

13. Swagger API Documentation & JWT Testing

13.1. Mục tiêu chương

Chương này quy định cách:

- Tạo tài liệu API bằng Swagger/OpenAPI
- Cấu hình Swagger cho Spring Boot
- Tích hợp xác thực JWT vào Swagger
- Test API có auth trực tiếp trên Swagger UI

Mục tiêu:

- Dev và QA có thể test API nhanh
 - Chuẩn hóa tài liệu API
 - Tránh test sai do thiếu token
 - Đồng nhất cách dùng Swagger giữa các team
-

13.2. Truy cập Swagger UI

Sau khi chạy service:

```
http://localhost:8080/swagger-ui/index.html
```

Hoặc:

```
http://localhost:8080/swagger-ui.html
```

Swagger hiển thị danh sách API theo controller.

13.3. Cấu hình Swagger trong Spring Boot

Dependency Maven:

```
<dependency>
  <groupId>org.springdoc</groupId>
  <artifactId>springdoc-openapi-starter-webmvc-ui</artifactId>
  <version>2.7.0</version>
</dependency>
```

13.3.1. Cấu hình OpenAPI + JWT

File:

config/OpenApiConfig.java

```
@Configuration
public class OpenApiConfig {

    @Bean
    public OpenAPI api() {
        return new OpenAPI()
            .info(new Info()
                .title("Company Backend API")
                .version("v1.0")
                .description("API documentation"))
            .components(new Components()
                .addSecuritySchemes("bearerAuth",
                    new SecurityScheme()
                        .type(SecurityScheme.Type.HTTP)
                        .scheme("bearer")
                        .bearerFormat("JWT"))
                )
            )
            .addSecurityItem(new SecurityRequirement().addList("bearerAuth"));
    }
}
```

13.4. Đánh dấu API cần JWT trong Controller

Controller cần auth:

```
@RestController
@RequestMapping("/api/v1/users")
@SecurityRequirement(name = "bearerAuth")
public class UserController {
Swagger sẽ hiển thị icon:
```

```
GET /api/v1/users
```

13.5. Cấu hình Spring Security cho Swagger

Swagger UI phải được phép truy cập không cần auth:

```
.requestMatchers(
    "/swagger-ui/**",
    "/swagger-ui.html",
    "/v3/api-docs/**"
).permitAll()
```

API business:

```
.anyRequest().authenticated()
```

13.6. Test API có JWT trên Swagger (Step-by-Step)

Bước 1. Login lấy JWT

Gọi API login:

```
POST /api/v1/auth/login
```

Response:

```
{
  "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9..."
}
```

Bước 2. Mở Swagger

`http://localhost:8080/swagger-ui/index.html`

Bước 3. Click Authorize

Góc phải Swagger:

Authorize

Click vào.

Bước 4. Nhập JWT

Nhập:

`Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...`

Lưu ý:

- Phải có chữ **Bearer**
- Có khoảng trắng sau Bearer

Ví dụ đúng:

`Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9`

Bước 5. Authorize

Click:

Authorize

Swagger sẽ lưu token cho toàn bộ API.

Bước 6. Test API

Chọn API có

`GET /api/v1/theme-config`

Click:

Execute

Swagger gửi request:

Authorization: Bearer eyJhbGciOiJIUzI1Ni...

13.7. Kiểm tra Swagger đã gửi token chưa

Trong Swagger phần Curl phải có:

-H "Authorization: Bearer eyJhbGciOiJIUzI1Ni..."

Nếu không có → chưa Authorize.

13.8. Lỗi thường gặp

403 Forbidden

Nguyên nhân:

- Chưa nhập token
 - Token sai
 - Token hết hạn
 - API cần auth nhưng Swagger chưa Authorize
-

Không thấy nút Authorize

Nguyên nhân:

- Chưa cấu hình SecurityScheme
- Swagger config sai
- Cache browser

Khắc phục:

Ctrl + F5

Swagger call được API không cần token

Nguyên nhân:

Security config permitAll API.

Ví dụ:

```
.requestMatchers("/api/v1/**").permitAll()
```

Swagger không cần JWT.

13.9. Quy định chuẩn sử dụng Swagger trong dự án

Controller cần auth:

```
@SecurityRequirement(name = "bearerAuth")
```

Controller public:

không cần annotation.

API test phải:

- Login lấy JWT
 - Authorize Swagger
 - Test API
-

13.10. Quy định commit & PR

API mới phải:

- Hiển thị trên Swagger
- Có request/response schema
- Có SecurityRequirement nếu cần auth
- Test được trên Swagger

PR bị reject nếu:

- API không có Swagger
 - Swagger lỗi
 - Không test được
-

13.11. Checklist Swagger cho Dev

Trước khi merge:

- Swagger mở được
 - API hiển thị
 - Authorize hoạt động
 - JWT call OK
 - Response đúng schema
-

13.12. Best Practice

Không permitAll API production.

Swagger chỉ permit:

```
/swagger-ui/**  
/v3/api-docs/**
```

JWT luôn test qua Authorize.

Phiên bản #1

Được tạo 2026-02-24 06:39:56 UTC bởi Tuấn Phùng

Được cập nhật 2026-02-24 06:40:12 UTC bởi Tuấn Phùng