Universidad Autónoma de Nuevo León

Facultad de Ciencias Físico Matemáticas

Laboratorio de Diseño Orientado a Objetos

Semana #7

Profesor:

Miguel Angel Salazar

Estudiante:

Angel Adolfo Pacheco Mazuca

1656991

En esta práctica se creó un a aplicación la cual tenía que conectar con una base de datos, se agrego un archivo .jar con el nombre de "derbyclient" el cual nos sirvió para hacer la conexión con el manejador de base de datos, lo que más se complico fue en la parte del servlet, con las diferentes entradas y salidas de las diferentes clases (comentariosDAO, comentariosPOJO) y lo que aprendió es que se tenía que importar un archivo (El que se muestra al principio) para poder hacer la conexión ya que en otros lenguajes no tenía que importase nada, solo se hacia la conexión, por lo menos en el lenguaje que se conoce.

Preguntas de Reflexión

1. ¿Cuál piensas que es el propósito de haber hecho una clase DAO en el modelo en lugar de acceder a la base de datos directamente desde el controlador?

Creo que es para mayor seguridad dentro de la aplicación ya que no entregamos usuario y contraseña y aunque estén en una cadena, en ningún momento se escribieron nuevamente en el servlet.

2. ¿Para qué sirve un objeto POJO o JavaBean?

Según la red, es un objeto general el cual no extiende de nada y sirve parasimplificar más aún el proceso de desarrollo de aplicaciones.

3. En caso de que los comentarios fueran muchos (digamos, cientos o miles) sería impráctico mostrarlos todos en una misma página. Generalmente los sitios de búsqueda (como Google) usan una técnica llamada "paginación", para ir mostrando solo cierta cantidad de registros cada vez. Describe cómo harías esa paginación en esta aplicación (cuál es la lógica que seguirías en el programa).

Lo que he visto en diferentes páginas o sitios es que ponen un etiqueta select y ahí se pone los artículos o objetos los cuales se mostraran en la página, también tiene diferentes paginas para la busqueda, lo que haría yo, con lo mismo de la etiqueta select dividimos todos los objetos entre lo que se encuentre dentro entre esa cantidad luego crear diferentes páginas que se rellenen con la información.

4. Cuando se muestra la tabla con los resultados de la búsqueda, desaparecen los valores de los campos de búsqueda. ¿Qué harías para que se sigan mostrando?

Desde el mismo sevlet donde le mandamos los datos de la lista, mandar los datos que se escribieron antes, y asignárselos al momento de recargar la página.

5. Haz una búsqueda, pero ahora, en lugar de escribir un nombre, escribe lo siguiente en el campo de búsqueda de nombre (la comilla inicial es importante, y también los dos guiones al final):

' or 1=1 --

¿Cuál fue el resultado de la búsqueda?

Me regreso todos los registros de la base de datos :C.

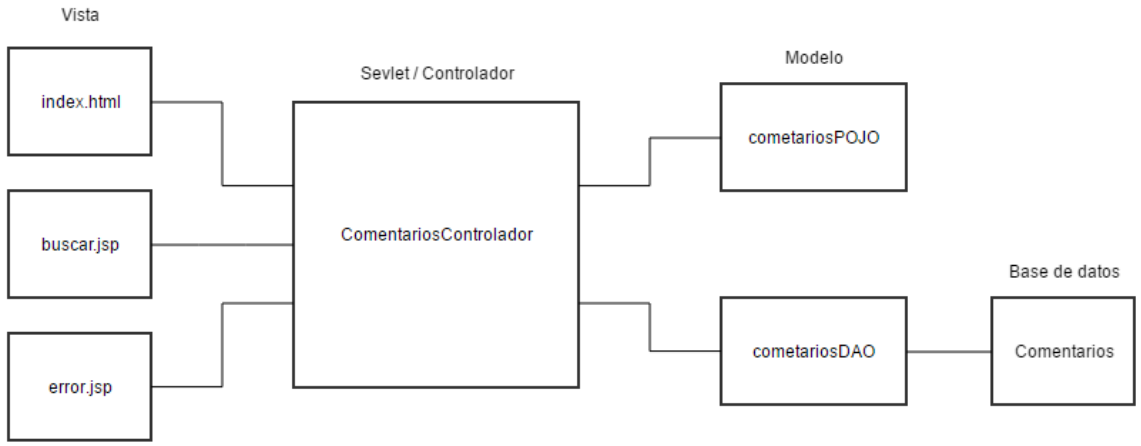
6. A lo que hiciste en la pregunta anterior se le conoce como SQL Injection (SQLi), y es una de las vulnerabilidades más explotadas en las aplicaciones Web. De acuerdo a la cadena de búsqueda y a los resultados obtenidos, explica qué fue lo que ocurrió.

Se cerró la condición anterior la palabra reservada or y la condición 1=1 se hace todo verdadero, así que regresa todos los registros ya que todo es verdadero.

7. ¿Cómo piensas que puede evitarse un SQL injection como el de la pregunta 4? (A estas alturas del curso no se vale responder "no sé" a una pregunta así).

