Spring Security

Petr Křemen, Bogdan Kostov

petr.kremen@fel.cvut.cz, bogdan.kostov@fel.cvut.cz

Winter Term 2018

Contents

Spring Security

Spring Security

Spring security offers the following annotations:

`@PreFilter` for filtering input list based on security constraints expressed in SpEL.

`@PostFilter` for filtering output list based on security constraints expressed in SpEL.

`@PreAuthorize` for authorizing method execution based on security constraints expressed in SpEL.

`@PostAuthorize` for authorizing return from the method execution based on security constraints expressed in SpEL.

Spring Security - SpEL

Relevant SpEL expressions:

`hasRole('ADMIN')` checks whether the currently logged in user has the 'ADMIN'

`and, or` logical operators

`principal` the currently logged in user, `principal.username`

`filterObject` the object filtered from the collection, e.g. filterObject.customer

Become familiar with these annotations (EAR lectures, Spring web) before starting the following tasks. Refer to the Spring web pages [1] and [2] for details.

Tasks

Task 1 – 1 point

Check out branch *b181-seminar-10-task* of the e-shop project (`https://gitlab.fel.cvut.cz/ear/b181-eshop`).
Fix the project. Hints - maven dependencies, security related beans necessary to build the spring application context.

Acceptance criteria:

- the code is compilable
- tests in the package cz.cvut.kbss.ear.eshop.security should pass

Task 2 – 1 point

Implement method security on methods in the service layer. Search for TODOs.

- Method `UserService.deleteUser` is accessible only by the administrator.
- Method `OrderService.findAll` should return only the orders of the current user or all orders if the current user has the ROLE_ADMIN.

Acceptance criteria:

- tests in cz.cvut.kbss.ear.eshop.service.SecurityTest.java should pass.

References


Spring Expression Language. Spring. https://docs.spring.io/spring/docs/4.3.12.RELEASE/spring-framework-reference/html/expressions.html


Expression-Based Access Control. Spring. https://docs.spring.io/spring-security/site/docs/3.0.x/reference/el-access.html


EAR Seminars. https://cw.fel.cvut.cz/wiki/courses/ear/seminars