**Hands-On: Stage 4 - Practice Check Case Study on Web API - Day 77 – Hands on**

1. **FSE Web API Specification Document**

**AdminController.cs**

using System;

using System.Collections.Generic;

using System.Linq;

using System.Threading.Tasks;

using Microsoft.AspNetCore.Authentication.JwtBearer;

using Microsoft.AspNetCore.Authorization;

using Microsoft.AspNetCore.Http;

using Microsoft.AspNetCore.Mvc;

using PracticeCheck.Models;

namespace PracticeCheck.Controllers

{

    [Route("api/[controller]")]

    [ApiController]

    [Authorize]

    [Authorize(Roles ="Admin")]

    public class AdminController : ControllerBase

    {

        // GET: api/Admin

        [HttpGet]

        public IEnumerable<MenuItem> Get()

        {

            return MenuItemOperation.GetConnection();

        }

        // PUT: api/Admin/5

        [HttpPut("{id}")]

        public IActionResult Put(int id, [FromBody] MenuItem menuitem)

        {

           MenuItemOperation.Update(id,menuitem);

            return Ok();

        }

    }

}

**AnonymousUserController.cs**

using System;

using System.Collections.Generic;

using System.Linq;

using System.Threading.Tasks;

using Microsoft.AspNetCore.Authorization;

using Microsoft.AspNetCore.Http;

using Microsoft.AspNetCore.Mvc;

using PracticeCheck.Models;

namespace PracticeCheck.Controllers

{

    [Route("api/[controller]")]

    [ApiController]

    [AllowAnonymous]

    public class AnonymousUserController : ControllerBase

    {

        // GET: api/AnonynousUser

        [HttpGet]

        public IEnumerable<MenuItem> Get()

        {

           return MenuItemOperation.GetConnection();

        }

    }

}

**AuthController.cs**

using System;

using System.Collections.Generic;

using System.IdentityModel.Tokens.Jwt;

using System.Linq;

using System.Security.Claims;

using System.Text;

using System.Threading.Tasks;

using Microsoft.AspNetCore.Http;

using Microsoft.AspNetCore.Mvc;

using Microsoft.IdentityModel.Tokens;

namespace PracticeCheck.Controllers

{

    //[Route("api/[controller]")]

    [ApiController]

    public class AuthController : ControllerBase

    {

        [HttpGet]

        [Route("api/Auth/{id}")]

        public IActionResult Get(int id)

        {

            if(id == -1)

                return Ok(GenerateJSONWebToken(""));

            if(id == 1)

                return Ok(GenerateJSONWebToken("Admin"));

            else

                return Ok(GenerateJSONWebToken("Customer"));

        }

        private string GenerateJSONWebToken(string userRole)

        {

            var securityKey = new SymmetricSecurityKey(Encoding.UTF8.GetBytes("mysuperdupersecret"));

            var credentials = new SigningCredentials(securityKey, SecurityAlgorithms.HmacSha256);

            var claims = new List<Claim>

            {

                new Claim(ClaimTypes.Role, userRole),

            };

            var token = new JwtSecurityToken(

                        issuer: "mySystem",

                        audience: "myUsers",

                        claims: claims,

                        expires: DateTime.Now.AddMinutes(5),

                        signingCredentials: credentials);

            return new JwtSecurityTokenHandler().WriteToken(token);

        }

    }

}

**CustomerController.cs**

using System;

using System.Collections.Generic;

using System.Linq;

using System.Threading.Tasks;

using Microsoft.AspNetCore.Authorization;

using Microsoft.AspNetCore.Http;

using Microsoft.AspNetCore.Mvc;

using PracticeCheck.Models;

namespace PracticeCheck.Controllers

{

    [Route("api/[controller]")]

    [ApiController]

    //[Authorize(Roles = "Customer")]

    public class CustomerController : ControllerBase

    {

        // GET: api/Customer

        [HttpGet]

        public IEnumerable<MenuItem> Get()

