**Spring Authentication**

|  |  |
| --- | --- |
| Ý chính | Nội dung chi tiết |
| Nội dung chính | 1. Khái niệm về Authentication 2. Giới thiệu các cơ chế thường được sử dụng để xác thực 3. Spring Security và các thành phần |
| 1. Khái niệm về Authentication | Authentication – Xác thực.  Là hành động xác nhận 1 người sử dụng, 1 hệ thống, 1 tài nguyên nào đó. Có thể sử dụng bên thứ 3 để xác thực ví dụ facebook. Google.. -> dùng để cấp quyền truy cập vào trang web. |
| 1. Các cơ chế xác thực | **HTTP Basic**: sử dụng username + password  Cookies  **JWT: Json web token** -> chuỗi mã đăng nhập đã được mã hóa. Bao gồm 3 phần:   * Header * Payload * Secret   Signature: chữ ký điện tử.  Oauth2: ứng dụng bên thứ 3. FB/ Gmail.  OTP one time password. |
| 1. Spring Security và các thành phần | • Spring Security là một dự án nổi bật trong hệ sinh thái Spring, cung cấp các dịch vụ bảo mật toàn diện cho các ứng dụng doanh nghiệp có nền tảng Java EE.  • Spring Security là một framework tập trung vào việc cung cấp khả năng xác thực (authentication) và phân quyền (authorization) cho ứng dụng Java.  • Authentication: là tiến trình thiết lập một principal. Principal có thể hiểu là một người, hoặc một thiết bị, hoặc một hệ thống nào đó có thể thực hiện một hành động trong ứng dụng.  • Authorization hay Access-control: là tiến trình quyết định xem một principal có được phép thực hiện một hành động trong ứng dụng hay không. Trước khi diễn tiến tới Authorization, principal cần phải được thiết lập bởi Authentication.  Các thành phần trong Spring Security:  • SecurityContext là interface, lưu trữ tất cả các chi tiết liên quan đến bảo mật trong ứng dụng. Khi kích hoạt Spring Security trong ứng dụng thì SecurityContext cũng sẽ được kích hoạt theo.  • Sử dụng lớp SecurityContextHolder để truy cập vào  SecurityContext. Lớp này lưu trữ security context hiện tại của ứng dụng, gồm chi tiết của principal đang tương tác với ứng dụng.  • UserDetails là một interface, đại điện cho một principal. Gồm các phương thức sau:    TÌM HIỂU CORS VÀ CSRF |
| 1. Tổng kết | 1. Nắm được khái niệm về Authentication 2. Trình bày được các cơ chế xác thực 3. Triển khai được Security trong Spring |

**Tổng kết**:

Câu hỏi tổng kết: Trình bày lại các cơ chế xác thực?

Dặn dò:

Câu hỏi cho bài mới:

1. Khái niệm và ý nghĩa của Authorization?
2. Triển khai Authorization trong Spring
3. Phân biệt CSRF và XSS?