**Hands On 8: Authorize based on JWT**

**CountryController.java**

package com.example.demo.controller;  
  
import org.springframework.web.bind.annotation.GetMapping;  
import org.springframework.web.bind.annotation.RestController;  
  
import java.util.ArrayList;  
import java.util.List;  
import java.util.Map;  
  
@RestController  
public class CountryController {  
  
 @GetMapping("/countries")  
 public List<Map<String, String>> getCountries() {  
 List<Map<String, String>> countries = new ArrayList<>();  
 countries.add(Map.*of*("code", "US", "name", "United States"));  
 countries.add(Map.*of*("code", "DE", "name", "Germany"));  
 countries.add(Map.*of*("code", "IN", "name", "India"));return countries;  
 }  
}

**JwtAuthFilter.java**

package com.example.demo.security;  
  
import java.io.IOException;  
import java.util.ArrayList;  
  
import jakarta.servlet.FilterChain;  
import jakarta.servlet.ServletException;  
import jakarta.servlet.http.HttpServletRequest;  
import jakarta.servlet.http.HttpServletResponse;  
  
import io.jsonwebtoken.Claims;  
import io.jsonwebtoken.Jws;  
import io.jsonwebtoken.JwtException;  
import io.jsonwebtoken.Jwts;  
  
import org.slf4j.Logger;  
import org.slf4j.LoggerFactory;  
  
import org.springframework.security.authentication.UsernamePasswordAuthenticationToken;  
import org.springframework.security.core.context.SecurityContextHolder;  
import org.springframework.security.web.authentication.www.BasicAuthenticationFilter;  
import org.springframework.security.authentication.AuthenticationManager;  
  
public class JwtAuthFilter extends BasicAuthenticationFilter {  
  
 private static final Logger *LOGGER* = LoggerFactory.*getLogger*(JwtAuthFilter.class);  
  
 public JwtAuthFilter(AuthenticationManager authenticationManager) {  
 super(authenticationManager);  
 *LOGGER*.info("JwtAuthFilter initialized");  
 }  
  
 @Override  
 protected void doFilterInternal(HttpServletRequest request, HttpServletResponse response,  
 FilterChain chain) throws IOException, ServletException {  
 String header = request.getHeader("Authorization");  
 *LOGGER*.debug("Authorization header: {}", header);  
  
 if (header == null || !header.startsWith("Bearer ")) {  
 chain.doFilter(request, response);  
 return;  
 }  
  
 UsernamePasswordAuthenticationToken authentication = getAuthentication(request);  
  
 SecurityContextHolder.*getContext*().setAuthentication(authentication);  
 chain.doFilter(request, response);  
 }  
  
 private UsernamePasswordAuthenticationToken getAuthentication(HttpServletRequest request) {  
 String token = request.getHeader("Authorization");  
 if (token != null) {  
 try {  
 Jws<Claims> jws = Jwts.*parser*()  
 .setSigningKey("ThisIsASecretKeyUsedToSignAndVerifyJWTsWithHmacSha256ItMustBeLongEnoughToProvideSecurityAndAvoidWarningsOrExceptionsRelatedToKeyLengthEspeciallyWhenUsingStrongEncryptionAlgorithmsInProduction")  
 .parseClaimsJws(token.replace("Bearer ", ""));  
  
 String user = jws.getBody().getSubject();  
 *LOGGER*.debug("User from JWT: {}", user);  
  
 if (user != null) {  
 return new UsernamePasswordAuthenticationToken(user, null, new ArrayList<>());  
 }  
 } catch (JwtException ex) {  
 *LOGGER*.error("Invalid JWT token", ex);  
 }  
 }  
 return null;  
 }  
}

**AuthController.java**

package com.example.demo.controller;  
  
import io.jsonwebtoken.JwtBuilder;  
import io.jsonwebtoken.Jwts;  
import io.jsonwebtoken.SignatureAlgorithm;  
import org.slf4j.Logger;  
import org.slf4j.LoggerFactory;  
import org.springframework.web.bind.annotation.\*;  
  
import java.util.Base64;  
import java.util.Date;  
import java.util.HashMap;  
import java.util.Map;  
  