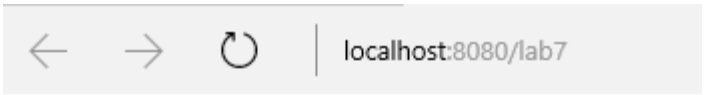
Lo primero debería hacerse una "limpieza" de lo introducido dentó de los imputs con algún método en el servidor eliminaremos todos los caracteres no deseados por ejemplo (´, +, ",), usar los mismo para lo que son ejemplo: para una contraseña utilizaremos un tipo "password" o un correo "email" y creo que para terminar una verificación o un capcha sería un plus que nos ayudaría demasiado.

8. Elabora un diagrama donde muestres todos los elementos que construiste en esta práctica y cómo están relacionados entre ellos.



Pantallas

Index.html



Datos generales

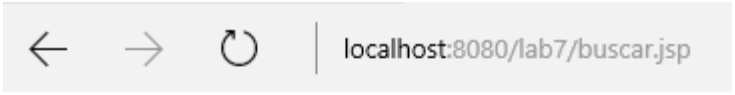
Nombre: Laura

Comentario:

me bulleas

Enviar

Busqueda.jsp sin datos



Datos buscar

Nombre:

Comentario: Enviar

Busqueda.jsp con datos

Datos buscar

Nombre:

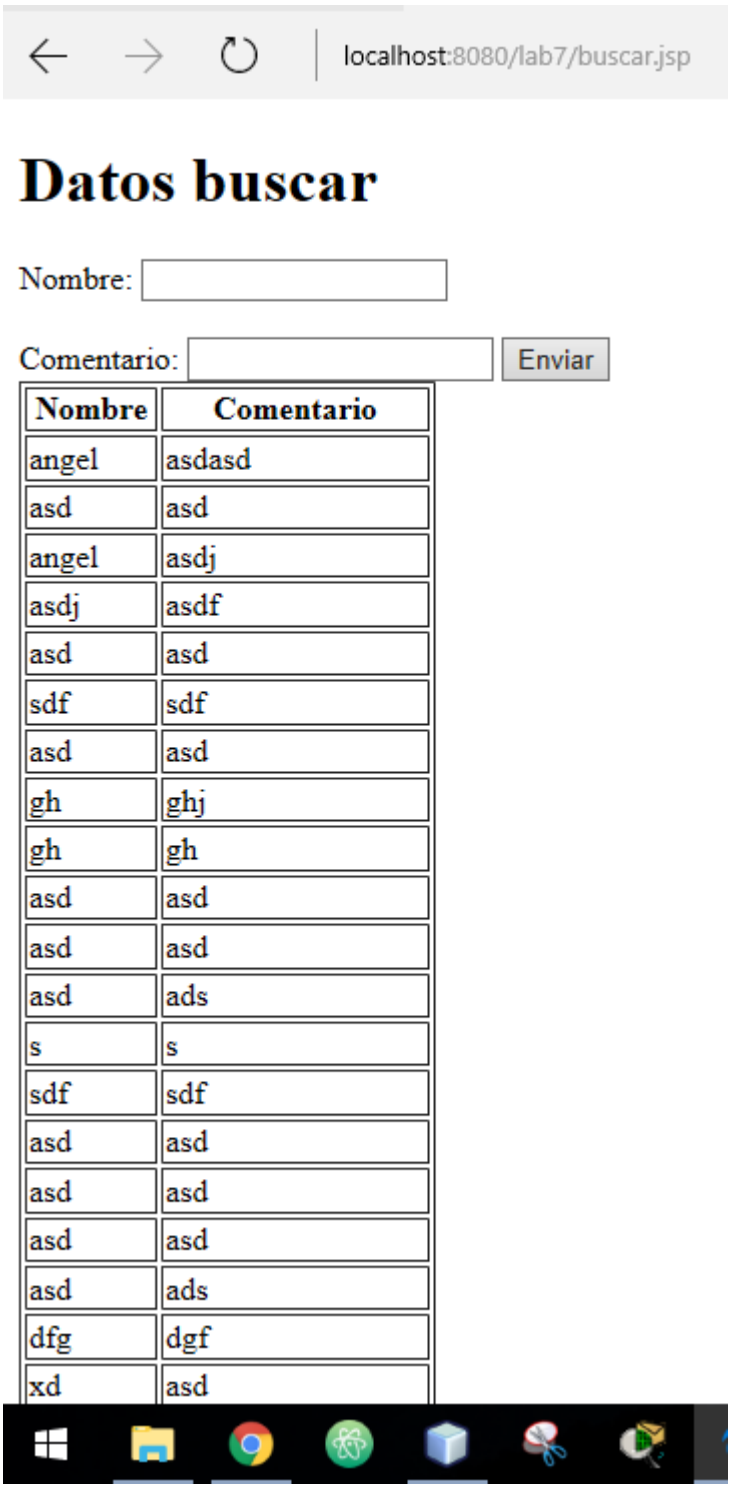
Comentario: Enviar

Nombre	Comentario
Laura	me bulleas

Error.jsp

Error xdxdxdxd

Resultados del SQL



Referencias

https://www.ibm.com/support/knowledgecenter/es/SS5JSH_9.1.1/org.eclipse.jst.ejb.doc.user/topics/cpojosandee5.html

La clase del martes c: