

03/05/2019



BEFIT GIMNASIOS

IMPLEMENTACIÓN

AUTORAS:

- SOFÍA MARTINEZ PARADA
- ALBERTO RUIBAL OJEA

BASES DE DATOS II – CURSO 2018/2019

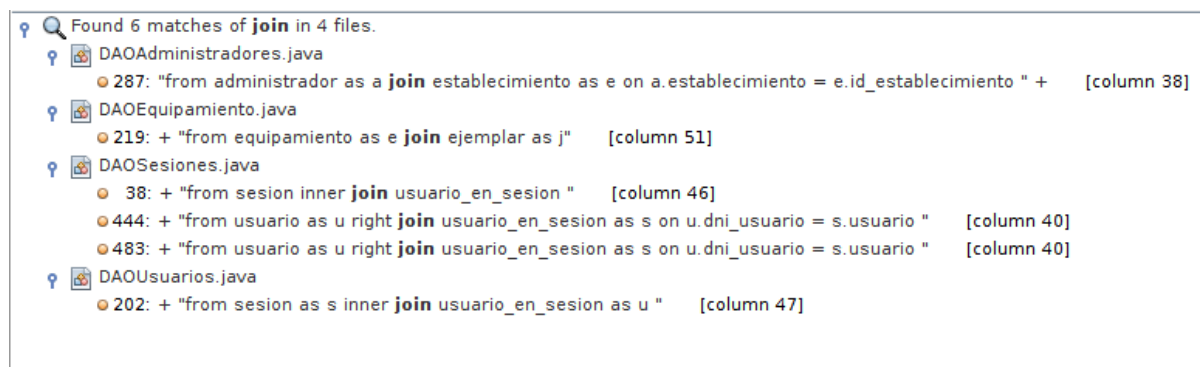
E.T.S.E. – GREI (USC)

CONTENIDO

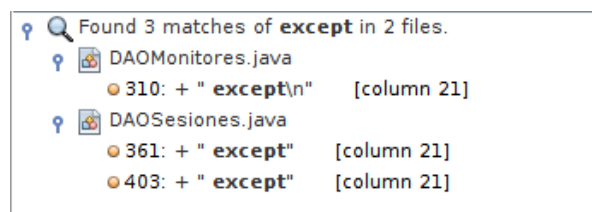
| | |
|--|---|
| <i>Transacciones Complejas</i> | 4 |
| Seguridad | 4 |
| Ventana de autenticación | 4 |
| Seguridad adicional..... | 5 |
| <i>Ejecución atómica de las transacciones</i> | 5 |

TRANSACCIONES COMPLEJAS

Hemos realizado un total de 6 transacciones complejas usando la cláusula *join*:



También consideramos como transacción compleja a aquellas en las que usamos "*except*", es decir, en la Ventana de Gestión de una sesión (*VGestionarUsersSesiones*), usamos este tipo de consulta en SQL para ver a las monitoras/usuarios que podrían asistir a la sesión (que ya no estén en otra sesión en ese momento, por ejemplo).



SEGURIDAD

VENTANA DE AUTENTIFICACIÓN

Con ella se conoce el establecimiento al que pertenece cada administradora, el cual se usa en todas las transacciones menos en la de usuarias.

A través de esta ventana la Gerente también puede acceder a su propia ventana de autenticación. En el archivo "*baseDatos.properties*" se encuentra la información de inicio de sesión de la Gerente, la cual se comprueba en la *FachadaGUI* de la aplicación si la información de inicio de sesión introducida coincide con las credenciales de la Gerente (**user:boss, pass:boss**).

La información de inicio de sesión (las contraseñas básicamente) del *user* que usan las administradoras para conectarse a la Base de Datos y del *user* que usa la Gerente están cifradas en este archivo. El método de cifrado ha consistido en usar una clave de cifrado para encriptarlas y guardarlas encriptadas de forma segura en dicho archivo, siendo solo posible conocer las contraseñas originales si se conoce la función de desencriptado y la clave de desencriptado. Esta clave se puede ver en *FachadaGUI*, mientras que los métodos usados para el encriptado de estas se encuentran tanto en *FachadaGUI* como en la clase *ProtectedConfigFile*¹.

¹ <https://exceptionshub.com/encrypt-password-in-configuration-files.html>

SEGURIDAD ADICIONAL

Se ha implementado una seguridad adicional cuando las administradoras o la Gerente van a eliminar algo de la Base de Datos (en los despidos, modificación de los datos del establecimiento o cuando se va a borrar el mismo). Esta seguridad adicional consiste en una nueva autenticación previa a la ejecución de las actualizaciones en SQL.

EJECUCIÓN ATÓMICA DE LAS TRANSACCIONES

Hemos tenido en cuenta la ejecución atómica de las transacciones en casos delicados como la actualización/inserción/eliminación de datos. Para ello, se han añadido dos líneas de código: *con.setAutoCommit(true / false)*.