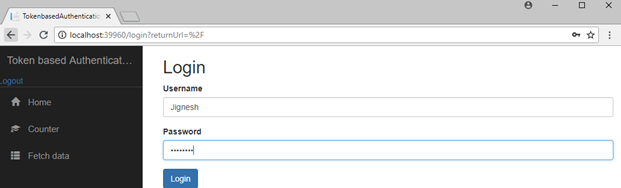
The login component template contains username and password fields. It also shows the validation for invalid fields when you will click submit button. The submit event of the form is bound to "OnLogin" method of login component. The "OnLogin" method uses the authentication service’s “login” method to validate user credential and generate token.

Login Template

1. <h2>Login</h2>
2. <form [formGroup]="loginForm" (ngSubmit)="onLogin()">
3. <div class="form-group">
4. <label for="username">Username</label>
5. <input type="text" formControlName="username" class="form-control" [ngClass]="{ 'is-invalid': submitted && formData.username.errors }" />
6. <div \*ngIf="submitted && formData.username.errors" class="invalid-feedback">
7. <div \*ngIf="formData.username.errors.required">Username is required</div>
8. </div>
9. </div>
10. <div class="form-group">
11. <label for="password">Password</label>
12. <input type="password" formControlName="password" class="form-control" [ngClass]="{ 'is-invalid': submitted && formData.password.errors }" />
13. <div \*ngIf="submitted && formData.password.errors" class="invalid-feedback">
14. <div \*ngIf="formData.password.errors.required">Password is required</div>
15. </div>
16. </div>
17. <div class="form-group">
18. <button [disabled]="submitClick" class="btn btn-primary">Login</button>
19. </div>
20. <div \*ngIf="error" class="alert alert-danger"></div>
21. </form>

Login Component

1. import { Component, OnInit } from '@angular/core';
2. import { Router, ActivatedRoute } from '@angular/router';
3. import { FormBuilder, FormGroup, Validators } from '@angular/forms';
4. import { first } from 'rxjs/operators';
6. import { AuthenticationService } from '../Services/authentication.service';
8. @Component({
9. templateUrl: 'login.html'
10. })
11. export class LoginComponent implements OnInit {
13. loginForm: FormGroup;
14. submitClick = false;
15. submitted = false;
16. returnUrl: string;
17. error = '';
19. constructor(
20. private formBuilder: FormBuilder,
21. private route: ActivatedRoute,
22. private router: Router,
23. private authenticationService: AuthenticationService) { }
25. ngOnInit() {
26. this.loginForm = this.formBuilder.group({
27. username: ['', Validators.required],
28. password: ['', Validators.required]
29. });
31. *// reset login status*
32. this.authenticationService.logout();
34. *// get return url from route parameters or default to '/'*
35. this.returnUrl = this.route.snapshot.queryParams['returnUrl'] || '/';
36. }
38. *// convenience getter for easy access to form fields*
39. get formData() { return this.loginForm.controls; }
41. onLogin() {
42. this.submitted = true;
44. *// stop here if form is invalid*
45. if (this.loginForm.invalid) {
46. return;
47. }
49. this.submitClick = true;
50. this.authenticationService.login(this.formData.username.value, this.formData.password.value)
51. .pipe(first())
52. .subscribe(
53. data => {
54. this.router.navigate([this.returnUrl]);
55. },
56. error => {
57. this.error = error;
58. this.submitClick = false;
59. });
60. }
61. }



Restrict Unauthenticated User to access the Application

I have created authorization check that prevent unauthenticated users from accessing restricted routes. Angular route provides the feature called Navigation Guards that allow us to write code before routing occurred. There are four different guard types available in Angular: CanActivate, CanActivateChild, CanDeactivate and CanLoad. Here I have check whether local storage contains the token information if yes than allow to navigate else navigate to login page.

Path:ClientApp\src\app\Services\authorizationCheck.ts

1. import { Injectable } from '@angular/core';
2. import { Router, CanActivate, ActivatedRouteSnapshot, RouterStateSnapshot } from '@angular/router';
4. @Injectable()
5. export class AuthorizationCheck implements CanActivate {
7. constructor(private router: Router) { }
9. canActivate(route: ActivatedRouteSnapshot, state: RouterStateSnapshot) {
10. *//If token data exist, user may login to application*
11. if (localStorage.getItem('TokenInfo')) {
12. return true;
13. }
15. *// otherwise redirect to login page with the return url*
16. this.router.navigate(['/login'], { queryParams: { returnUrl: state.url } });
17. return false;
18. }
19. }

Http Interceptor

After successful login to application, we need to pass token with every http request header. For the same we can write common code using Http Interceptor. It intercepts the http request and add the JWT (auth token) to the header of request if user is logged in. The TypeScript has allowed us to extend any predefined class, so we can create custom http interceptor by extending the HttpInterceptor class. This allow us to modify http request before it sent to the server. To register this Http interceptor, we need to add it to request pipeline by configure in the provider section of the app.module.ts file.

Path: ClientApp\src\app\Interceptor\httpInterceptor.ts

1. import { Injectable } from '@angular/core';
2. import { HttpRequest, HttpHandler, HttpEvent, HttpInterceptor } from '@angular/common/http';
3. import { Observable } from 'rxjs';
5. @Injectable()
6. export class httpInterceptor implements HttpInterceptor {
7. intercept(request: HttpRequest<any>, newRequest: HttpHandler): Observable<HttpEvent<any>> {
8. *// add authorization header to request*
10. *//Get Token data from local storage*
11. let tokenInfo = JSON.parse(localStorage.getItem('TokenInfo'));
13. if (tokenInfo && tokenInfo.token) {
14. request = request.clone({
15. setHeaders: {
16. Authorization: `Bearer ${tokenInfo.token}`,
17. 'Content-Type': 'application/x-www-form-urlencoded;charset=utf-8'
18. }
19. });
20. }
22. return newRequest.handle(request);
23. }
24. }

Error Interceptor

I have added one more interceptor that check the errors from the http responses and re-throw the error. This interceptor analyses http response error and if the status code is a (401 Unauthorized response), user get logout automatically.

