**INFORME EVALUACIÓN FINAL DSS**

1. Segurización por medio de token:

Podemos segurizar las rutas por medio de token, en este caso se hace por medio de la función “authToken”, acá está aplicada solamente a la solicitud tipo DELETE:

Captura de pantalla de computadora

Descripción generada automáticamente

Contenido de la función authToken:

Texto

Descripción generada automáticamente

Manejo de las funciones necesarias de login y verificación:

Captura de pantalla de computadora

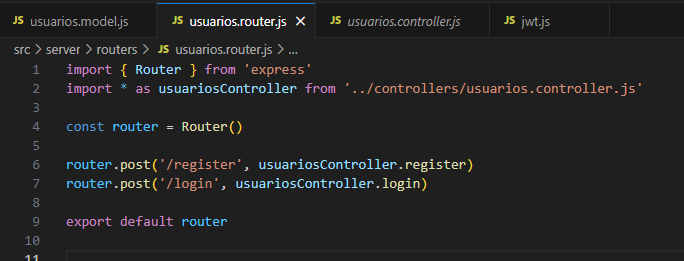
Descripción generada automáticamente

Token propio de la aplicación:

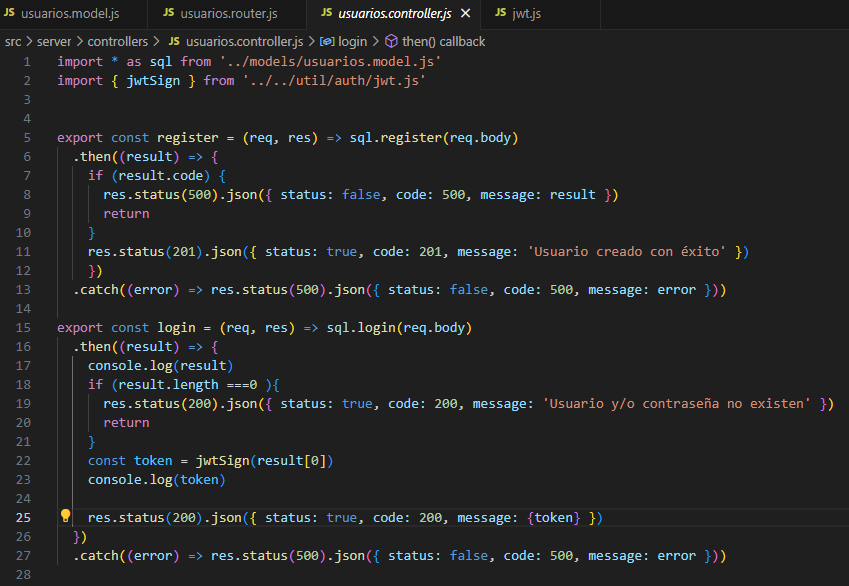
Texto

Descripción generada automáticamente

Rutas usuario:



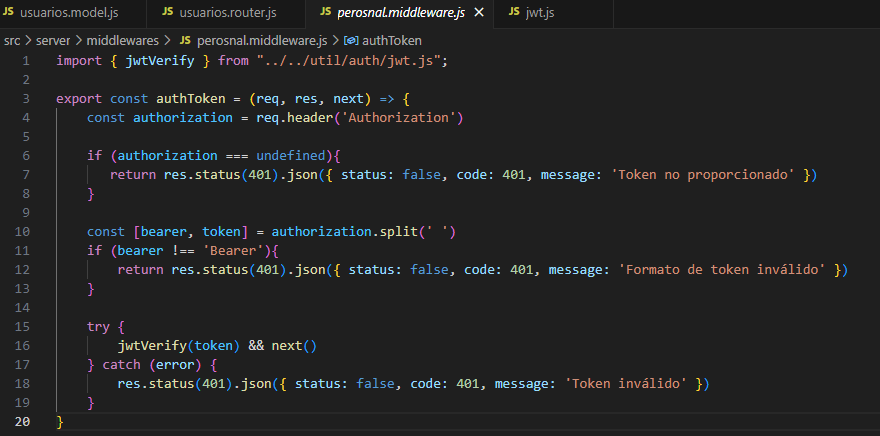
Controlador de usuario:



Lo que se muestra en las imágenes corresponde a la parte de segurización de la aplicación. Tenemos la ruta de personal con solicitud tipo DELETE incluyendo la función “authToken”, por lo que es necesario hacer un login para poder realizarla. En las rutas de usuario tenemos un register y un login (que son solicitudes tipo POST), lo importante lo encontramos al iniciar sesión donde el usuario ingresa sus datos en el BODY, en este caso es solamente correo y contraseña, estos datos se verificarán en la base de datos de Farmacia y se obtendrá una diferente respuesta según el caso, lo esperado es que el usuario y contraseña estén correctos y la respuesta a nuestro login sea la firma del token de la aplicación, si la obtenemos entonces pasamos a la parte de verificación.

1. Verificación de token:

Luego de tener un login exitoso con la firma de la aplicación, podemos acceder a las rutas que requieran de proporción de token, esto se logra por medio de la habilitación de un apartado de “Authorization” en el HEADER de la solicitud, seguido por la indicación de la palabra “Bearer ” (incluyendo el espacio) y al lado la firma de la aplicación. Si enviamos la solicitud correctamente entonces se ejecutará la verificación por medio de la función del middleware, que se encarga de comparar la firma proporcionada con el token propio de la aplicación, para eso tenemos diferentes respuestas según el caso:



Si el token no coincide, si el formato esta incorrecto o no se encuentra el apartado de “Authorization”, entonces no nos permitirá realizar la solicitud DELETE (en este caso)

En resumen, el usuario hace un login, si los datos del usuario existen en la base de datos, en respuesta obtenemos la firma de la aplicación. Luego para hacer una solicitud a una ruta segurizada, debemos agregar el apartado de “Authorization”, el Bearer y proporcionar la firma obtenida en el login dentro del HEADER, el middleware recibe estos datos y verifica no solamente el formato, sino que también que la firma coincida con el token de la aplicación y si todo está correcto, la solicitud a la ruta segurizada se ejecuta sin problemas.

1. Solución anti-inyección de código:

En la sección del modelo de la tabla de personal, encontramos las funciones con el lenguaje SQL que traerá los datos de la base de datos, cuando es necesario pasarle parámetros a la función, estos dentro del script de SQL no se colocan simplemente como variables, sino que en su lugar se asigna la posición del parámetro, por lo que no se concatena como script.

Ejemplo de lo mencionado:

