JWT TOKEN AND REFRESH TOKEN AUTHENTICATION

JWT TOKEN:

JWT token is a base64url encoded string that is used to transmit the information between server and client. JWT token mostly contains the user information which is used for authorization.

JWT token can be sent through a URL, POST parameter, and HTTP header.  
The information that is sent by JWT is verified and trusted because it is [digitally signed](https://lazyhacker22.blogspot.com/2022/05/what-is-digital-signature.html).

**JWT token looks like:**  
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9**.**eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ**.**SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV\_adQssw5c

JWT token has three parts:<https://jwt.io/>

Header:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9  
*{“alg”: “HS256”,”typ”: “JWT”}*

**Payload:**  
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ  
*{“sub”: “1234567890”,”name”: “John Doe”,”iat”: 1516239022}*

Signature:SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV\_adQssw5c  
*HMACSHA256(base64UrlEncode(header) + “.” +base64UrlEncode(payload), your-secret)*

**Uses of JWT token**\*Authorization:After successful authentication, the application receives the JWT token. That JWT token is passed in every request for accessing the services.  
\* The JWT token is also used for exchanging information.

**Refresh Token:**

A refresh token is a special key that enables a client for an API or service to retrieve new access tokens without requiring the user to perform a complete login. In other words, an application can exchange a valid refresh token for a new access token.

**Requirements for creating jwt tokens and refresh tokens in asp.net core6 web Api?**

**Install packages:** Microsoft.AspNetCore.Authentication.JwtBearer;

**Program.cs:**

using Microsoft.AspNetCore.Authentication.JwtBearer;

// read the key from AppSettings:

var appSettingsread = configRoot.GetSection("AppSettings");

services.Configure<AppSettings>(appSettingsread);

// jwt authentication:

var settings = appSettingsread.Get<AppSettings>();

var secret = Encoding.UTF8.GetBytes(settings.Key);

// jwt authentication:

// default:

var key = configRoot["AppSettings:Key"] ?? throw new InvalidProgramException("Secret key not configured");

services.AddSingleton<IHttpContextAccessor, HttpContextAccessor>();

// configure authentication

services.AddAuthentication(options =>

{

options.DefaultAuthenticateScheme = JwtBearerDefaults.AuthenticationScheme;

options.DefaultChallengeScheme = JwtBearerDefaults.AuthenticationScheme;

options.DefaultScheme = JwtBearerDefaults.AuthenticationScheme;

})

.AddCookie(options =>

options.Cookie.Name = "token"

)

.AddJwtBearer(options =>

{

options.SaveToken = true;

options.RequireHttpsMetadata = false;

options.TokenValidationParameters = new TokenValidationParameters

{

ValidateIssuer = true,

ValidateAudience = true,

ValidateLifetime = true,

ValidateIssuerSigningKey = true,

// ClockSkew = TimeSpan.Zero,

ClockSkew = new TimeSpan(0, 0, 5),

ValidAudience = configRoot["JWT:ValidAudience"],

ValidIssuer = configRoot["JWT:ValidIssuer"],

IssuerSigningKey = new SymmetricSecurityKey(secret),

//ValidateIssuerSigningKey = true,

//IssuerSigningKey = new SymmetricSecurityKey(secret),

//ValidateIssuer = false,

//ValidateAudience = false

};

options.Events = new JwtBearerEvents

{

OnMessageReceived = context =>

{

context.Token = context.Request.Cookies["token"];

return Task.CompletedTask;

}

};

});

Data Access Layer:

ILoginAuthRepo:

public interface ILoginAuthRepo

{

//bool Register(RegisterModel register);

// Task<RegisterModel> GetByEmail(string email);

public Response Register(RegisterModel register);

Response Login(LoginModel login);

Response GetByEmail(string email);

Response Refresh([FromBody] TokenModel model);

}

LoginAuthRepo:

Configs:

private readonly IOptions<ConnectionStrings> \_config;

private readonly IOptions<AppSettings> \_appsettings;

private readonly IConfiguration \_configuration;

private readonly IOptions<JWT> \_jwt;

private readonly IHttpContextAccessor \_httpContextAccessor;

public LoginAuthRepo(

IOptions<ConnectionStrings> config,

IOptions<AppSettings> appsettings,

IConfiguration configuration,

IOptions<JWT> jwt,

IHttpContextAccessor httpContextAccessor

)

{

\_config = config;

\_appsettings = appsettings;

\_configuration = configuration;

\_jwt = jwt;

\_httpContextAccessor = httpContextAccessor;

}

Generate jwt token:

private JwtSecurityToken GenerateJwtToken(string username)

{

var authClaims = new List<Claim>

{

new Claim(ClaimTypes.Name,username),

new Claim(JwtRegisteredClaimNames.Jti,Guid.NewGuid().ToString())

};

var validIssuer = \_jwt.Value.ValidIssuer;

var ValidAudience = \_jwt.Value.ValidAudience;

var tokenValidityInMinutes = \_jwt.Value.TokenValidityInMinutes;

var secret = \_configuration["AppSettings:Key"] ?? throw new InvalidOperationException("Secret Key is not configured");

var Key = new SymmetricSecurityKey(Encoding.UTF8.GetBytes(secret));

var token = new JwtSecurityToken(

issuer:validIssuer,

audience:ValidAudience,

expires: DateTime.UtcNow.AddMinutes(tokenValidityInMinutes),

claims:authClaims,

signingCredentials:new SigningCredentials(Key,SecurityAlgorithms.HmacSha256)

);

return token;

}

GetPrincipalFromExpiredToken:

private ClaimsPrincipal? GetPrincipalFromExpiredToken(string token)

{

var secret = \_configuration["AppSettings:Key"] ?? throw new InvalidOperationException("Secret Key is not configured");

var tokenValidationParameters = new TokenValidationParameters

{

ValidateAudience = false,

ValidateIssuer = false,

ValidateIssuerSigningKey = true,

ValidateLifetime = false,

IssuerSigningKey = new SymmetricSecurityKey(Encoding.UTF8.GetBytes(secret))

};

var tokenHandler = new JwtSecurityTokenHandler ();

var principal = tokenHandler.ValidateToken(token, tokenValidationParameters, out SecurityToken securityToken);

if(securityToken is not JwtSecurityToken jwtSecurityToken || !jwtSecurityToken.Header.Alg.Equals(SecurityAlgorithms.HmacSha256,StringComparison.InvariantCultureIgnoreCase))

throw new SecurityTokenException("Invalid Token");

return principal;

}

Generate refresh token:

private static string RefreshTokenGenerator ()

{

var randomNumber = new byte[640];

using var generator = RandomNumberGenerator.Create();

generator.GetBytes(randomNumber);

return Convert.ToBase64String(randomNumber);

}

encrypted password

public static string EncryptedPassword(string password)

{

if (string.IsNullOrEmpty(password))

{

return "";

}

else

{

byte[] passwordBase64 = ASCIIEncoding.ASCII.GetBytes(password);

string encryptPassword = Convert.ToBase64String(passwordBase64);

return encryptPassword;

}

}

Decrypted password

public static string DecryptedPassword(string password)

{

if (string.IsNullOrEmpty(password))

{

return "";

}

else

{

byte[] encryptPassword = Convert.FromBase64String(password);

string DecryptedPassword = ASCIIEncoding.ASCII.GetString(encryptPassword);

return DecryptedPassword;

}

}

sha256 password:

public static string EncryptSha256Password (string password)

{

using var sha256 = SHA256.Create();

byte[] hashPassword = Encoding.UTF8.GetBytes(password);

byte[] EncryptPasswordstorage = sha256.ComputeHash(hashPassword);

return Convert.ToBase64String(EncryptPasswordstorage);

}

Register:

public Response Register(RegisterModel register)

{

Response resposne = new Response();

string connection = \_config.Value.SNCon.ToString();

using (SqlConnection conn = new SqlConnection(connection))

{

conn.Open();

SqlCommand checkEmail = new SqlCommand("check\_email\_register", conn);

checkEmail.CommandType = System.Data.CommandType.StoredProcedure;

checkEmail.Parameters.AddWithValue("@Email", register.Email);

string email = (string)checkEmail.ExecuteScalar();

if(email == register.Email)

