```java
package app.security;

import org.springframework.context.annotation.Bean;
import org.springframework.context.annotation.Configuration;
import org.springframework.http.HttpMethod;
import org.springframework.security.config.annotation.method.configuration.EnableMethodSecurity;
import org.springframework.security.config.annotation.web.builders.HttpSecurity;
import org.springframework.security.web.SecurityFilterChain;

@Configuration
//@EnableMethodSecurity
public class MySecurityConfiguration {
        @Bean
        public SecurityFilterChain filterChain(HttpSecurity http) throws Exception {
            // Anyone can access /all
            http.authorizeHttpRequests().requestMatchers("/all/**").permitAll();

            // Only admins can access /admin
            http.authorizeHttpRequests().requestMatchers("/admin/**").hasRole("ADMIN");

            //http.authorizeHttpRequests().requestMatchers(HttpMethod.DELETE, "/admin/**").denyAll();

            // Needs authentication
            http.authorizeHttpRequests().anyRequest().authenticated();


            http.httpBasic();
            //http.formLogin();

            http.csrf().disable();

            return http.build();
        }
}
```