

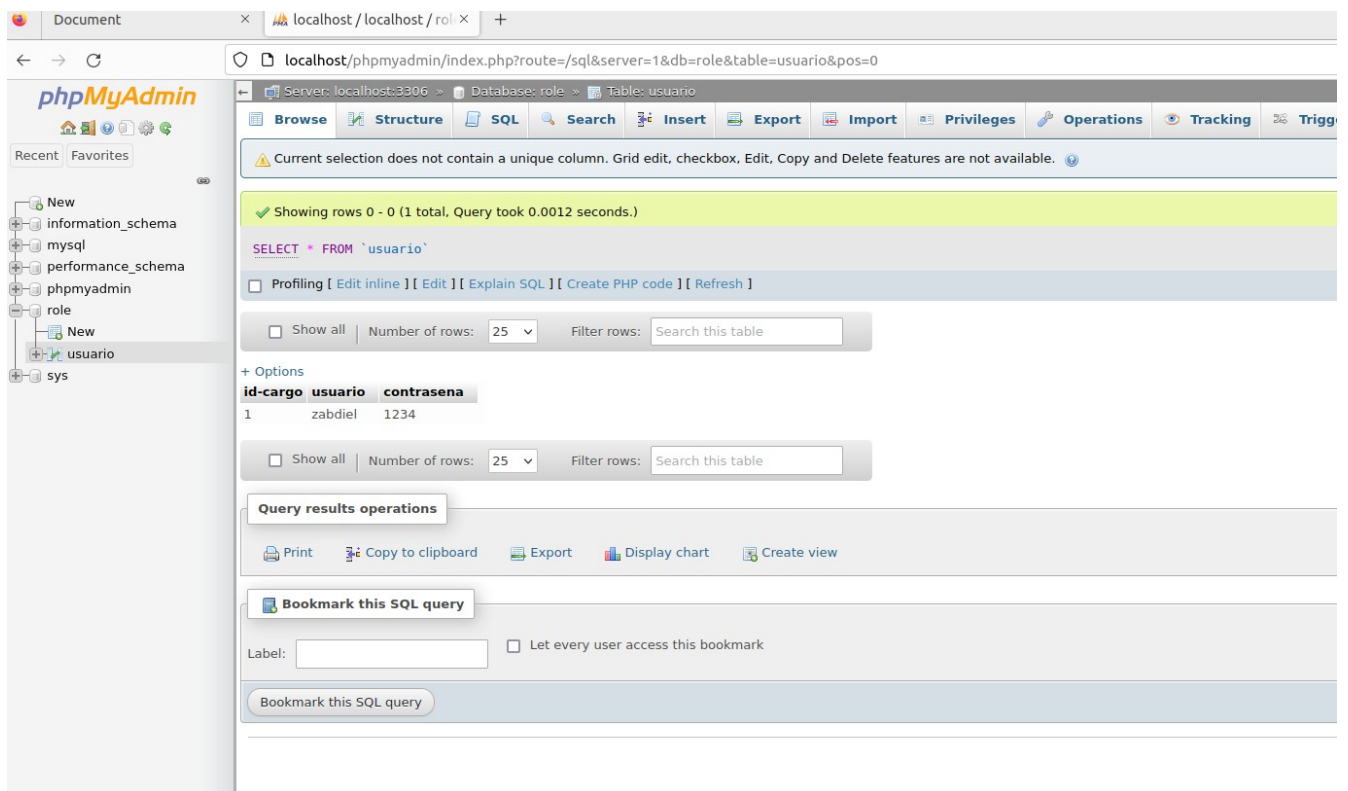
Reto 2

Nombre: Díaz Sotelo Iván Zabdiel

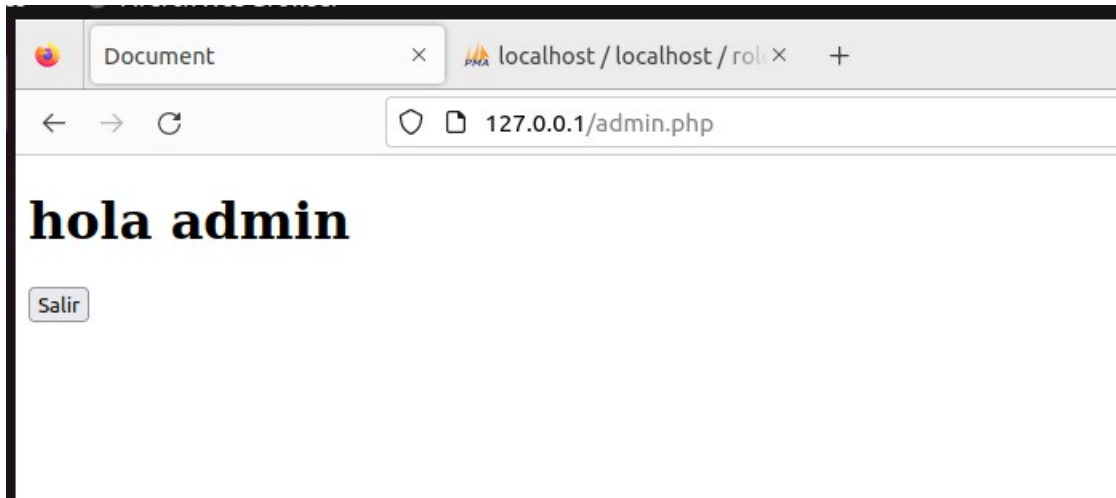
Administración y manejo de sesiones.