{

resposne.StatusCode = 400;

resposne.StatusMessage = "Email id already existed";

}

else

{

SqlCommand cmd = new SqlCommand("Usp\_Register", conn);

cmd.CommandType = System.Data.CommandType.StoredProcedure;

cmd.Parameters.AddWithValue("@UserName", register.UserName);

cmd.Parameters.AddWithValue("@Email", register.Email);

// without encypted password

// cmd.Parameters.AddWithValue("@Password", register.Password); EncryptSha256Password

cmd.Parameters.AddWithValue("@Password", EncryptedPassword(register.Password));

// cmd.Parameters.AddWithValue("@Password", EncryptSha256Password(register.Password));

int i = cmd.ExecuteNonQuery();

conn.Close();

RegisterModel model = new RegisterModel();

if (i > 0)

{

model.UserName= register.UserName;

model.Email= register.Email;

model.Password= register.Password;

resposne.StatusCode = 200;

resposne.StatusMessage = "Successfully registered";

resposne.Register = model;

}

else

{

resposne.StatusCode = 400;

resposne.StatusMessage = "Registration has been failed";

resposne.Register = null;

}

}

return resposne;

}

}

Login:

public Response Login(LoginModel login)

{

Response response = new Response();

string connection = \_config.Value.SNCon.ToString();

using (SqlConnection conn = new SqlConnection(connection))

{

conn.Open();

SqlCommand checkLogins = new SqlCommand("check\_email\_password", conn);

checkLogins.CommandType = System.Data.CommandType.StoredProcedure;

checkLogins.Parameters.AddWithValue("@Email", login.Email);

checkLogins.Parameters.AddWithValue("@Password", EncryptedPassword(login.Password));

int Variable = (int)checkLogins.ExecuteScalar();

conn.Close();

if (Variable == 1)

{

var tokenHandler = new System.IdentityModel.Tokens.Jwt.JwtSecurityTokenHandler();

var KEY = Encoding.UTF8.GetBytes(\_appsettings.Value.Key);

var issuer = \_jwt.Value.ValidIssuer;

var audience = \_jwt.Value.ValidAudience;

var tokenValidityInMinutes = \_jwt.Value.TokenValidityInMinutes;

var refreshTokenValidityInMinutes = \_jwt.Value.RefreshTokenValidityInMinutes;

var tokenDescriptor = new Microsoft.IdentityModel.Tokens.SecurityTokenDescriptor

{

Subject = new System.Security.Claims.ClaimsIdentity(new Claim[]

{

new Claim(ClaimTypes.Name, login.Email.ToString()),

//new Claim("Id", Guid.NewGuid().ToString()),

new Claim(JwtRegisteredClaimNames.Sub, login.Email),

new Claim(JwtRegisteredClaimNames.Email, login.Email),

new Claim(JwtRegisteredClaimNames.Jti,

Guid.NewGuid().ToString())

}),

//Expires = DateTime.UtcNow.AddMinutes(10),

//Issuer = \_configuration["JWT:ValidIssuer"],

//Audience = \_configuration["JWT:ValidAudience"],

Expires = DateTime.UtcNow.AddMinutes(tokenValidityInMinutes),

Issuer = issuer,

Audience = audience,

SigningCredentials = new Microsoft.IdentityModel.Tokens.SigningCredentials(new Microsoft.IdentityModel.Tokens.SymmetricSecurityKey(KEY), Microsoft.IdentityModel.Tokens.SecurityAlgorithms.HmacSha256Signature)

};

var token = tokenHandler.CreateToken(tokenDescriptor);

var refreshToken = RefreshTokenGenerator();

//\_ = int.TryParse(\_configuration["JWT:RefreshTokenValidityInMinutes"], out int refreshTokenValidityInMinutes);

var Token = tokenHandler.WriteToken(token);

TokenModel model = new TokenModel();

model.RefreshToken = refreshToken;

model.ExpireRefreshTokenTime = DateTime.UtcNow.AddMinutes(refreshTokenValidityInMinutes);

model.AccessToken = Token;

response.Token = model;

response.Login = login;

response.StatusCode = 200;

response.StatusMessage = "Login Successful";

\_httpContextAccessor.HttpContext.Response.Cookies.Append("token", Token, new CookieOptions()

{

Expires = DateTime.UtcNow.AddMinutes(tokenValidityInMinutes),

//HttpOnly = true,

//Secure = true,

//IsEssential = true,

//SameSite = SameSiteMode.None

HttpOnly = true,

SameSite = SameSiteMode.Strict

});

\_httpContextAccessor.HttpContext.Response.Cookies.Append("X-Refresh-Token", refreshToken, new CookieOptions() { HttpOnly = true, SameSite = SameSiteMode.Strict });

\_httpContextAccessor.HttpContext.Response.Cookies.Append("X-Username", login.Email, new CookieOptions() { HttpOnly = true, SameSite = SameSiteMode.Strict });

}

else

{

response.StatusCode = 400;

response.StatusMessage = "Invalid UserName or Password";

}

return response;

}

}

Refresh Token:

public Response Refresh([FromBody] TokenModel model)

{

Response response = new Response();

string connection = \_config.Value.SNCon.ToString();

using(SqlConnection conn = new SqlConnection(connection))

{

conn.Open();

var principal = GetPrincipalFromExpiredToken(model.AccessToken);

if (principal == null)

{

response.StatusCode = 400;

response.StatusMessage = "Invalid access token or refresh token";

}

var username = principal?.Identity?.Name;

// var user = GetByEmail(username);

// check by username

SqlCommand checkEmail = new SqlCommand("check\_email\_register", conn);

checkEmail.CommandType = CommandType.StoredProcedure;

checkEmail.Parameters.AddWithValue("@Email", username);

string email = (string)checkEmail.ExecuteScalar();

conn.Close();

if (email != username)

{

response.StatusCode = 400;

response.StatusMessage = "Invalid access token or Invalid refresh token";

} else

{

var newAccessToken = GenerateJwtToken(username);

var newRefreshToken = RefreshTokenGenerator();

model.RefreshToken = newRefreshToken;

var jwtToken = new JwtSecurityTokenHandler().WriteToken(newAccessToken);

model.AccessToken = jwtToken;

model.ExpireRefreshTokenTime = DateTime.UtcNow.AddMinutes(\_jwt.Value.RefreshTokenValidityInMinutes);

if (model.AccessToken != null)

{

response.StatusCode = 200;

response.StatusMessage = "Refresh successfully..";

response.Token = model;

}

}

// Store Token data into the Cookies …. Refresh and Access token data

\_httpContextAccessor.HttpContext.Response.Cookies.Append("token", model.AccessToken, new CookieOptions()

{

Expires = DateTime.UtcNow.AddMinutes(\_jwt.Value.TokenValidityInMinutes),

//HttpOnly = true,

//Secure = true,

//IsEssential = true,

//SameSite = SameSiteMode.None

HttpOnly = true,

SameSite = SameSiteMode.Strict

});

\_httpContextAccessor.HttpContext.Response.Cookies.Append("X-Refresh-Token", model.RefreshToken, new CookieOptions() { HttpOnly = true, SameSite = SameSiteMode.Strict });

\_httpContextAccessor.HttpContext.Response.Cookies.Append("X-Username", username, new CookieOptions() { HttpOnly = true, SameSite = SameSiteMode.Strict });

return response;

}

}

Controller:

using BusinessLogicLayer;

using CommonLayer.Models;

using DataAccessLayer.Entities;

using DataAccessLayer.Interfaces;

using Microsoft.AspNetCore.Http;

using Microsoft.AspNetCore.Mvc;

namespace StudentThreeTier.Controllers

{

[Route("api/[controller]")]

[ApiController]

public class AccountController : ControllerBase

{

private readonly ILoginAuthService \_loginAuthService;

private readonly IHttpContextAccessor \_httpContextAccessor;

private readonly ILoginAuthRepo \_loginAuthRepo;

public AccountController(

ILoginAuthRepo loginAuthRepo,

ILoginAuthService loginAuthService,

IHttpContextAccessor httpContextAccessor

)

{

\_loginAuthService = loginAuthService;

\_httpContextAccessor = httpContextAccessor;

\_loginAuthRepo = loginAuthRepo;