        {

            DateTime dt = DateTime.Now;

            return MenuItemOperation.GetConnection().Where(p => p.Active == true && p.DateOfLaunch <= dt);

        }

        // GET: api/Customer/5

        [HttpGet("{userid}", Name = "Get Customer")]

        public object Get(int userid)

        {

            int totalprice=0;

            List<MenuItem> list = new List<MenuItem>(MenuItemOperation.CartList(userid, ref totalprice));

            return new {list,totalprice };

        }

        // POST: api/Customer

        [HttpPost]

        public IActionResult Post([FromBody] List<Cart> cart)

        {

            MenuItemOperation.InsertIntoCart(cart);

            return Ok();

        }

        // DELETE: api/ApiWithActions/5

        [HttpDelete("{cartid}")]

        public string Delete(int cartid)

        {

            return MenuItemOperation.Delete(cartid);

        }

    }

}

**UserDetailsController.cs**

using System;

using System.Collections.Generic;

using System.Linq;

using System.Threading.Tasks;

using Microsoft.AspNetCore.Http;

using Microsoft.AspNetCore.Mvc;

using PracticeCheck.Models;

namespace PracticeCheck.Controllers

{

    [Route("api/[controller]")]

    [ApiController]

    public class UserDetailsController : ControllerBase

    {

        // GET: api/User/5

        [HttpGet("{id}", Name = "Get")]

        public string Get(int id,[FromBody]string password)

        {

            List<User> list = MenuItemOperation.UserList();

            bool user = list.Any(p => p.Id == id && p.Password == password);

              if (user == true)

                  return "true";

              return "falseSubmission";

        }

        // POST: api/User

        [HttpPost]

        public IActionResult Post([FromBody] User user)

        {

            MenuItemOperation.Insert(user);

            return Ok();

        }

    }

}

**Cart.cs**

using System;

using System.Collections.Generic;

using System.Linq;

using System.Threading.Tasks;

namespace PracticeCheck.Models

{

    public class Cart

    {

        public int Id { get; set; }

        public int MenuItemId { get; set; }

        public int UserId { get; set; }

    }

}

**Category.cs**

using System;

using System.Collections.Generic;

using System.Linq;

using System.Threading.Tasks;

namespace PracticeCheck.Models

{

    public class Category

    {

        public int Id { get; set; }

        public string Name { get; set; }

    }

}

**MenuItem.cs**

using System;

using System.Collections;

using System.Collections.Generic;

using System.ComponentModel.DataAnnotations.Schema;

using System.Linq;

using System.Threading.Tasks;

namespace PracticeCheck.Models

{

    public class MenuItem

    {

        public int Id { get; set; }

        public string Name { get; set; }

        public int Price { get; set; }

        public bool Active { get; set; }

        public DateTime DateOfLaunch { get; set; }

        [ForeignKey("Category")]

        public int CategoryId { get; set; }

        public string CategoryName { get; set; }

        public bool FreeDelivery { get; set; }

    }

}

**User.cs**

using System;

using System.Collections.Generic;

using System.Linq;

using System.Threading.Tasks;

namespace PracticeCheck.Models

{

    public class User

    {

        public int Id { get; set; }

        public string UserName { get; set; }

        public string FirstName { get; set; }

        public string LastName { get; set; }

        public string Password { get; set; }

        public string ConfirmPassword { get; set; }

    }

}

**MenuItemOperation.cs**

using PracticeCheck.Models;

using System;

using System.Collections.Generic;

using System.Data;

using System.Data.SqlClient;

using System.Linq;

using System.Threading.Tasks;

namespace PracticeCheck

{

    public class MenuItemOperation

    {

        public static string sqlDataSource = "Server=DESKTOP-B0SQG0N;Database=MenuItems;Trusted\_Connection=True;MultipleActiveResultSets=true;";

        //private List<string> list = new List<string>{ "Starter", "Main Course", "Drinks", "Dessert" };

        public static IEnumerable<MenuItem> GetConnection()

