TRƯỜNG ĐẠI HỌC VĂN LANG
KHOA CÔNG NGHỆ THÔNG TIN

LẬP TRÌNH JAVA NÂNG CAO

CHƯƠNG 8: Spring Security

Giảng Viên Giảng Dạy:
ThS. Nguyễn Minh Tân
ThS. Đặng Đình Hòa
ThS. Trần Công Thanh

HỌC KỲ III – NĂM HỌC 2023-2024

KHÓA 27T-IT

Nội dung

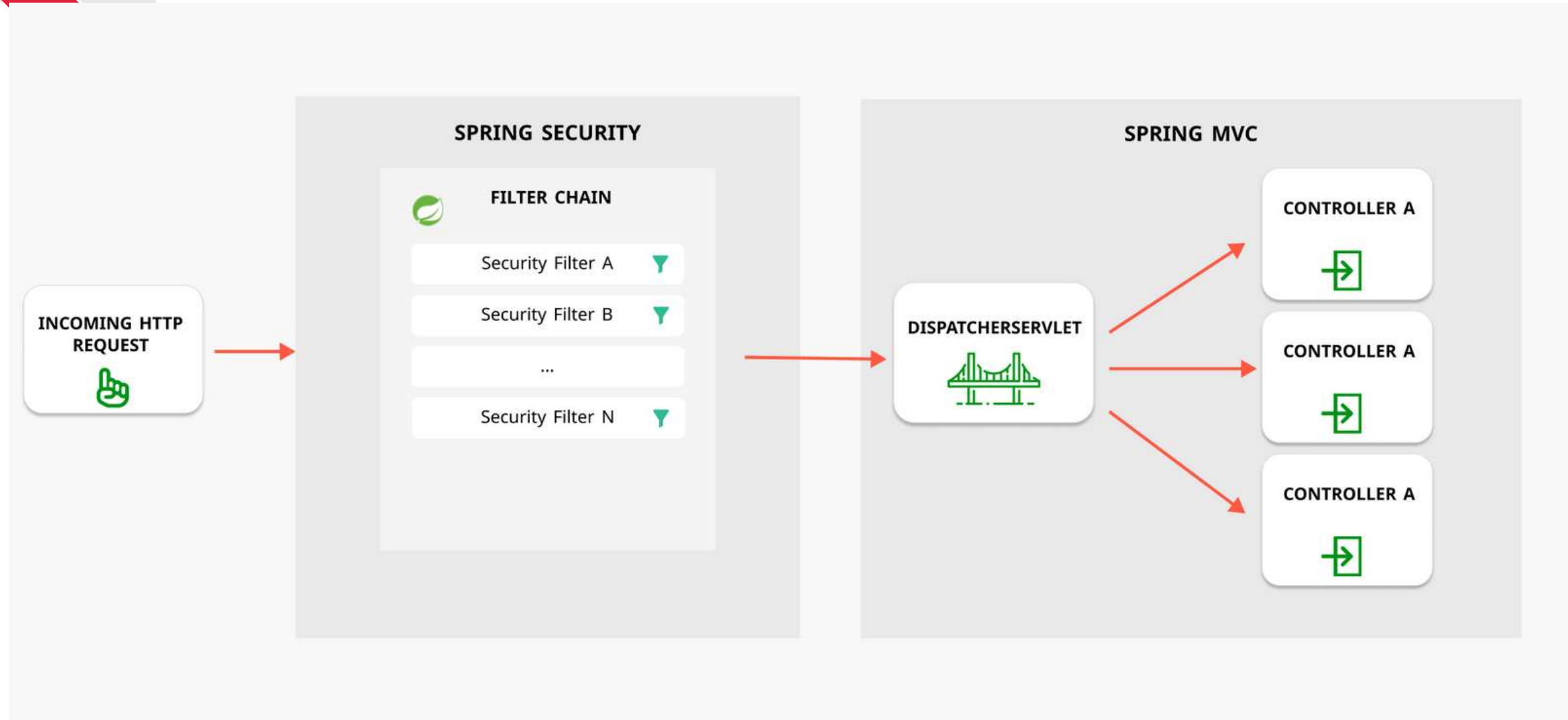
1. Giới thiệu Spring Security
2. Cơ chế hoạt động Spring Security
3. Các thành phần của Spring Security
4. Ưu và nhược điểm của Spring Security
5. Q & A

Tổng quan về Security

Spring Security là gì ?

- Spring Security là một framework phổ biến của Spring được sử dụng để xác thực và phân quyền cho các ứng dụng Java.
- Spring Security cung cấp các tính năng xác thực (authentication) và phân quyền (authorization) cho các ứng dụng, cũng như hỗ trợ các tiêu chuẩn và giao thức bảo mật như HTTPS, OAuth2, JWT, LDAP, SAML, OpenID Connect.