}

[HttpPost]

[Route("Login")]

public IActionResult Login(LoginModel loginModel)

{

var result = \_loginAuthService.Login(loginModel);

if (result.StatusCode != 200)

{

return BadRequest(new { message = result.StatusMessage });

}

//if(result)

//{

// return Ok(result);

//}

//else

//{

// return BadRequest(new { message = "Invalid username or password" });

//}

return Ok(new { result.Token,result.StatusMessage,result.StatusCode});

}

[HttpPost]

[Route("RegisterDetails")]

[Produces("application/json")]

public IActionResult RegisterDetails(RegisterModel register)

{

var result = \_loginAuthService.Register(register);

if(result.StatusCode != 200)

{

return BadRequest(new { message = result.StatusMessage});

}

return Ok(result);

}

[HttpPost]

[Route("Refresh-token")]

public async Task<IActionResult> RefreshToken([FromBody] TokenModel model)

{

\_ = \_httpContextAccessor.HttpContext.Request.Cookies.TryGetValue("token", out var token);

\_ = \_httpContextAccessor.HttpContext.Request.Cookies.TryGetValue("X-Refresh-Token", out var cookieRefreshToken);

if (token != model.AccessToken || cookieRefreshToken != model.RefreshToken || model.ExpireRefreshTokenTime < DateTime.UtcNow)

//if ( model.ExpireRefreshTokenTime < DateTime.UtcNow)

{

return BadRequest("Invalid token or refresh credentials");

// throw new InvalidProgramException("Invalid token credentials");

}

var result = \_loginAuthService.Refresh(model);

if(result.StatusCode != 200)

{

return BadRequest(new {message = result.StatusMessage});

}

return Ok(new { token = result.Token.AccessToken, refreshToken = result.Token.RefreshToken,expire = result.Token.ExpireRefreshTokenTime

});

}

[HttpGet]

[Route("GetByEmailId")]

public async Task<IActionResult> GetByEmailId(string email)

{

if(email == null)

{

return BadRequest();

}

var result = \_loginAuthService.GetByEmail(email);

if(result.StatusCode != 200) {

return NotFound("Email Address is not found.");

}

return Ok(new {Status = result.StatusCode,Message = result.StatusMessage,Details = result.Register});

}

}

}

Business Access Layer:

ILoginAuthService:

namespace BusinessLogicLayer

{

public interface ILoginAuthService

{

Response Register(RegisterModel register);

Response Login(LoginModel login);

Response Refresh([FromBody] TokenModel model);

Response GetByEmail(string email);

}

}

LoginAuthService:

using CommonLayer.Models;

using DataAccessLayer.Entities;

using DataAccessLayer.Interfaces;

using Microsoft.AspNetCore.Mvc;

using System;

using System.Collections.Generic;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

namespace BusinessLogicLayer

{

public class LoginAuthService : ILoginAuthService

{

private readonly ILoginAuthRepo \_repo;

public LoginAuthService(ILoginAuthRepo repo)

{

\_repo = repo;

}

public Response GetByEmail(string email)

{

var result = \_repo.GetByEmail(email);

return result;

}

public Response Login(LoginModel login)

{

var result = \_repo.Login(login);

return result;

}

public Response Refresh([FromBody] TokenModel model)

{

var result = \_repo.Refresh(model);

return result;

}

public Response Register(RegisterModel register)

{

var result = \_repo.Register(register);

return result;

}

}

}

SQL QUERY PROCEDURES:

use StudentDB;

CREATE TABLE Employee(

Id int Identity(1,1) primary key,

FirstName varchar(100),

LastName varchar(100),

Email varchar(100),

PhoneNumber varchar(100),

DOB DATE,

Salary decimal

);

--drop table Login;

CREATE TABLE Register(

Id Int Identity(1,1) primary key,

UserName varchar(100),

Email varchar(100),

Password varchar(100)

);

select \* from Register;

Check exis

create proc check\_email\_password(

@Email varchar(100),

@Password varchar(100)

)

as

begin

select Email,Password from Register where Email=@Email and Password =@Password;

end

exec check\_email\_password @Email='saikumar@gmail.com',@Password='sai123'