# Lập trình web SPRING MVC

## Bài 9: Spring Security

# Mục tiêu :

**Nắm Tổng quan Spring Security, một số khái niệm cơ bản**

**01** Phân biệt sự khác nhau giữa Authentication và Authorization

**02** Tổng quan Spring Security, một số khái niệm cơ bản

# Phân biệt sự khác nhau giữa Authentication và Authorization

- Cả 2 thuật ngữ thường được sử dụng kết hợp với nhau để nói về bảo mật, đặc biệt là khi nói đến quyền truy cập vào hệ thống. Giao diện tham chiếu đến các nội dung định nghĩa trong các file tài nguyên.
- Cả hai đều là những chủ đề rất quan trọng thường đi kèm với các trang web như phần quan trọng trong cơ sở hạ tầng dịch vụ.
- Tuy nhiên, cả hai thuật ngữ rất khác nhau có các khái niệm hoàn toàn khác nhau.

*Nguồn: https://viblo.asia/p/phan-biet-su-khac-nhau-giua-authentication-va-authorization-Eb85oad4Z2G*

# AUTHENTICATION

- Authentication là về việc xác thực thông tin đăng nhập của bạn như Tên người dùng / ID người dùng và mật khẩu để xác minh danh tính của bạn.
- Trong các public và private network, hệ thống xác thực danh tính người dùng thông qua mật khẩu đăng nhập.
- Authentication thường được thực hiện bởi tên người dùng và mật khẩu, và đôi khi kết hợp với các yếu tố xác thực, trong đó đề cập đến các cách khác nhau để được xác thực.

*Nguồn: https://viblo.asia/p/phan-biet-su-khac-nhau-giua-authentication-va-authorization-Eb85oad4Z2G*

# AUTHENTICATION

Dựa trên cấp độ bảo mật, authentication factor có thể thay đổi theo một trong các cách sau:

- **Single-Factor Authentication** - là phương thức xác thực đơn giản nhất thường dựa vào mật khẩu đơn giản để cấp cho người dùng quyền truy cập vào một hệ thống cụ thể là một website hoặc network.
- **Two-Factor Authentication** - một quy trình xác minh gồm hai bước, không chỉ yêu cầu tên người dùng và mật khẩu, mà còn một thứ mà chỉ người dùng biết, để đảm bảo mức độ bảo mật bổ sung, chẳng hạn như pin ATM, chỉ người dùng mới biết.
- **Multi-Factor Authentication** - một phương thức xác thực tiên tiến nhất sử dụng hai hoặc nhiều mức bảo mật từ các loại xác thực độc lập để cấp quyền truy cập cho người dùng vào hệ thống.

*Nguồn: https://viblo.asia/p/phan-biet-su-khac-nhau-giua-authentication-va-authorization-Eb85oad4Z2G*

# AUTHORIZATION

- Authorization xảy ra sau khi hệ thống của bạn được authentication (xác thực) thành công, cuối cùng cho phép bạn toàn quyền truy cập các tài nguyên như thông tin, file, cơ sở dữ liệu, quỹ, địa điểm, hầu hết mọi thứ.
- Authorization thường được đưa ra sau khi xác thực xác nhận các đặc quyền của bạn để thực hiện. Nói một cách đơn giản hơn, nó giống như cho phép ai đó chính thức làm điều gì đó hoặc bất cứ điều gì.

*Nguồn: https://viblo.asia/p/phan-biet-su-khac-nhau-giua-authentication-va-authorization-Eb85oad4Z2G*

# SỰ KHÁC NHAU GIỮA AUTHENTICATION VÀ AUTHORIZATION

| Authentication | Authorization |
|---|---|
| Authentication xác nhận danh tính của bạn để cấp quyền truy cập vào hệ thống. | Authorization xác định xem bạn có được phép truy cập tài nguyên không. |
| Đây là quá trình xác nhận thông tin đăng nhập để có quyền truy cập của người dùng. | Đó là quá trình xác minh xem có cho phép truy cập hay không. |
| Nó quyết định liệu người dùng có phải là những gì anh ta tuyên bố hay không. | Nó xác định những gì người dùng có thể và không thể truy cập. |
| Authentication thường yêu cầu tên người dùng và mật khẩu. | Các yếu tố xác thực cần thiết để authorization có thể khác nhau, tùy thuộc vào mức độ bảo mật. |
| Authentication là bước đầu tiên của authorization vì vậy luôn luôn đến trước. | Authorization được thực hiện sau khi authentication thành công. |

*Nguồn: https://viblo.asia/p/phan-biet-su-khac-nhau-giua-authentication-va-authorization-Eb85oad4Z2G*

# Tổng quan Spring Security

Spring security là 1 framework thuộc hệ thống Spring, dành riêng cho việc thiết lập bảo mật của ứng dụng bao gồm authentication và authorization.

*Nguồn: https://kipalog.com/posts/Tong-quan-Spring-Security--mot-so-khai-niem-co-ban*

# MỘT SỐ THUẬT NGỮ CƠ BẢN

## 1. Authentication vs Authorization

- Authentication: quá trình xác minh user, dựa vào thông tin đăng nhập mà user cung cấp.

  **Ví dụ** khi login, bạn nhập username và password, nó giúp hệ thống nhận ra bạn là ai.

- Authorization: Quá tình xác định xem user có quyền thực hiện những chức năng nào của hệ thống (đọc/sửa/xóa data), sau khi user đã authenticated thành công.

*Nguồn: https://kipalog.com/posts/Tong-quan-Spring-Security--mot-so-khai-niem-co-ban*

## 2. Principle, Granted authority, Role

- Principle: chỉ authenticated user hiện tại (user đã đăng nhập thành công và thực hiện action hiện tại)
- Granted authority: quyền được thực hiện action của authenticated user.
- Role: một NHÓM QUYỀN của authenticated user.

*Nguồn: https://kipalog.com/posts/Tong-quan-Spring-Security--mot-so-khai-niem-co-ban*

## 3. Encoding, Encrypt và Hashing

- Encoding: quá trình convert data từ dạng này sang dạng khác, không sử dụng mã hóa. Trong nhiều trường hợp, encoding dùng để giảm size của data (video và audio file). Một số kiểu encoding thường dùng: ASCII, BASE64, UNICODE
- Encrypt: quá trình transform data mà các data này cần được bảo vệ. Có 2 kiểu encrypt là symetric (đối xứng) và asymetric (bất đối xứng). Về cơ bản thì mã hóa đối xứng là sử dụng 1 key (gọi là secret key) để encrypt data và decrypt data, một số thuật toán mã hóa đối xứng thường gặp là AES-128, AES-192, AES-256. Trong khi đó, mã hóa bất đối xứng sử dụng hai keys: public key và private key, public key để encrypt data và private key để decrypt data, một số kiểu mã hóa bất đối xứng thường gặp là RSA (phổ biến nhất), DSA.
- Hashing: quá trình convert data thành một chuỗi hash sử dụng hash function. Một số giải thuật hash thường gặp: MD5, SHA256. Data hashed không thể được chuyển đổi theo hướng ngược lại (theo lý thuyết). Do vậy, một trong những ứng dụng quan trọng của hashing là lưu password.

*Nguồn: https://kipalog.com/posts/Tong-quan-Spring-Security--mot-so-khai-niem-co-ban*