Hackademics Hanoi
Hack your passion, Code your life!

CHƯƠNG 17 – SPRING SECURITY

Nội dung

1. Giới thiệu Spring Security
2. Xác thực cơ bản với Spring Security
3. Tùy biến trang login trong xác thực cơ bản
4. Logout và Remember me trong Spring Security
5. Authentication-provider
6. Ví dụ

1. Giới thiệu Spring Security

Giới thiệu

- Trong bảo mật, hai chủ đề hay được nhắc đến đó là cơ chế xác thực (Authentication) và cơ chế phân quyền (Authorization)
- Xác thực (Authentication):
  - xác thực cơ bản (basic authentication),
  - xác thực tập trung (central authentication),
  - OpenID
  - ...

Giới thiệu

- Spring đã phát triển một phần trong framework của mình để hỗ trợ cho việc thực hiện các cơ chế xác thực và phân quyền trên ứng dụng - Spring security.

2. Xác thực cơ bản với Spring Security

Xác thực cơ bản

- Xét ví dụ bài toán quản lý user:
  - Mỗi admin có thể đăng nhập bằng username và passord
  - Một admin có quyền xem thông tin của user hay danh sách user
  - Tài khoản user chỉ xem thong tin tài khoản user của mình mà thôi
- Chúng ta sẽ thiết lập bảo mật như sau:
  - Cần xác thực đăng nhập (ROLE_NAME = ROLE_USER) để truy cập User detail
  - Cần quyền ROLE_NAME = ROLE_ADMIN để truy cập User list
  - Các trang khác, mọi người đều có thể truy cập (không cần xác thực)

3. Tùy biến trang login

Tùy biến trang login

- Trong ví dụ xác thực cơ bản một trang login của Spring Security sẽ tự động hiện ra và yêu cầu người dùng nhập username và password trước khi muốn truy cập vào hệ thống.
- Tuy nhiên trang login đó rất đơn giản và chúng ta không thể tùy biến để hiển thị theo cách mà ta mong muốn được.
- => Cần tạo ra một trang login riêng biệt của chính ứng dụng web.

4. Logout và Remember me trong Spring Security

Cơ chế logout

- Về mặt căn bản, cơ chế logout là cơ chế cho phép người dùng thoát khỏi môi trường làm việc sau khi đã xác thực thành công.
- Đối với ứng dụng web, việc này sẽ là xóa bỏ session đang tồn tại giữa client và web server. Việc này sẽ được đơn giản hóa đi rất nhiều đối với Spring Security, việc logout ra khỏi ứng dụng web có sử dụng Spring Security chỉ đơn giản là nhấp chuột lên một đường link đã được cấu hình từ trước.

Cơ chế Remember Me

- Cơ chế remember me là cơ chế góp phần tiện lợi hơn cho người dùng khi muốn quay trở lại sử dụng ứng dụng mà không cần login.

Cụ thể như sau:

- Khi người dùng lần đầu tiên login thành công thì ứng dụng sẽ tạo ra một cookie trên trình duyệt lưu thông tin xác thực của người dùng. Và cookie này sẽ tồn tại trên trình duyệt web cho đến khi người dùng bấm vào logout.

Cơ chế Remember Me

- Nếu như người dùng không bấm vào logout mà chỉ đơn giản là tắt trình duyệt đi, như vậy ở lần truy cập sau này người dùng sẽ không phải xác thực lại nữa. Ứng dụng sẽ đọc cookie của người dùng từ trình duyệt và lấy ra thông tin cho việc xác thực.

5. Authentication-provider

AUTHENTICATION-PROVIDER

- Authentication-provider được cấu hình trong file config: spring--security.xml.
- Spring Security có một authentication manager để quản lý việc xác thực, các thông tin để xác thực và phân quyền sẽ được cung cấp bởi một authentication-provider.
- Bên trong authentication provider, thông tin cho mỗi một cá thể sẽ được gói vào trong một user và được quản lý bởi một user-service. User service sẽ làm nhiệm vụ cung cấp các thông tin về một user nào đó cho việc xác thực và phân quyền.

```
<security:authentication-manager>
     <security:authentication-provider>
          <security:user-service>
               <security:user name="admincp" password="111111" authorities="ADMIN"/>
               <security:user name="user" password="222222" authorities="USER"/>
          </security:user-service>
     </security:authentication-provider>
</security:authentication-manager>
```

AUTHENTICATION-PROVIDER

- Trên thực tế, thông tin xác thực và phân quyền hay được lưu và lấy ra từ nguồn nào đó (ví dụ như database chẳng hạn) thay vì cố định trong file cấu hình như trên.
- Tùy thuộc từng hệ thống thì các thông tin này sẽ được lưu trữ trong những cấu trúc khác nhau.
- Một user và user service phải cung cấp đầy đủ các api mà Spring Security yêu cầu.
- Spring Security đã cung cấp sẵn hai interface là UserDetails và UserDetailsService lần lượt phục vụ cho việc tạo ra một User và user service của riêng ứng dụng.

6. Ví dụ triển khai

Ví dụ demo triển khai

Hackademics Hanoi
Hack your passion, Code your life!

HẾT CHƯƠNG 17