Instituto Politécnico Nacional

ESCUELA SUPERIOR DE CÓMPUTO

Unidad de aprendizaje:

Ingeniería de Software

Documentación Técnica – Proyecto Individual

Alumno:

Ramos Velasco Gabriel Antonio

Grupo:

6CV4

Fecha de entrega:

9 de marzo del 2024

Descripción General del Proyecto

El proyecto es una aplicación web desarrollada con Spring Boot que implementa un sistema de gestión de usuarios con autenticación, autorización y funcionalidades CRUD. El sistema soporta roles diferenciados (administrador y usuario normal) y ofrece tanto interfaces web tradicionales como endpoints REST para la integración con clientes externos.

Arquitectura

El proyecto sigue una arquitectura por capas típica de Spring:

1. **Capa de Presentación**: Controladores y vistas
2. **Capa de Servicio**: Lógica de negocio
3. **Capa de Acceso a Datos**: Repositorios JPA
4. **Capa de Modelo**: Entidades y DTOs

Tecnologías Utilizadas

- **Spring Boot**: Framework principal
- **Spring Security**: Autenticación y autorización
- **Spring Data JPA**: Persistencia de datos
- **Thymeleaf**: Motor de plantillas
- **PostgreSQL**: Base de datos relacional
- **Hibernate**: ORM
- **Docker**: Contenedores

Modelo de Datos

Entidades Principales

1. **Usuario**
    - Campos: id, nombre, email, password, roles
    - Representa a los usuarios del sistema
2. **Rol**
    - Campos: id, nombre
    - Almacena los roles disponibles (ROLE_ADMIN, ROLE_USER)

Relaciones

- Usuario y Rol: Relación muchos a muchos implementada mediante una tabla intermedia usuarios_roles

Configuración de Seguridad

La configuración de seguridad está definida en SecurityConfig.java y proporciona:

- Políticas de acceso basadas en rutas
- Configuración de login/logout
- Manejo de sesiones
- Codificación de contraseñas con BCrypt

Gestión de Sesiones

El sistema utiliza el manejo de sesiones basado en cookies de Spring Security:

1. **Autenticación basada en sesión**: Se crea una sesión HTTP tras la autenticación exitosa
2. **SecurityContext**: Almacena información del usuario autenticado
3. **Actualización del contexto de seguridad**: Al cambiar datos sensibles como el nombre de usuario

Cómo Probar los Endpoints

Requisitos Previos

1. Asegúrate de tener la aplicación en ejecución (usando Docker o localmente)
2. El sistema inicia con un usuario administrador predefinido:
    - Usuario: Antonio
    - Contraseña: 12345

Pruebas de Endpoints Web

1. **Acceso como Usuario Anónimo**:
    - Navega a http://localhost:5173/login
    - Intenta acceder a http://localhost:5173/admin (debería redirigir al login)
    - Registra un nuevo usuario en http://localhost:5173/registro
2. **Acceso como Usuario Regular**:
    - Inicia sesión con el usuario recién creado
    - Verifica acceso a /perfil

- Prueba editar el perfil en /perfil/editar
- Verifica que no puedas acceder a /admin

3. **Acceso como Administrador**:
   - Inicia sesión con el usuario "Antonio" y password "admin123"
   - Accede a /admin y observa las opciones disponibles
   - Navega a /admin/usuarios para ver todos los usuarios
   - Edita un usuario con /admin/usuarios/editar/{id}
   - Elimina un usuario con /admin/usuarios/eliminar/{id}