UNIVERSIDAD AUTONOMA DE NUEVO LEON

FACULTAD DE CIENCIAS FISICO MATEMATICAS

Laboratorio de DOO

Practica 7

Alumno: Alexis Blanco González

Matricula: 1725357

Carrera: LSTI

Grupo: 007

Aula: Lab de DOO

23 de Marzo del 2017

Opinión Personal

Esta Práctica se me dificulto mucho ya que me confundí y no recordaba las variables librerías de código ya que esas las utilizamos para cargar dicha base de datos en la aplicación que creamos, mucho del código que aparece no lo conocía y eso me dificulto más al realizar la práctica.

Lo que más se me dificulto fue la parte del JSP, ya que los símbolos (<% %>), no reconocía para que se utilizaban y cuando y donde usarlos, en el HTML los utilice pero me confundieron más el código.

Las cosas nuevas que aprendí de esta práctica fue a intercalar el código del HTML y Java en un JSP y utilizar la base de datos de Neatbeans.

Preguntas

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?

Es por seguridad, ya que es más seguro acceder por otro lado que no sea directamente.

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

Se utiliza para poder guardar la información.

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).

Insertaría una columna de números para obtener y controlar 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?

Crearía un cuadro de texto para guardar los datos y controlarla la información.

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?

Muestra todos los datos que tiene la base de datos

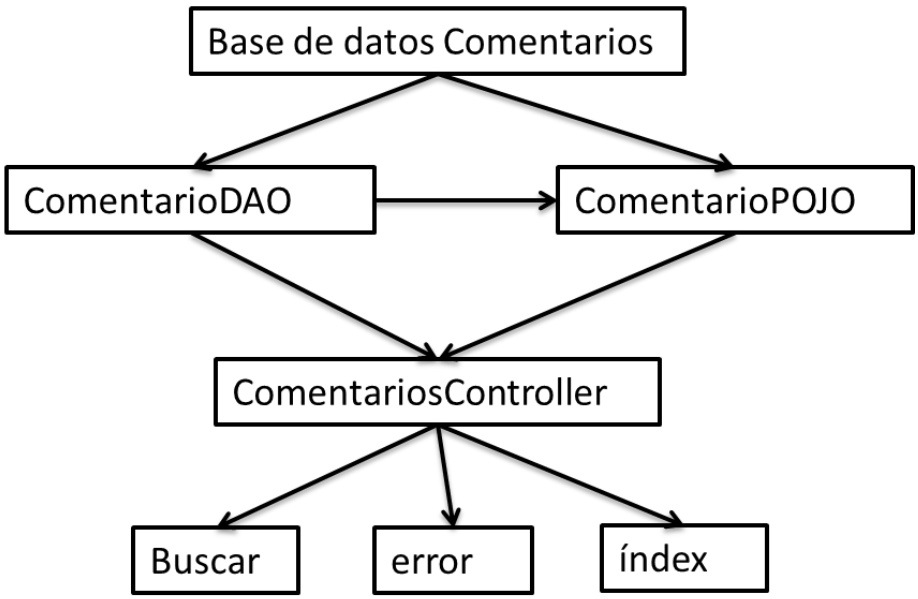
6. A lo que hiciste en la pregunta anterior se le conoce como SQL Injection (SQLi), y es una de las vulnerabilidades más explotadas en las aplicaciones Web. De acuerdo a la cadena de búsqueda y a los resultados obtenidos, explica qué fue lo que ocurrió.

Al poner ese código de SQL se utiliza para una búsqueda de toda la información de la base de datos.

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).

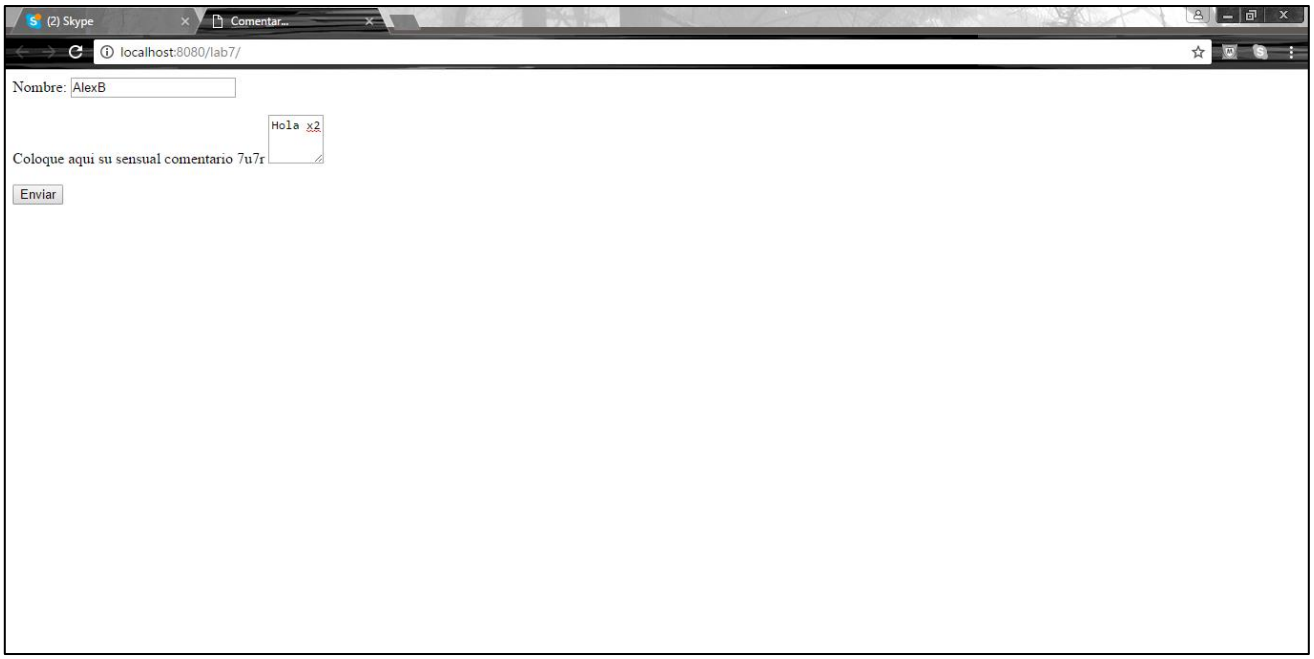
Para evitar esto, podríamos validar el campo de texto, poniendo que no pueda poner comillas simples.

