**AuthController – Get Profile**

**In AuthController.java -> add this below code**

@GetMapping(value = "/profile", produces = "application/json")

    @Operation(summary = "View Profile")

    @ApiResponse(responseCode = "200", description = "List of users")

    @ApiResponse(responseCode = "401", description = "Token missing")

    @ApiResponse(responseCode = "403", description = "Token error")

    @SecurityRequirement(name = "studyeasy-demo-api")

    public ProfileDTO profile(Authentication authentication){

        String email = authentication.getName();

        Optional<Account> optionalAccount = accountService.findByEmail(email);

        if(optionalAccount.isPresent()){

            Account account = optionalAccount.get();

            ProfileDTO profileDTO = new ProfileDTO(account.getId(), account.getEmail(), account.getAuthorities());

            return profileDTO;

        }

        return null;

    }

**Create a DTO -> in payload -> ProfileDTO.java**

package org.studyeasy.SpringRestdemo.payload.auth;

import lombok.AllArgsConstructor;

import lombok.Getter;

import lombok.Setter;

@Setter

@Getter

@AllArgsConstructor

public class ProfileDTO {

    private long id;

    private String email;

    private String authorities;

}

**In AccountService.java -> add this below code**

public Optional<Account> findByEmail(String email){

        return accountRepository.findByEmail(email);

    }

**In SecurityConfig.java -> add below line**

.requestMatchers("/auth/profile").authenticated()

**Updated SecurityConfig.java**

package org.studyeasy.SpringRestdemo.security;

import org.springframework.context.annotation.Bean;

import org.springframework.context.annotation.Configuration;

import org.springframework.security.authentication.AuthenticationManager;

import org.springframework.security.authentication.ProviderManager;

import org.springframework.security.authentication.dao.DaoAuthenticationProvider;

import org.springframework.security.config.Customizer;

import org.springframework.security.config.annotation.web.builders.HttpSecurity;

import org.springframework.security.config.annotation.web.configuration.EnableWebSecurity;

import org.springframework.security.config.http.SessionCreationPolicy;

import org.springframework.security.core.userdetails.UserDetailsService;

import org.springframework.security.crypto.bcrypt.BCryptPasswordEncoder;

import org.springframework.security.crypto.password.PasswordEncoder;

import org.springframework.security.oauth2.jwt.JwtDecoder;

import org.springframework.security.oauth2.jwt.JwtEncoder;

import org.springframework.security.oauth2.jwt.NimbusJwtDecoder;

import org.springframework.security.oauth2.jwt.NimbusJwtEncoder;

import org.springframework.security.web.SecurityFilterChain;

import com.nimbusds.jose.JOSEException;

import com.nimbusds.jose.jwk.JWKSet;

import com.nimbusds.jose.jwk.RSAKey;

import com.nimbusds.jose.jwk.source.JWKSource;

import com.nimbusds.jose.proc.SecurityContext;

@Configuration

@EnableWebSecurity

public class SecurityConfig {

    private RSAKey rsaKey;

    @Bean

    public JWKSource<SecurityContext> jwkSource() {

        rsaKey = Jwks.generateRsa();

        JWKSet jwkSet = new JWKSet(rsaKey);

        return (jwkSelector, securityContext) -> jwkSelector.select(jwkSet);

    }

    @Bean

    public static PasswordEncoder passwordEncoder() {

        return new BCryptPasswordEncoder();

    }

    // @Bean

    // public InMemoryUserDetailsManager users() {

    // return new InMemoryUserDetailsManager(

    // User.withUsername("chaand")

    // .password("{noop}password")

    // .authorities("read")

    // .build());

    // }

    @Bean

    public AuthenticationManager authManager(UserDetailsService userDetailsService) {

        var authProvider = new DaoAuthenticationProvider();

        authProvider.setPasswordEncoder(passwordEncoder());

        authProvider.setUserDetailsService(userDetailsService);

        return new ProviderManager(authProvider);

    }

    @Bean

    JwtEncoder jwtEncoder(JWKSource<SecurityContext> jwks) {

        return new NimbusJwtEncoder(jwks);

