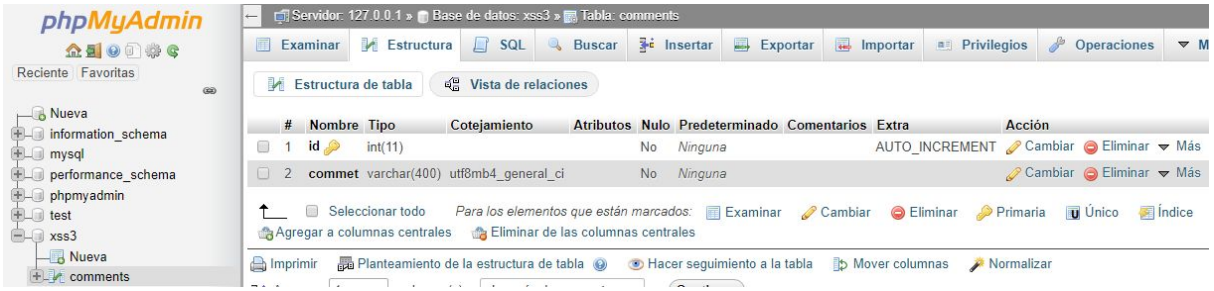
El código ejemplo está escrito en php y se utiliza la herramienta XAMPP para su ejecución. Se necesita de una base de datos que se crea en localhost/phpmyadmin llamada “xss3” y que tiene una tabla de 2 columnas que son “id” y “comment”. El campo id es un INT primario y autoincremental mientras que comment es un VARCHAR.



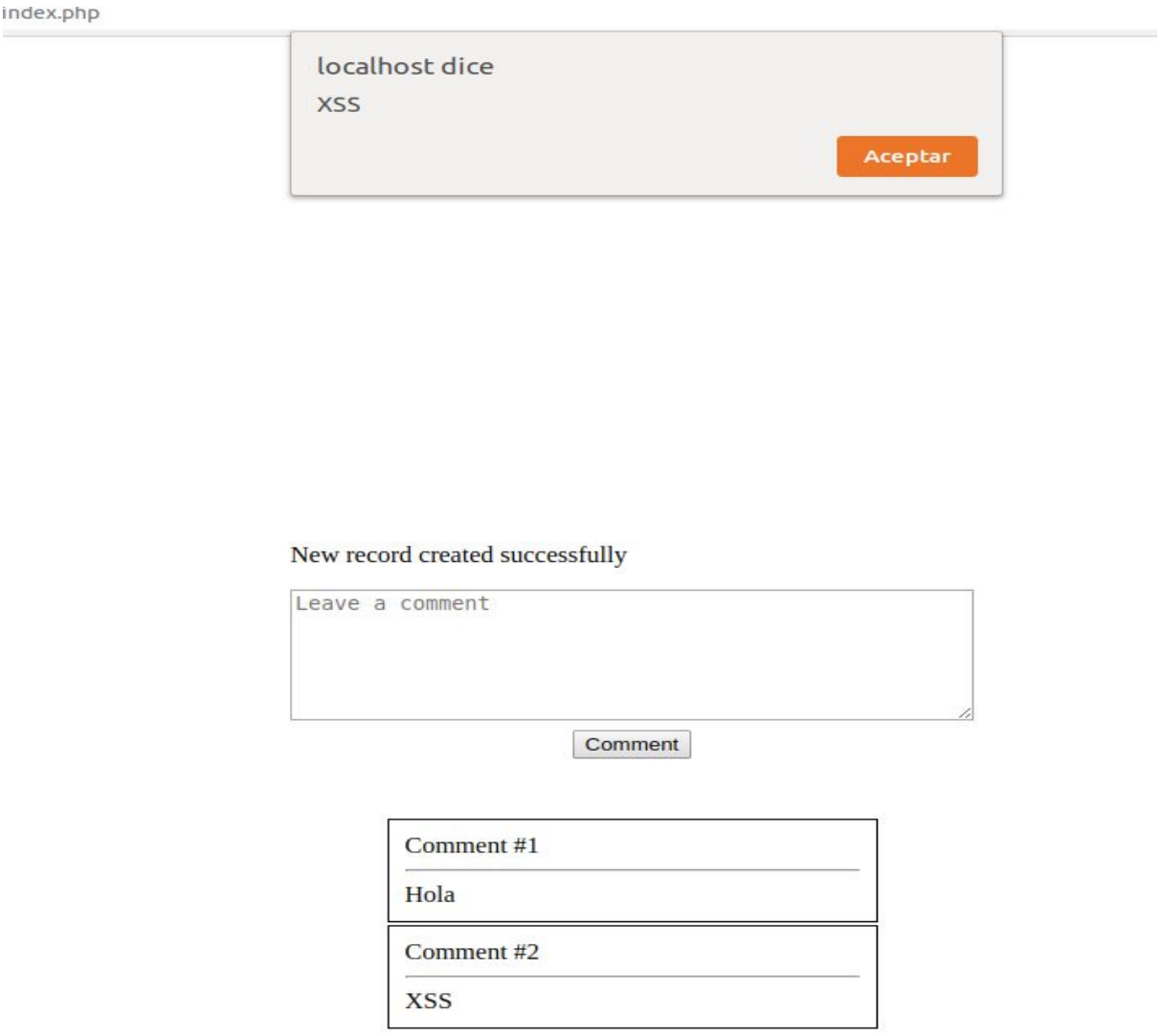
El archivo del código se debe ubicar en una carpeta que se crea de nombre “xss” y que se tiene que ubicar en la carpeta ”htdocs” de XAMPP.
La ruta para acceder al ejemplo será http://localhost/xss/index.php

Al acceder se mostrará la página

Si añadimos un comentario, este quedará impreso en la página

Si ingresamos un comentario acompañado de código script, este se ejecutará en la página
Por ejemplo ingresamos lo siguiente: XSS<script>alert(“XSS”)</script>

Al comentar se muestra el alert y se guarda el comentario



Esto se ve reflejado en la base de datos

Debido a esto el script siempre se ejecutará cada vez que se ingrese a la página mientras esté almacenado en la base de datos.

Así, básicamente se puede inyectar cualquier tipo de código script a esta página de ejemplo vulnerable