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

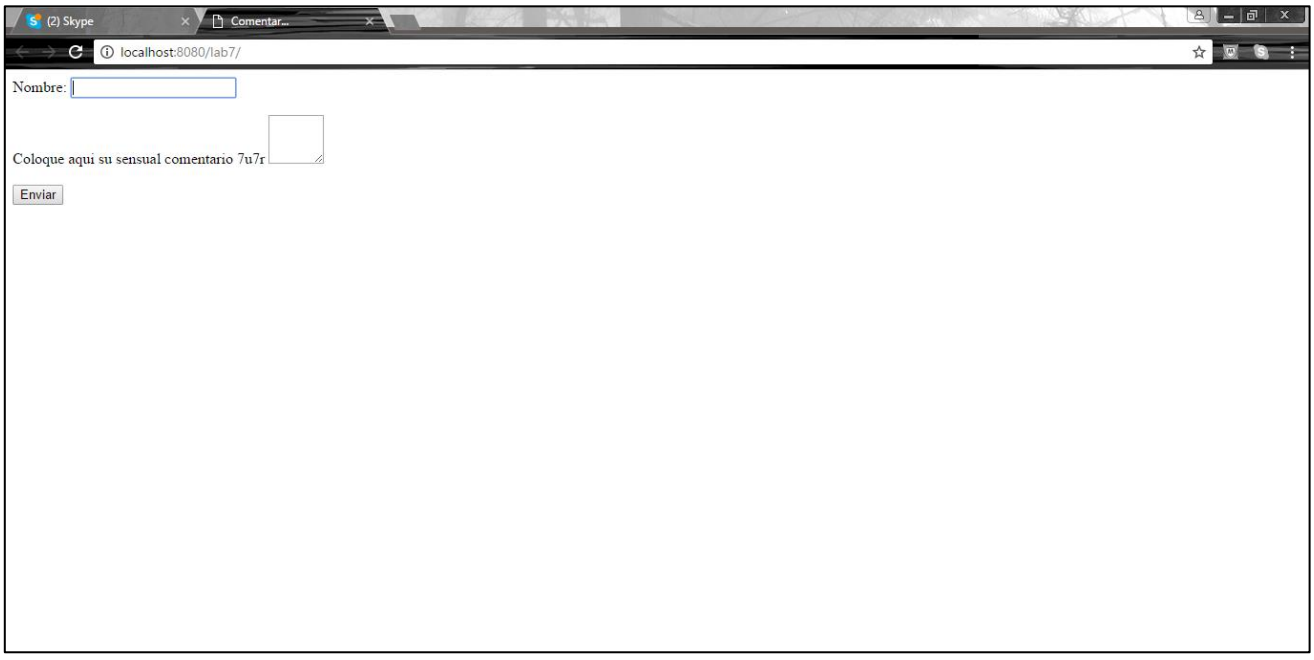


CAPTURAS DE PANTALLA

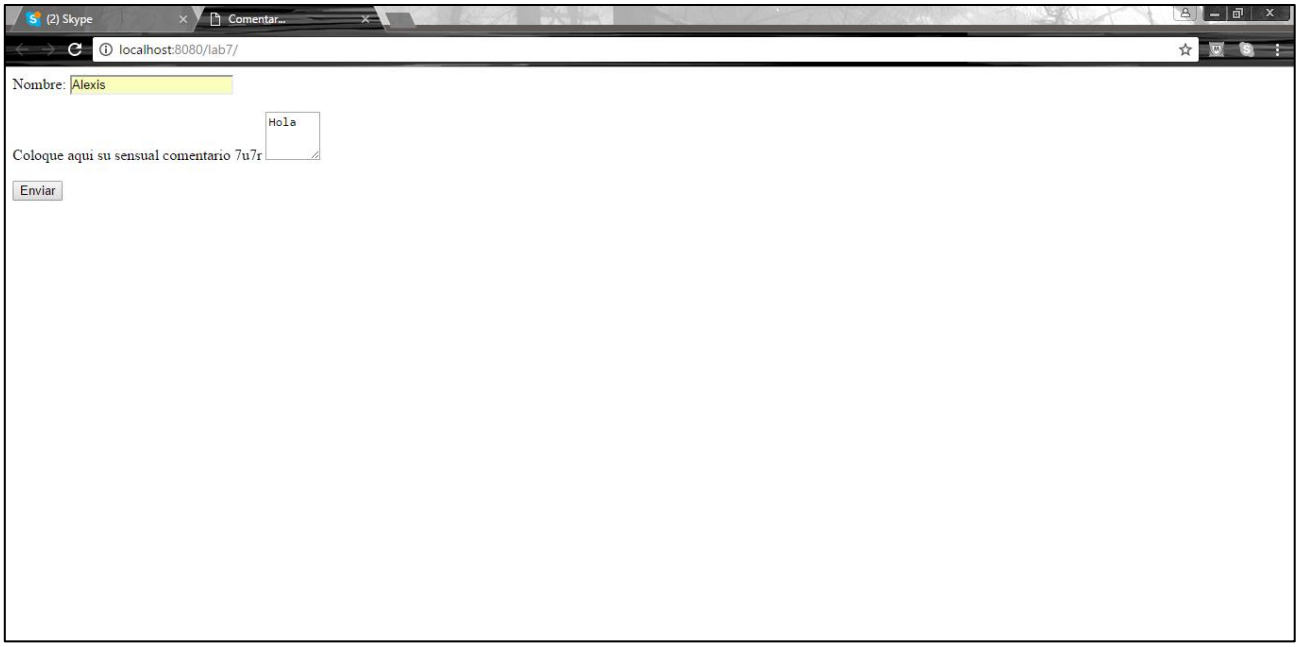
