Enable CORS

Cross-Origin Resource Sharing (CORS) is a security policy that uses HTTP concept that allows restricting the resources implemented in web browsers. It prevents the JavaScript code producing or consuming the requests against different origin.

Spring Boot CORS

The following Spring Boot application uses Angular for the frontend. The Angular SPA is run on localhost:4200 and makes a request to the Spring Boot backend, which runs on localhost:8080. For this to work, we need to enable CORS in the Spring Boot application.

A web page can embed cross-origin images, stylesheets, scripts, iframes, and videos. Some cross-domain requests, notably Ajax requests, are forbidden by default by the same-origin security policy.

Global CORS Configuration in Spring Boot main class

```
@SpringBootApplication
public class MyApplication {
   public static void main(String[] args) {
      SpringApplication.run(MyApplication.class, args);
   }
   @Bean
   public WebMvcConfigurer corsConfigurer() {
      return new WebMvcConfigurerAdapter(){
         @Override
        public void addCorsMappings(CorsRegistry registry) {
                CorsRegistration cors = registry.addMapping("/**");
                cors.allowedOrigins("http://localhost:4200");
                cors.allowedHeaders("*");
                cors.allowCredentials(true);
        }
      };
   }
}
```