



UNIVERSIDAD AUTÓNOMA DE
NUEVO LEÓN
FCFM



UNIDAD DE APRENDIZAJE: LABORATORIO DE DISEÑO ORIENTADO
A OBJETOS.

PRACTICA #7

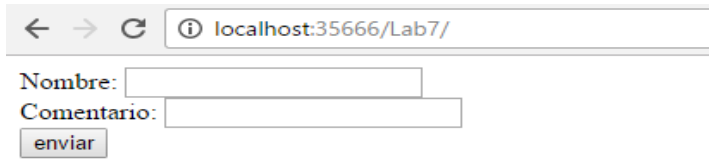
PROFESOR. MIGUEL ÁNGEL SALAZAR S.

ALUMNA. VALERIA MARTÍNEZ DE LA ROSA

MATRICULA. 1678575

San Nicolás de los garza, Nuevo león a 22 de marzo de 2017

Esta es la primera pantalla que deberá de mostrar. Es la página del índice.

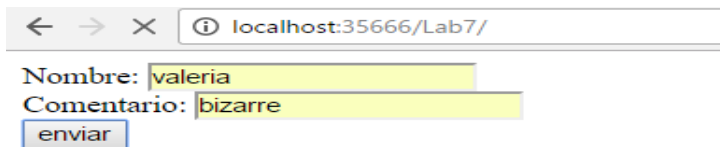


Nombre:

Comentario:

enviar

Se envía información nueva a la base de datos.

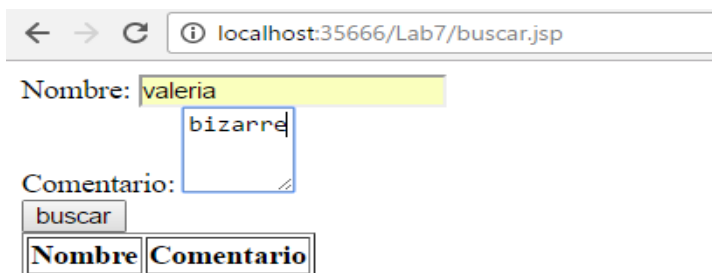


Nombre:

Comentario:

enviar

Después del paso anterior, te re-envía a la página de buscar.jsp, ahí escribes lo mismo que insertaste en el índice.



Nombre:

Comentario:

buscar

Nombre	Comentario
--------	------------

Y deberá de mostrarte todos los comentarios que tengan la palabra que buscaste de la persona.



Nombre:

Comentario:

buscar

Nombre	Comentario
valeria	bizarre love triangle
valeria	bizarre
valeria	bizarre
valeria	bizarre
valeria	bizarre
valeria	bizarre
valeria	bizarre
valeria	bizarre
valeria	bizarre lve triangle
valeria	bizarre love triangle-new order

Sí de nuevo le das clic en buscar de nuevo, sin nada de información te muestra lo siguiente:

Nombre:

Comentario:

buscar

Nombre	Comentario

En nombre escribimos ' or 1=1 -- , nos aparecen todos los registros de la base de datos.

Nombre:

Comentario:

buscar

Nombre	Comentario
Nestor	boys don't cry
valeria	bizarre love triangle
cecilia	feeling good
valeria	bizarre
valeria	bizarre
valeria	bizarre
alonso	hey
valeria	bizarre
valeria	bizarre
valeria	bizarre
valeria	comentario
valeria	bizarre lve triangle
valeria	bizarre love triangle-new order

En mi opinión, creo que este tipo de trabajos nos ayuda a el manejo de base de datos, para saber cómo es que funciona este, y así poder evitar los ataques más utilizados.

Aunque es algo complejo, a mi parecer, porqué debes de entender bien para que es cada cosa, sino no funcionara. Yo, por ejemplo, batallé con los String de las sesiones porqué los llamé de diferentes maneras.

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?

Para poder interactuar la página con la base de datos, al momento de insertar y buscar información.

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

Es una clase qué tiene sus atributos privados, por lo tanto tiene getter y setters.

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).

Al devolver la información de los campos con la información solicitada, validar que si la información a mostrar es mayor de 20, por ejemplo, que sólo muestro los primeros 15 con arreglos.

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?
Podríamos agregar cookies, para esto, y validar según las sesiones.
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?

Mostro todo los registros.

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.
La comilla simple es parte del código de sql, entonces este termina alguna parte del código de sql, y después ejecuta el resto, y como `1=1`, es true, devuelve todos los valores capturados.
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).
Podríamos validar que tipo de datos se puede introducir a los input, poner, por ejemplo que cuando el usuario escriba comillas o palabras clave del sql, muestre incorrecto.
8. Elabora un diagrama donde muestres todos los elementos que construiste en esta práctica y cómo están relacionados entre ellos.