    }

    @Bean

    JwtDecoder jwtDecoder() throws JOSEException {

        return NimbusJwtDecoder.withPublicKey(rsaKey.toRSAPublicKey()).build();

    }

    @Bean

    public SecurityFilterChain securityFilterChain(HttpSecurity http) throws Exception {

        http

                // CSRF configuration

                .csrf(csrf -> csrf

                        .disable()) // Disable CSRF for stateless JWT authentication

                // Frame options for H2 console

                .headers(headers -> headers

                        .frameOptions(frameOptions -> frameOptions.sameOrigin()))

                // Authorization configuration

                .authorizeHttpRequests(authorize -> authorize

                        .requestMatchers("/auth/token").permitAll()

                        .requestMatchers("/auth/users/add").permitAll()

                        .requestMatchers("/auth/users").hasAnyAuthority("SCOPE\_ADMIN")

                        .requestMatchers("/auth/profile").authenticated()

                        .requestMatchers("/swagger-ui/\*\*").permitAll()

                        .requestMatchers("/v3/api-docs/\*\*").permitAll()

                        .requestMatchers("/test").authenticated() // `/test` requires authentication

                )

                // JWT-based authentication

                .oauth2ResourceServer(oauth2 -> oauth2

                        .jwt(Customizer.withDefaults()))

                // Stateless session management

                .sessionManagement(session -> session

                        .sessionCreationPolicy(SessionCreationPolicy.STATELESS))

                .headers(headers -> headers

                        .frameOptions(frameOptions -> frameOptions.sameOrigin())); // Required for H2 console

        return http.build();