Página inicial



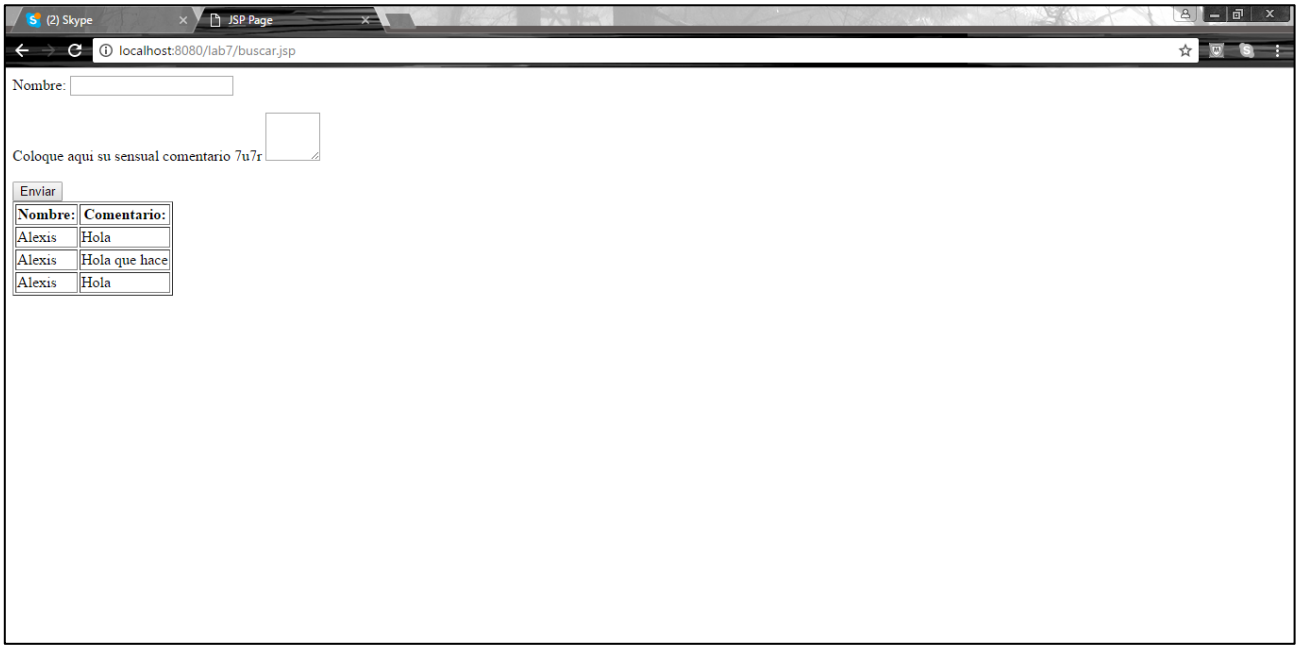
Página de búsqueda sin datos



Página de búsqueda con datos



Resultados del SQL



Página de error