Práctica 2

Desarrollo de una aplicación completa para la para la gestión de una clínica de fisioterapia con Express, Mongoose y un motor de plantillas.

Parte 3. Autenticación basada en sesiones

Vamos a modificar la autenticación en la aplicación para reemplazar el sistema basado en tokens por un sistema de autenticación mediante sesiones. Este sistema permitirá gestionar roles y aplicar restricciones de acceso según los permisos definidos.

3.1 Pasos previos

- Desinstala jsonwebtoken y elimina cualquier referencia a tokens en el proyecto, incluidas las funciones de generación y validación de tokens, así como el middleware correspondiente, si aún no lo has hecho.
- Actualiza las rutas protegidas para usar el sistema basado en sesiones.
- Instala la librería `express-session` para la gestión de sesiones:
    - Configura las sesiones para almacenar datos persistentes del usuario (ID, login, rol)

3.2 Proceso de login

Comenzaremos definiendo una vista **`login.njk`** para pedirle las credenciales al usuario (login y password). Definiremos en el enrutador **`routes/auth.js`** un servicio **`GET /auth/login`** que muestre este formulario.

A su vez, el formulario se enviará al servicio **`POST /auth/login`** de ese mismo enrutador, que buscará las credenciales en la base de datos y, si son correctas, dará de alta al usuario en la sesión.

Recuerda definir el enrutador adecuadamente en el fichero principal `index.js` si no lo tienes ya.

3.3 Protección de rutas

- Crea middleware para restringir acceso basado en roles.

Recuerda que los roles definidos y sus permisos son los siguientes:

- **admin**: acceso completo a toda la API (gestión de pacientes, fisioterapeutas, expedientes).
- **physio**: gestión de pacientes y expedientes médicos. No puede gestionar fisioterapeutas.
- **patient**: acceso restringido únicamente a sus propios datos (pacientes y expedientes).

3.4 Logout

- Añade un servicio **`GET /auth/logout`** en el enrutador **`routes/auth.js`** para que cierre la sesión del usuario y redirija a la página inicial.

3.5 Cambios en las vistas

- Usa condicionales en las vistas para mostrar u ocultar elementos según el rol.

Criterios de calificación

La práctica se evaluará sobre 10 puntos, distribuidos de la siguiente manera:

- Configuración Inicial (1 punto)
- Desarrollo de Vistas Dinámicas (4.5 puntos)
  - Listado de pacientes (0.3 puntos)
  - Formulario de búsqueda de pacientes (0.2 puntos)
  - Vista de detalles de paciente (0.4 puntos)
  - Formulario de alta de un paciente (0.4 puntos)
  - Formulario de edición de un paciente (0.4 puntos)
  - Listado de fisioterapeutas (0.3 puntos)
  - Formulario de búsqueda de fisioterapeutas (0.2 puntos)
  - Vista de detalles de fisioterapeuta (0.4 puntos)
  - Formulario de alta de un fisioterapeuta (0.4 puntos)
  - Formulario de edición de un fisioterapeuta (0.4 puntos)
  - Listado de expedientes médicos (0.3 puntos)
  - Formulario de búsqueda de expedientes médicos(0.2 puntos)
  - Vista de detalles de un expediente (0.4 puntos)
- Cambios en enrutadores para eliminar pacientes, fisios y expedientes (0.5)
- Validaciones de datos en formularios de pacientes y fisioterapeutas (1 punto)
- Gestión de subida de imágenes (1 punto)
- Autenticación basada en sesiones (2 puntos)