    }

}

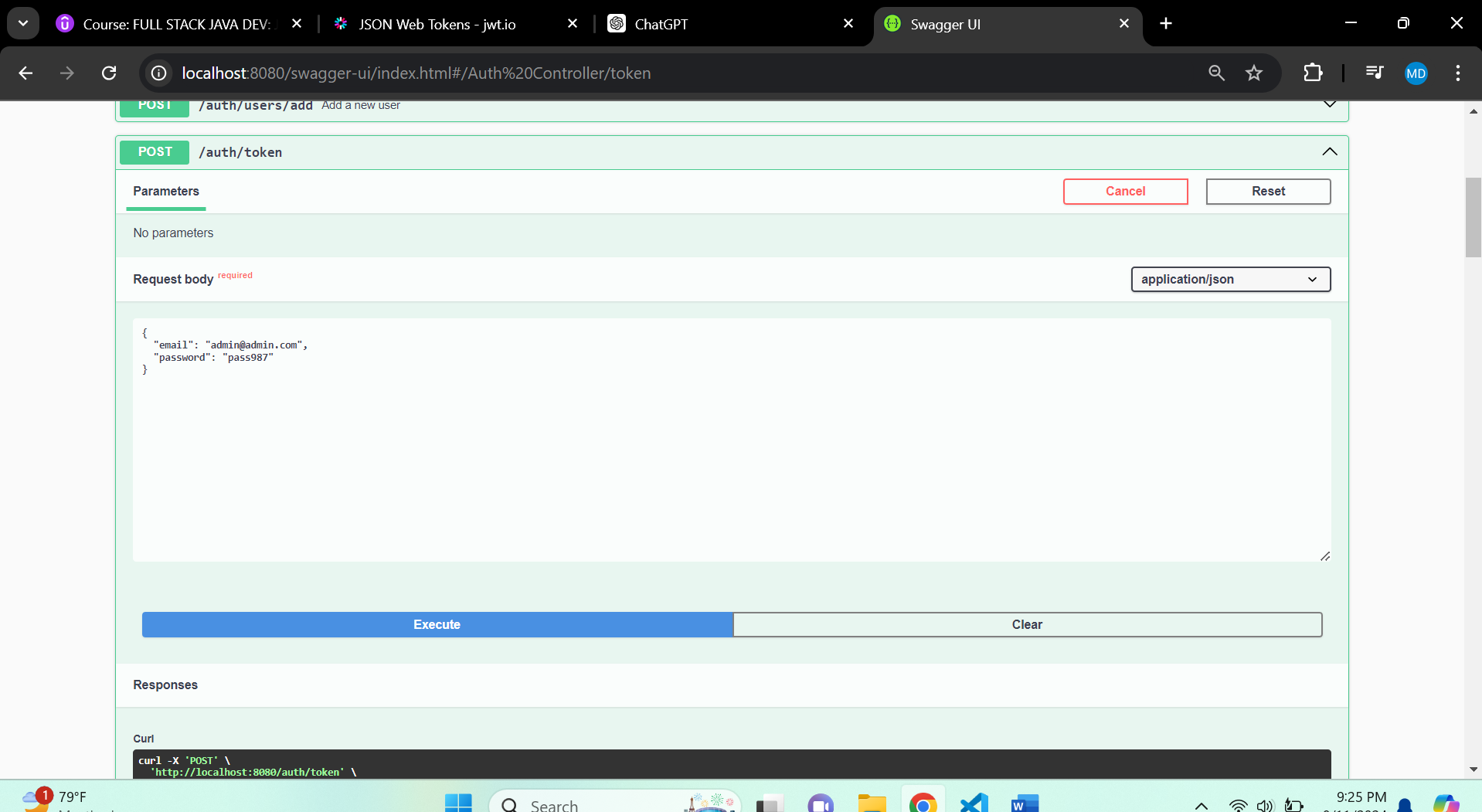
**Output**

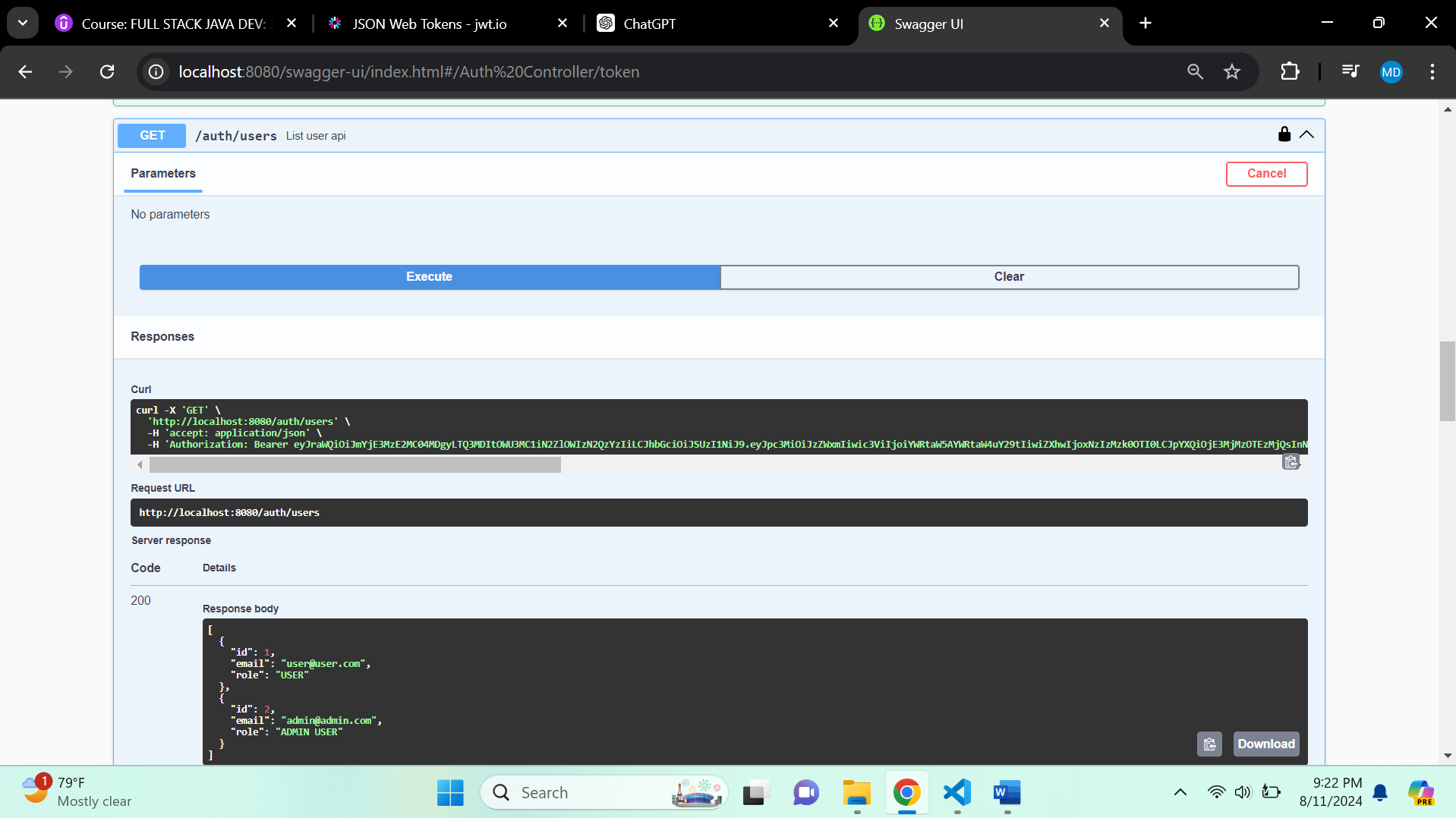
**If you try to access list of users or view profile directly, you get error (401).**