        {

            List<MenuItem> Items = new List<MenuItem>();

            var list = new List<string> { "Starter", "Main Course", "Drinks", "Dessert" };

            using (SqlConnection con = new SqlConnection(sqlDataSource))

            {

                con.Open();

                using (SqlCommand cmd = new SqlCommand())

                {

                    cmd.Connection = con;

                    cmd.CommandText = "select \* from MenuItem";

                    SqlDataReader rd = cmd.ExecuteReader();

                    while (rd.Read())

                    {

                        Items.Add(new MenuItem

                        {

                            Id = Convert.ToInt32(rd["Id"]),

                            Name = rd["Name"].ToString(),

                            Price = Convert.ToInt32(rd["Price"]),

                            Active = Convert.ToBoolean(rd["Active"]),

                            DateOfLaunch = Convert.ToDateTime(rd["DateOfLaunch"]),

                            CategoryId = Convert.ToInt32(rd["CategoryId"]),

                            CategoryName = list[Convert.ToInt32(rd["CategoryId"]) - 1].ToString(),

                            FreeDelivery = Convert.ToBoolean(rd["FreeDelivery"]),

                        }); ; ;

                    }

                    con.Close();

                }

                return Items;

            }

        }

        public static void Update(int id, MenuItem menuitem)

        {

            var list = new List<string> { "Starter", "Main Course", "Drinks", "Dessert" };

            using (SqlConnection con = new SqlConnection(sqlDataSource))

            {

                SqlCommand cmd = new SqlCommand("UpdateItem", con);

                cmd.CommandType = CommandType.StoredProcedure;

                cmd.Parameters.AddWithValue("@Id", id);

                cmd.Parameters.AddWithValue("@Name", menuitem.Name);

                cmd.Parameters.AddWithValue("@Price", menuitem.Price);

                cmd.Parameters.AddWithValue("@Active", menuitem.Active);

                cmd.Parameters.AddWithValue("@DateOfLaunch", menuitem.DateOfLaunch);

                cmd.Parameters.AddWithValue("@CategoryId", menuitem.CategoryId);

                cmd.Parameters.AddWithValue("@FreeDelivery", menuitem.FreeDelivery);

                con.Open();

                cmd.ExecuteNonQuery();

                con.Close();

            }

        }

        public static void Insert(User user)

        {

            SqlConnection con = new SqlConnection(sqlDataSource);

            SqlCommand sqlCmd = new SqlCommand();

            sqlCmd.CommandType = CommandType.Text;

            sqlCmd.CommandText = "INSERT INTO UserDetails(Id,UserName,FirstName,LastName,Password,ConfirmPassword) Values (@Id,@UserName,@FirstName,@LastName,@Password,@ConfirmPassword)";

            sqlCmd.Connection = con;

            sqlCmd.Parameters.AddWithValue("@Id", user.Id);

            sqlCmd.Parameters.AddWithValue("@UserName", user.UserName);

            sqlCmd.Parameters.AddWithValue("@FirstName", user.FirstName);

            sqlCmd.Parameters.AddWithValue("@LastName", user.LastName);

            sqlCmd.Parameters.AddWithValue("@Password", user.Password);

            sqlCmd.Parameters.AddWithValue("@ConfirmPassword", user.ConfirmPassword);

            con.Open();

            sqlCmd.ExecuteNonQuery();

            con.Close();

        }

        public static List<User>UserList()

        {

            List<User> users = new List<User>();

            using (SqlConnection con = new SqlConnection(sqlDataSource))

            {

                con.Open();

                using (SqlCommand cmd = new SqlCommand())

                {

                    cmd.Connection = con;

                    cmd.CommandText = "select \* from UserDetails";

                    SqlDataReader rd = cmd.ExecuteReader();

                    while (rd.Read())

