**Spring framework**

# **5. Security**

# **1. Thế nào là authentication, authorization**

**Authentication** và **Authorization** là hai khái niệm quan trọng trong lĩnh vực bảo mật, thường được sử dụng trong các hệ thống web và ứng dụng phần mềm. Mặc dù chúng có liên quan với nhau, nhưng chúng phục vụ những mục đích khác nhau:

1. **Authentication (Xác thực)**:
   * Đây là quá trình xác minh danh tính của người dùng hoặc một hệ thống.
   * Mục đích chính của quá trình này là kiểm tra xem người dùng có phải là người mà họ tuyên bố hay không.
   * Ví dụ: Khi bạn đăng nhập vào một trang web, quá trình nhập tên người dùng và mật khẩu chính là bước xác thực để hệ thống kiểm tra danh tính của bạn.
2. **Authorization (Phân quyền)**:
   * Sau khi danh tính đã được xác thực, authorization quyết định những gì người dùng được phép làm.
   * Mục đích chính của quá trình này là xác định quyền truy cập của người dùng vào các tài nguyên hoặc chức năng trong hệ thống.
   * Ví dụ: Sau khi bạn đăng nhập vào một trang quản trị, quá trình authorization sẽ xác định bạn có quyền sửa, xoá dữ liệu hay chỉ có thể xem mà không có quyền chỉnh sửa.

# **2. JWT, các thành phần của JWT**

**JWT (JSON Web Token)** là một tiêu chuẩn mở dùng để chia sẻ thông tin một cách an toàn giữa các bên dưới dạng đối tượng JSON. JWT thường được sử dụng để xác thực người dùng và truyền tải thông tin có bảo mật trong các ứng dụng web hoặc API.

Một JWT bao gồm ba thành phần chính, được phân tách bởi dấu chấm (.):

1. **Header**:
   * Phần này chứa metadata về JWT, gồm hai thành phần chính:
   * Header này sau đó sẽ được mã hóa thành Base64Url.
     + **Algorithm**: Thuật toán sử dụng để ký (chẳng hạn như HS256 hoặc RS256).
   * **Type**: Loại token, trong trường hợp này là JWT.
2. **Payload**

* Phần payload chứa các thông tin (claims) mà bạn muốn chia sẻ, bao gồm các loại thông tin:
  + **Registered claims**: Một số claims được định nghĩa sẵn như:
    - iss (issuer): Ai phát hành token.
    - sub (subject): Chủ thể của token (thường là người dùng).
    - iat (issued at): Thời gian phát hành.
    - exp (expiration): Thời gian hết hạn của token.
  + **Public claims**: Các claims tùy chọn do người dùng định nghĩa.
  + **Private claims**: Các thông tin đặc thù, tùy chỉnh cho một hệ thống cụ thể.
* Payload cũng được mã hóa thành Base64Url.

1. **Signature**
   * Phần signature được tạo bằng cách lấy header và payload đã mã hóa rồi ký chúng với một khóa bí mật bằng thuật toán đã xác định trong header (chẳng hạn như HMAC, RSA).
   * Phần này đảm bảo rằng token không bị thay đổi trong quá trình truyền tải.

### **Tính bảo mật của JWT:**

* JWT không mã hóa (encrypt) dữ liệu mà chỉ mã hóa bằng Base64Url, nghĩa là nội dung có thể đọc được nhưng không thể thay đổi nếu không có khóa bí mật phù hợp để tạo chữ ký mới.
* Thường thì trong phần payload, các thông tin nhạy cảm không nên được lưu trữ mà chỉ lưu những thông tin cần thiết cho quá trình xác thực và phân quyền.