Cơ chế hoạt động Spring Security Filter Chain



Các thành phần trong Spring Security

- **Authentication là gì? Who are you ?**
- **Authorization là gì? What can I do ?**

Authentication là gì? (Xác thực) - Who are you ?

- Authentication là quá trình xác thực xem người dùng có quyền truy cập vào ứng dụng hay không. Khi người dùng đăng nhập vào hệ thống, thông tin đăng nhập của họ sẽ được xác thực để đảm bảo rằng họ là người dùng hợp lệ và có quyền truy cập vào các tài nguyên yêu cầu.
- Hoặc thông qua các phương thức xác thực bổ sung như Single Sign-On (SSO) và OAuth

Authorization là gì? (Ủy quyền) - What can I do ?

- Authorization là quá trình xác định quyền truy cập của người dùng đối với các tài nguyên trong ứng dụng. Khi người dùng truy cập vào một tài nguyên, Spring Security sẽ kiểm tra xem người dùng có được phép truy cập vào tài nguyên đó hay không hoặc thực hiện một hành động nào đó trong hệ thống thông qua (roles) và (permission).

Các nguyên tắc thiết kế Security cho hệ thống

- Trust nothing
- Xác định quyền hạn cho hệ thống

Các tính năng nâng cao của Spring Security

Spring Security không chỉ hỗ trợ xác thực và phân quyền cơ bản, mà còn cung cấp nhiều tính năng nâng cao để bảo vệ ứng dụng web của bạn. Một số tính năng nâng cao của Spring Security bao gồm

- CSRF protection (bảo vệ chống lại tấn công CSRF)
- Session management (quản lý phiên)
- Password encoding (mã hóa mật khẩu)

Chúng ta có thể kích hoạt và tùy chỉnh các tính năng nâng cao này thông qua các annotation, XML, hoặc Java configuration trong Spring Security.

Ưu điểm của Spring Security

- Spring Security là một framework bảo mật mạnh mẽ và linh hoạt, hỗ trợ rất nhiều tiêu chuẩn và giao thức bảo mật.
- Được tích hợp sẵn với Spring Framework, giúp việc phát triển ứng dụng web an toàn và hiệu quả hơn.
- Spring Security có một cộng đồng lớn và sôi động, với rất nhiều tài liệu hướng dẫn và ví dụ minh họa.

Nhược điểm của Spring Security

- Cấu hình Spring Security có thể khá phức tạp và khó hiểu, đặc biệt là khi làm việc với các tính năng nâng cao.
- Một số tính năng của Spring Security có thể không phù hợp với loại ứng dụng web, ví dụ như ứng dụng web không sử dụng Spring Framework. Và cả các ứng dụng có quy mô lớn hoặc các ứng dụng yêu cầu tốc độ phản hồi cao.
- Yêu cầu kiến thức chuyên môn về bảo mật để sử dụng hiệu quả.

Setup Spring Security

https://docs.spring.io/spring-security/reference/getting-spring-security.html

```
<dependencies> <!-- ... other dependency elements ... -->
    <dependency>
        <groupId>org.springframework.boot</groupId>
        <artifactId>spring-boot-starter-security</artifactId>
    </dependency>
</dependencies>
```

Tổng kết bài học

- Trong bài học này, chúng ta đã tìm hiểu về cơ chế hoạt động của Spring Security - một trong những framework bảo mật phổ biến nhất trong thế giới phát triển ứng dụng web.
- Chúng ta đã tìm hiểu chi tiết về các thành phần cơ bản của Spring Security bao gồm Authentication, Authorization và Authentication Provider, cũng như các tính năng nâng cao của Spring Security

Bài tập thực hành

Yêu cầu:

- Các em sẽ làm một ứng dụng phân quyền tùy thuộc vào user đăng nhập vào hệ thống là: user hay admin mà ta cho phép họ vào trang web tương ứng.

Ví dụ.

- Trang Home thì ai vào cũng được .
- Trang Admin thì chỉ có admin được vào và thấy được trang . Nếu là role user và vào trang Admin thì mình hiện thông báo lỗi bạn không có quyền.
- Trang User Info thì user và admin được phép vào. Cái này do mình hoàn toàn có thể thay đổi quyền trong database để phân quyền ai được phép vào trang nào.
- Deadline: 19/7/2024. Nộp toàn bộ source code lên elearning.

TRƯỜNG ĐẠI HỌC
VĂN LANG

KHOA CÔNG NGHỆ THÔNG TIN