                    {

                        users.Add(new User

                        {

                            Id = Convert.ToInt32(rd["Id"]),

                            UserName = rd["UserName"].ToString(),

                            FirstName = rd["FirstName"].ToString(),

                            LastName = rd["LastName"].ToString(),

                            Password = rd["Password"].ToString(),

                            ConfirmPassword = rd["ConfirmPassword"].ToString()

                        });

                    }

                    con.Close();

                }

            }

            return users;

        }

        public static void InsertIntoCart(List<Cart> cart)

        {

            SqlConnection con = new SqlConnection(sqlDataSource);

            SqlCommand sqlCmd = new SqlCommand();

            sqlCmd.CommandType = CommandType.Text;

            sqlCmd.CommandText = "INSERT INTO Cart(Id,MenuItemId,UserId) Values (@Id,@MenuItemId,@UserId)";

            sqlCmd.Connection = con;

            con.Open();

            foreach (var i in cart)

            {

                sqlCmd.Parameters.AddWithValue("@Id", i.Id);

                sqlCmd.Parameters.AddWithValue("@MenuItemId", i.MenuItemId);

                sqlCmd.Parameters.AddWithValue("@UserId", i.UserId);

                sqlCmd.ExecuteNonQuery();

                sqlCmd.Parameters.Clear();

            }

             con.Close();

        }

        public static List<MenuItem> CartList(int userid,ref int totalprice)

        {

            List<MenuItem> Items = new List<MenuItem>();

            List<int> list = new List<int>();

            var l = new List<string> { "Starter", "Main Course", "Drinks", "Dessert" };

            using (SqlConnection con = new SqlConnection(sqlDataSource))

            {

                con.Open();

                using (SqlCommand cmd = new SqlCommand())

                {

                    cmd.Connection = con;

                    cmd.CommandText = "select MenuItemId from Cart where Userid = @userid";

                    cmd.Parameters.AddWithValue("@userid",userid);

                    SqlDataReader rd = cmd.ExecuteReader();

                     while (rd.Read())

                     {

                         list.Add(Convert.ToInt32(rd["MenuItemId"]));

                     }

                    rd.Close();

                      foreach (var i in list)

                      {

                       cmd.CommandText = "select \* from MenuItem where Id = @i";

                       cmd.Parameters.AddWithValue("@i", i);

                       SqlDataReader rd1 = cmd.ExecuteReader();

                        while (rd1.Read())

                         {

                             Items.Add(new MenuItem

                             {

                                 Id = Convert.ToInt32(rd1["Id"]),

                                 Name = rd1["Name"].ToString(),

                                 Price = Convert.ToInt32(rd1["Price"]),

                                 Active = Convert.ToBoolean(rd1["Active"]),

                                 DateOfLaunch = Convert.ToDateTime(rd1["DateOfLaunch"]),

                                 CategoryId = Convert.ToInt32(rd1["CategoryId"]),

                                 CategoryName = l[Convert.ToInt32(rd1["CategoryId"]) - 1].ToString(),

                                 FreeDelivery = Convert.ToBoolean(rd1["FreeDelivery"]),

                         });

                           totalprice += Convert.ToInt32(rd1["Price"]);

                         }

                        cmd.Parameters.Clear();

                        rd1.Close();

                    }

                    con.Close();

                 }

             }

            return Items;

        }

        public static string Delete(int cartid)

        {

            SqlConnection con = new SqlConnection(sqlDataSource);

            SqlCommand sqlCmd = new SqlCommand();

            sqlCmd.CommandType = CommandType.Text;

            sqlCmd.CommandText = "delete from Cart where Id =@cartid";

            sqlCmd.Connection = con;

            con.Open();

            sqlCmd.Parameters.AddWithValue("@cartid",cartid);

            int i = sqlCmd.ExecuteNonQuery();

            if (i >= 1)

                return "record deleted";

            else

                return "no record";