@RestController  
public class AuthController {  
  
 private static final Logger *LOGGER* = LoggerFactory.*getLogger*(AuthController.class);  
  
 @GetMapping("/authenticate")  
 public Map<String, String> authenticate(@RequestHeader("Authorization") String authHeader) {  
 *LOGGER*.info("Start of authenticate()");  
 *LOGGER*.debug("Authorization header: {}", authHeader);  
  
 String user = getUser(authHeader);  
 *LOGGER*.debug("Extracted user from header: {}", user);  
  
 String token = generateJwt(user);  
 *LOGGER*.debug("Generated token: {}", token);  
  
 Map<String, String> map = new HashMap<>();  
 map.put("token", token);  
  
 *LOGGER*.info("End of authenticate()");  
 return map;  
 }  
  
 private String getUser(String authHeader) {  
 String encodedCredentials = authHeader.substring("Basic ".length());  
 byte[] decodedBytes = Base64.*getDecoder*().decode(encodedCredentials);  
 String decodedString = new String(decodedBytes);  
 return decodedString.split(":")[0];  
 }  
  
 private String generateJwt(String user) {  
 JwtBuilder builder = Jwts.*builder*();  
 builder.setSubject(user);  
 builder.setIssuedAt(new Date());  
 builder.setExpiration(new Date(new Date().getTime() + 20 \* 60 \* 1000));  
 builder.signWith(SignatureAlgorithm.*HS256*, "ThisIsASecretKeyUsedToSignAndVerifyJWTsWithHmacSha256ItMustBeLongEnoughToProvideSecurityAndAvoidWarningsOrExceptionsRelatedToKeyLengthEspeciallyWhenUsingStrongEncryptionAlgorithmsInProduction");  
 return builder.compact();  
 }  
}

**SecurityConfig.java**

package com.example.demo.security;  
  
import org.springframework.context.annotation.Bean;  
import org.springframework.context.annotation.Configuration;  
import org.springframework.security.config.annotation.web.configuration. EnableWebSecurity;  
import org.springframework.security.config.annotation.web.builders.HttpSecurity;  
import org.springframework.security.web.SecurityFilterChain;  
import org.springframework.security.core.userdetails.User;  
import org.springframework.security.core.userdetails.UserDetails;  
import org.springframework.security.provisioning.InMemoryUserDetailsManager;  
import org.springframework.security.crypto.password.PasswordEncoder;  
import org.springframework.security.crypto.password.NoOpPasswordEncoder;  
  
@Configuration  
@EnableWebSecurity  
public class SecurityConfig {  
  
 @Bean  
 public InMemoryUserDetailsManager userDetailsService() {  
 UserDetails user = User.*withUsername*("user")  
 .password("pwd")  
 .roles("USER")  
 .build();  
  
 UserDetails admin = User.*withUsername*("admin")  
 .password("pwd")  
 .roles("ADMIN")  
 .build();  
  
 return new InMemoryUserDetailsManager(user, admin);  
 }  
  
 @Bean  
 public PasswordEncoder passwordEncoder() {  
 return NoOpPasswordEncoder.*getInstance*();}  
  
 @Bean  
 public SecurityFilterChain securityFilterChain(HttpSecurity http) throws Exception {  
 http  
 .csrf(csrf -> csrf.disable())  
 .authorizeHttpRequests(auth -> auth  
 .requestMatchers("/countries").hasRole("USER")  
 .requestMatchers("/authenticate").hasAnyRole("USER", "ADMIN")  
 .anyRequest().authenticated()  
 )  
 .httpBasic(customizer -> {});  
  
 return http.build();  
 }  
}

**DemoApplication.java**

package com.example.demo;  
import org.springframework.boot.SpringApplication;  
import org.springframework.boot.autoconfigure.SpringBootApplication;  
  
@SpringBootApplication  
public class DemoApplication {  
  
 public static void main(String[] args) {  
 SpringApplication.*run*(DemoApplication.class, args);  
 }  
  
}

**Output**