Path: ClientApp\src\app\Interceptor\errorInterceptor.ts

1. import { Injectable } from '@angular/core';
2. import { HttpRequest, HttpHandler, HttpEvent, HttpInterceptor } from '@angular/common/http';
3. import { Observable } from 'rxjs/Rx';
4. import { catchError } from 'rxjs/operators';
6. import { AuthenticationService } from '../Services/authentication.service';
7. import { Router } from '@angular/router';
9. @Injectable()
10. export class ErrorInterceptor implements HttpInterceptor {
11. constructor(private authenticationService: AuthenticationService, private router: Router) { }
13. intercept(request: HttpRequest<any>, newRequest: HttpHandler): Observable<HttpEvent<any>> {
15. return newRequest.handle(request).pipe(catchError(err =>{
16. if (err.status === 401) {
17. *//if 401 response returned from api, logout from application & redirect to login page.*
18. this.authenticationService.logout();
19. }
21. const error = err.error.message || err.statusText;
22. return Observable.throw(error);
23. }));
24. }
25. }

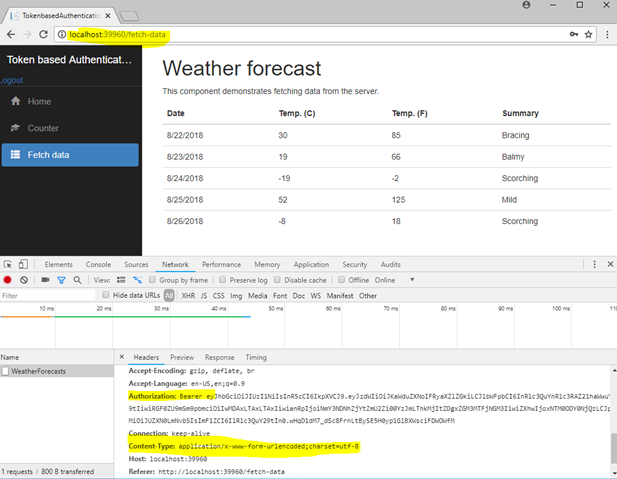
App Module and Routing

The app module defines the root module of the application that contains the metadata about the module. We need to register all the interceptors, services, components and other modules within this app module. We can also define routing with-in app module.

1. import { BrowserModule } from '@angular/platform-browser';
2. import { NgModule } from '@angular/core';
3. import { FormsModule, ReactiveFormsModule } from '@angular/forms';
4. import { HttpClientModule, HTTP\_INTERCEPTORS } from '@angular/common/http';
5. import { RouterModule } from '@angular/router';
7. import { AppComponent } from './app.component';
8. import { NavMenuComponent } from './nav-menu/nav-menu.component';
9. import { HomeComponent } from './home/home.component';
10. import { CounterComponent } from './counter/counter.component';
11. import { FetchDataComponent } from './fetch-data/fetch-data.component';
13. import { LoginComponent } from './Login/login.component'
15. import { httpInterceptor } from './Interceptor/httpInterceptor';
16. import { ErrorInterceptor } from './Interceptor/errorInterceptor';
18. import { AuthorizationCheck } from './Services/authorizationCheck'
19. import { AuthenticationService } from './Services/authentication.service'
21. @NgModule({
22. declarations: [
23. AppComponent,
24. NavMenuComponent,
25. HomeComponent,
26. CounterComponent,
27. FetchDataComponent,
28. LoginComponent
29. ],
30. imports: [
31. BrowserModule.withServerTransition({ appId: 'ng-cli-universal' }),
32. HttpClientModule,
33. FormsModule,
34. ReactiveFormsModule,
35. RouterModule.forRoot([
36. { path: '', component: HomeComponent, pathMatch: 'full', canActivate: [AuthorizationCheck] },
37. { path: 'counter', component: CounterComponent, canActivate: [AuthorizationCheck] },
38. { path: 'fetch-data', component: FetchDataComponent, canActivate: [AuthorizationCheck] },
39. { path: 'login', component: LoginComponent }
40. ])
41. ],
42. providers: [
43. { provide: HTTP\_INTERCEPTORS, useClass: httpInterceptor, multi: true },
44. { provide: HTTP\_INTERCEPTORS, useClass: ErrorInterceptor, multi: true },
45. AuthorizationCheck, AuthenticationService],
46. bootstrap: [AppComponent]
47. })
48. export class AppModule { }

Demo

To demonstration, I have mark SampleDataController with Authorize attribute so only authenticated user can able to access the method within this controller. Using “fetch-data” route, I am trying to access the page. As see in following snap, request header contains the authorization token and after successful authentication on server side, it returns weather forecast data.



Summary

JWT (JSON Web Token) is most popular and open standard that allows transmitting data between parties as a JSON object in a secure and compact way. Following are some summary of this article.

* JWT allow us to do token-based authentication
* help of the Angular guard, we can redirection for anonymous users to the login page by client-side code.
* Angular interceptors help us to set authorization header to each http request and handle 401 unauthorized access status code
* Using AllowAnonymous attribute, we can bypass the authorization at server side. This attribute can either applied to controller or individual action method
* Controller or action method which mark with Authorize attribute, they allow only the authenticated user to access, You can view or download source code from the top of the article.