        }

    }

}

**Program.cs**

using System;

using System.Collections.Generic;

using System.Linq;

using System.Threading.Tasks;

using Microsoft.AspNetCore.Hosting;

using Microsoft.Extensions.Configuration;

using Microsoft.Extensions.Hosting;

using Microsoft.Extensions.Logging;

namespace PracticeCheck

{

    public class Program

    {

        public static void Main(string[] args)

        {

            CreateHostBuilder(args).Build().Run();

        }

        public static IHostBuilder CreateHostBuilder(string[] args) =>

            Host.CreateDefaultBuilder(args)

                .ConfigureWebHostDefaults(webBuilder =>

                {

                    webBuilder.UseStartup<Startup>();

                });

    }

}

**Startup.cs**

using System;

using System.Collections.Generic;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

using Microsoft.AspNetCore.Authentication.JwtBearer;

using Microsoft.AspNetCore.Builder;

using Microsoft.AspNetCore.Hosting;

using Microsoft.AspNetCore.HttpsPolicy;

using Microsoft.AspNetCore.Mvc;

using Microsoft.Extensions.Configuration;

using Microsoft.Extensions.DependencyInjection;

using Microsoft.Extensions.Hosting;

using Microsoft.Extensions.Logging;

using Microsoft.IdentityModel.Tokens;

using Microsoft.OpenApi.Models;

namespace PracticeCheck

{

    public class Startup

    {

        public Startup(IConfiguration configuration)

        {

            Configuration = configuration;

        }

        public IConfiguration Configuration { get; }

        // This method gets called by the runtime. Use this method to add services to the container.

        public void ConfigureServices(IServiceCollection services)

        {

            services.AddControllers();

            services.AddSwaggerGen(c =>

            {

                c.SwaggerDoc("v1", new OpenApiInfo

                {

                    Title = "Swagger Demo",

                    Version = "v1",

                    Description = "TBD",

                    TermsOfService = new Uri("https://www.example.com"),

                    Contact = new OpenApiContact() { Name = "John Doe", Email = "john@xyzmail.com", Url = new Uri("https://www.example.com") },

                    License = new OpenApiLicense() { Name = "License Terms", Url = new Uri("https://www.example.com") }

                });

            });

            string securityKey = "mysuperdupersecret";

            var symmetricSecurityKey = new SymmetricSecurityKey(Encoding.UTF8.GetBytes(securityKey));

            services.AddAuthentication(x =>

            {

                x.DefaultAuthenticateScheme = JwtBearerDefaults.AuthenticationScheme;

                x.DefaultChallengeScheme = JwtBearerDefaults.AuthenticationScheme;

                x.DefaultSignInScheme = JwtBearerDefaults.AuthenticationScheme;

            })

          .AddJwtBearer(JwtBearerDefaults.AuthenticationScheme, x =>

          {

              x.TokenValidationParameters = new TokenValidationParameters

              {

                    //what to validate

                  ValidateIssuer = true,

                  ValidateAudience = true,

                  ValidateLifetime = true,

                  ValidateIssuerSigningKey = true,

                  ClockSkew = TimeSpan.FromSeconds(1),

                    //setup validate data

                  ValidIssuer = "mySystem",

                  ValidAudience = "myUsers",

                  IssuerSigningKey = symmetricSecurityKey

              };

          });

        }

        // This method gets called by the runtime. Use this method to configure the HTTP request pipeline.

        public void Configure(IApplicationBuilder app, IWebHostEnvironment env)

        {

            if (env.IsDevelopment())

            {

                app.UseDeveloperExceptionPage();

            }

            app.UseSwagger();

            app.UseSwaggerUI(c =>

            {

                // specifying the Swagger JSON endpoint.

                c.SwaggerEndpoint("/swagger/v1/swagger.json", "Swagger Demo");

            });

            app.UseHttpsRedirection();

            app.UseRouting();

            app.UseAuthentication();

            app.UseAuthorization();

            app.UseEndpoints(endpoints =>

            {

                endpoints.MapControllers();

            });

        }

    }

}

**OUTPUT:**