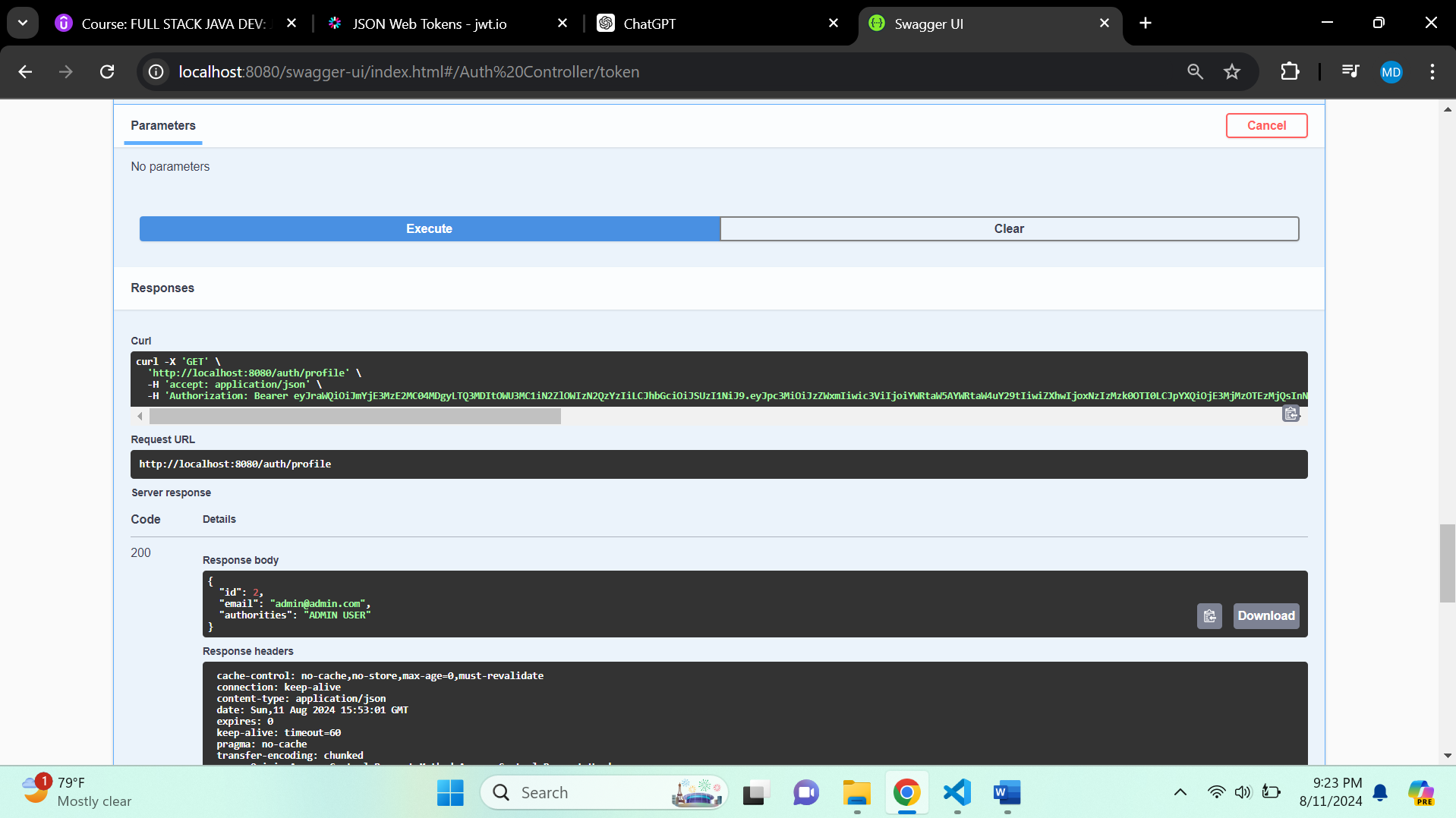
**If you try generating token and then access as Admin, you get list of data and profile.**

