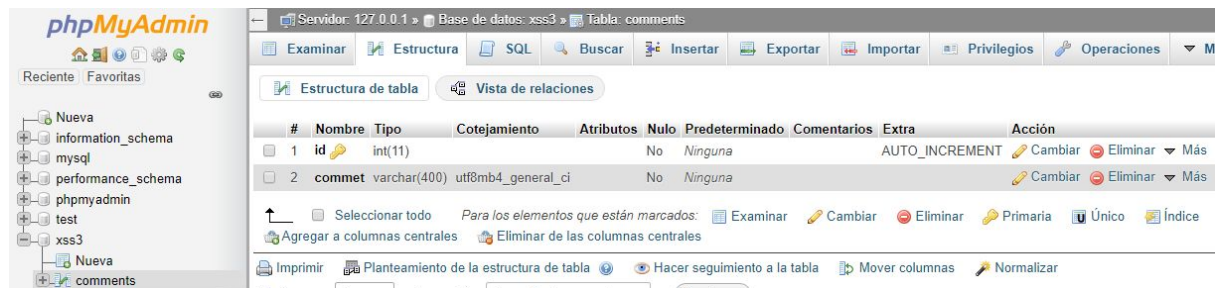


El código ejemplo está escrito en php y se utiliza la herramienta XAMPP para su ejecución. Se necesita de una base de datos que se crea en localhost/phpmyadmin llamada “xss3” y que tiene una tabla de 2 columnas que son “id” y “comment”. El campo id es un INT primario y autoincremental mientras que comment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

Try My New Comment Website!

Leave a comment

Comment

No Comments!

This website was made by me! I hope you really really like it!

Debug: Clear Table

Si añadimos un comentario, este quedará impreso en la página

Try My New Comment Website!

New record created successfully

Leave a comment

Comment

Comment #1

Hola

This website was made by me! I hope you really really like it!

Debug:

Clear Table

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

Try My New Comment Website!

New record created successfully

XSS<script>alert("XSS")</script>

Comment

Comment #1

Hola

Al comentar se muestra el alert y se guarda el comentario

index.php

localhost dice
XSS

Aceptar

New record created successfully

Leave a comment

Comment

Comment #1

Hola

Comment #2

XSS

Esto se ve reflejado en la base de datos



+ Opciones	
<input type="checkbox"/>	id comment
<input type="checkbox"/>	1 Hola
<input type="checkbox"/>	2 XSS<script>alert("XSS")</script>

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