**Spring Security**

1. **Spring security: Authentication và Authorization**
2. **Spring security là gì?**

- Một tính năng cốt lõi của spring framework: quản lý phân quyền và xác thực người dùng, hỗ trợ các tiêu chuẩn và giao thức bảo mật.

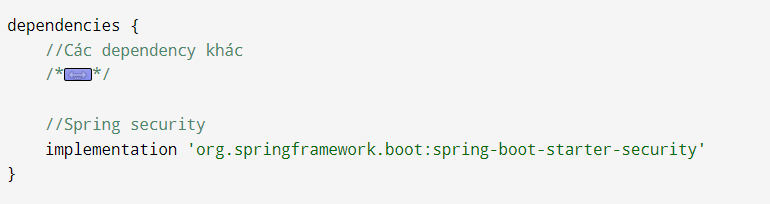
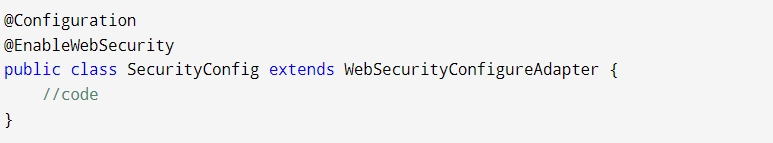
- Tính năng nâng cao: CSRF protection, quản lý phiên, mã hóa mật khẩu,...

- Cơ chế hoạt động:

* Theo mô hình client-server.
* Dựa trên cơ chế lọc và sự kiện để can thiệp quá trình xử lý yêu cầu và phản hồi.

- Thành phần cơ bản: Authentication, Authorization, Authentication Provider.

- Bắt đầu với Spring Security:

* Thêm các phụ thuộc cần thiết: **spring-boot-starter-security** 
* Kích hoạt Spring Security với annotation **@EnableWebSecurity**: 

1. **Authentication trong Spring security**

- Quá trình xác thực xem người dùng là ai.

- Authentication dựa trên các thông tin nhận dạng và thông tin bí mật. Ví dụ: tài khoản và mật khẩu, vân tay,...

- Spring security hỗ trợ xác thực thông qua:

* Form/Trang đăng nhập
* Các header authorization
* Các giá trị được máy khách cung cấp

- Spring security hỗ trợ cả trạng thái và phi trạng thái.

* **Trạng thái (Stateful)**: Lưu thông tin xác thực trong một phiên trên máy chủ. Máy chủ kiểm tra phiên hiện tại để xác định danh tính và quyền hạn mà không yêu cầu đăng nhập lại.
* **Phi trạng thái (Stateless)**: Máy chủ không lưu bất kỳ thông tin xác thực nào của người dùng mà chỉ sử dụng các mã token đã được đăng ký để xác thực.

1. **Authorization trong Spring security**

- Quá trình xác thực xem người dùng được làm gì hoặc được truy cập loại tài nguyên nào.

- Authorization dựa trên các thông tin về vai trò, nhóm, quyền hạn, chính sách.

- Spring security hỗ trợ xác thực bằng cách sử dụng các annotation hoặc XML. Các thành phần gồm:

* AccessDecisionManager
* AccessDecisionVoter
* SecurityExpressionHandler

1. **Authentication Provider**

- Thành phần trong Spring security chịu trách nhiệm xác minh thông tin xác thực của người dùng.

- Mỗi Authentication Provider chỉ hỗ trợ một loại authentication cụ thể như: UsernamePasswordAuthenticationToken, JwtAuthenticationToken, PreAuthenticatedAuthenticationToken,...