**If you try generating token and then access as User, you will not get list of data, but you will get profile.**

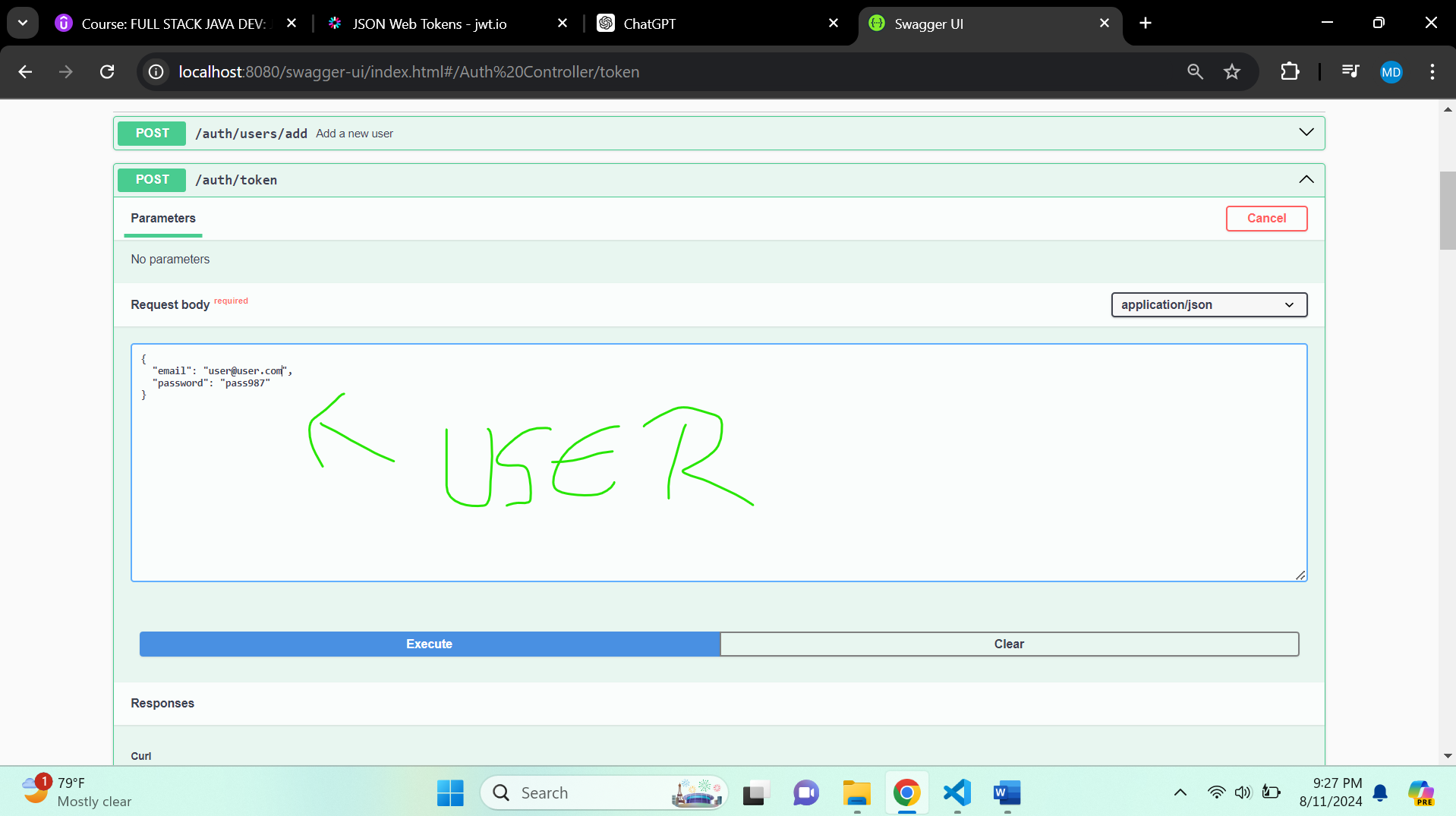
**ADMIN**

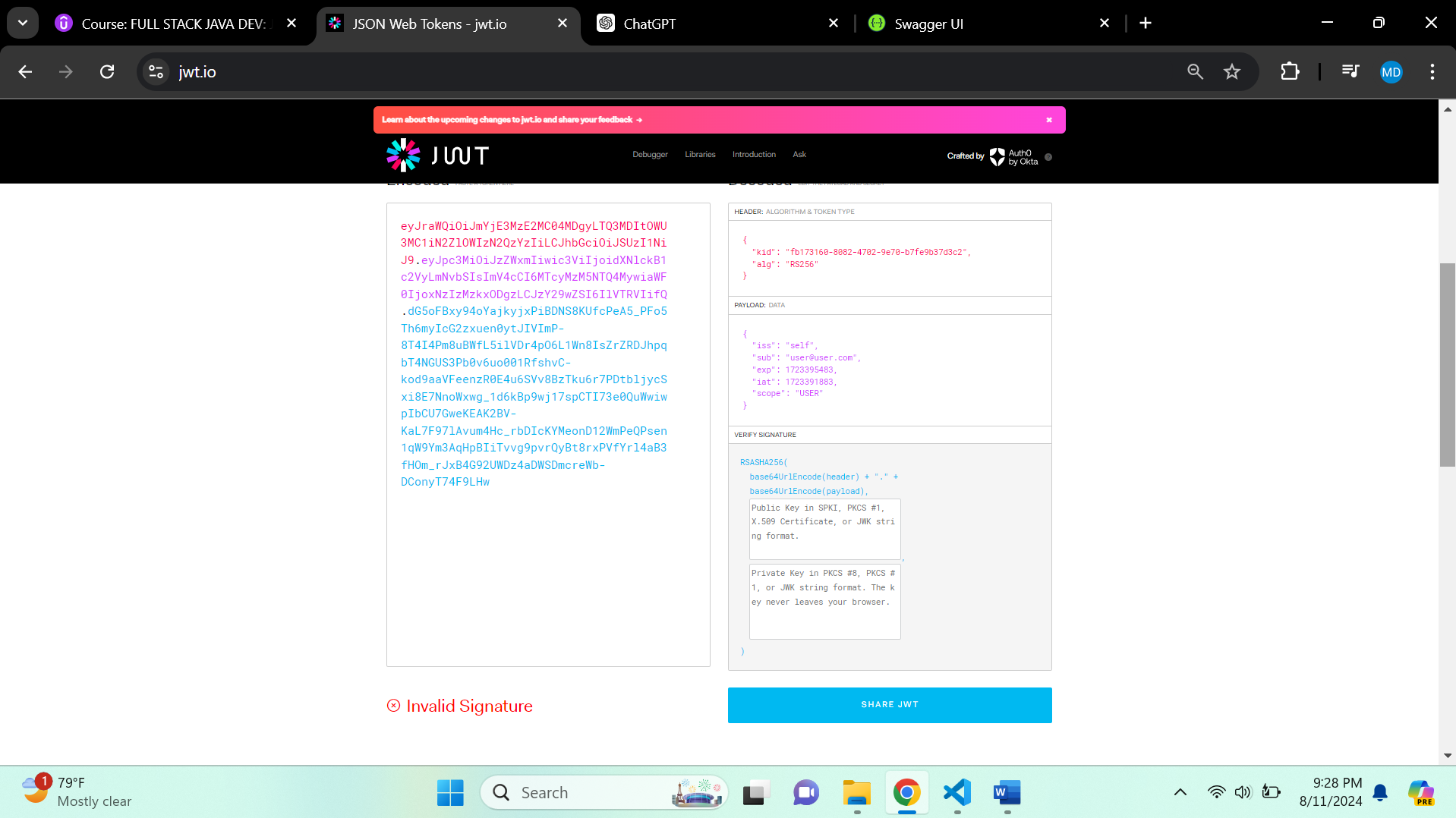
****

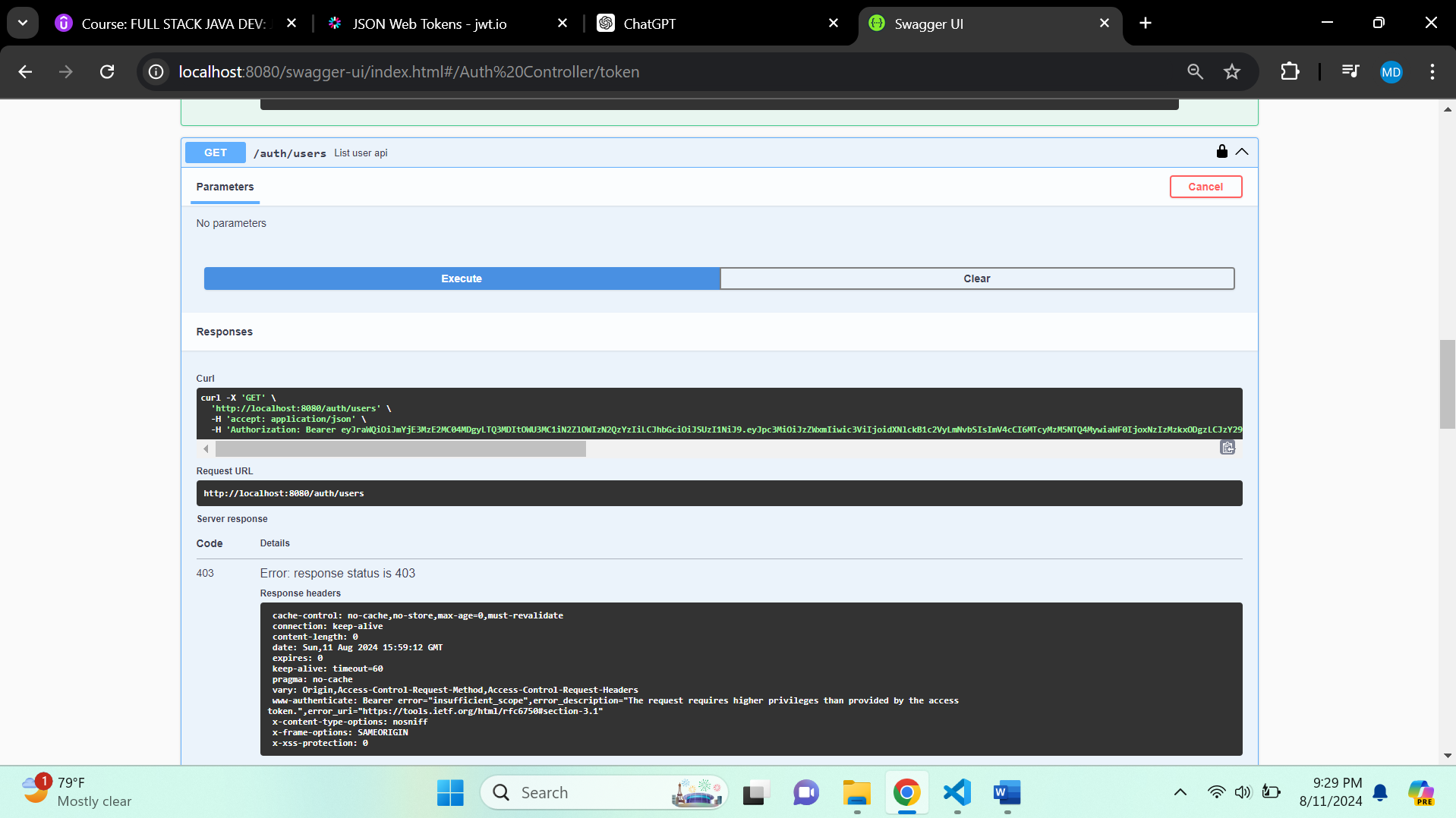
****

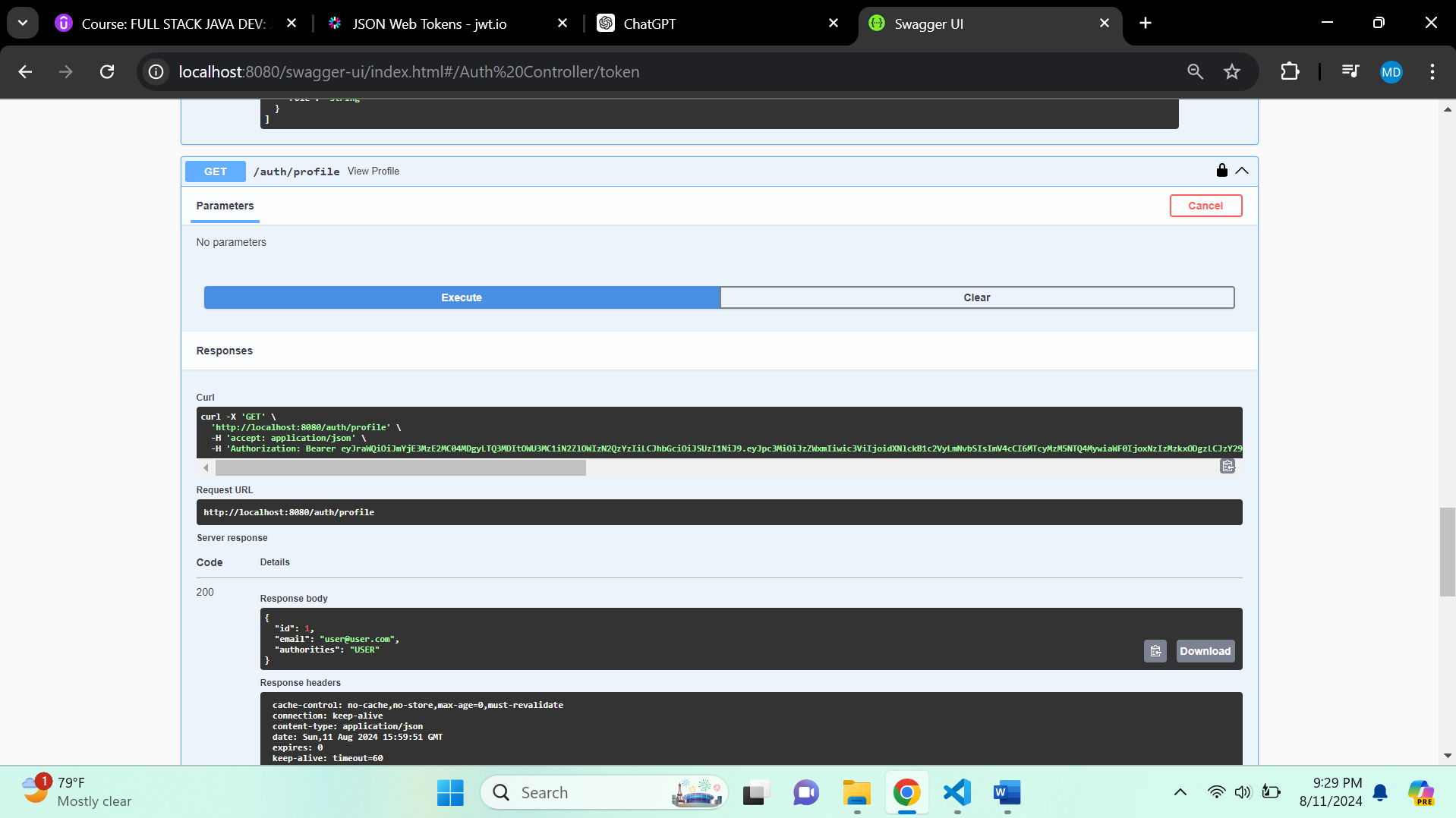
****

**USER**

****

****

****

****