Para esta práctica se utilizaron principalmente 3 tecnologías: PHP para la programación de una pequeña aplicación web tipo login, apache para alojar la aplicación web dentro de un servidor y phpmyadmin para la administración de una base de datos mysql.

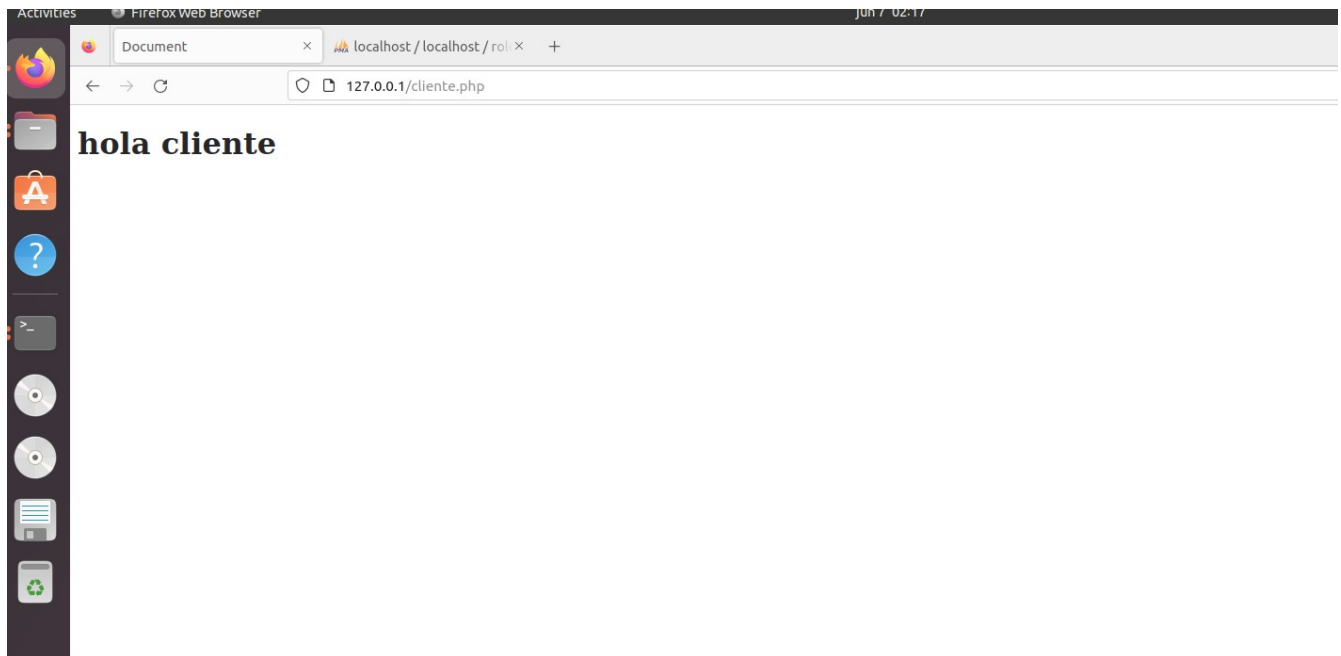
En la siguiente imagen se puede apreciar phpmyadmin con la tabla usada para la creación de un usuario , contraseña y tipo de rol.



Dentro de la aplicación tendremos dos campos, usuario y contraseña. Si la contraseña o el usuario es correcto y el usuario tiene como rol administrador se nos mostrará el siguiente mensaje:



De forma análoga, si el usuario es un cliente se debera mostrar una pantalla como la siguiente:



Por el contrario, si la contraseña o el usuario son incorrectos el sistema mostrara un mensaje de error:

Sistema de login

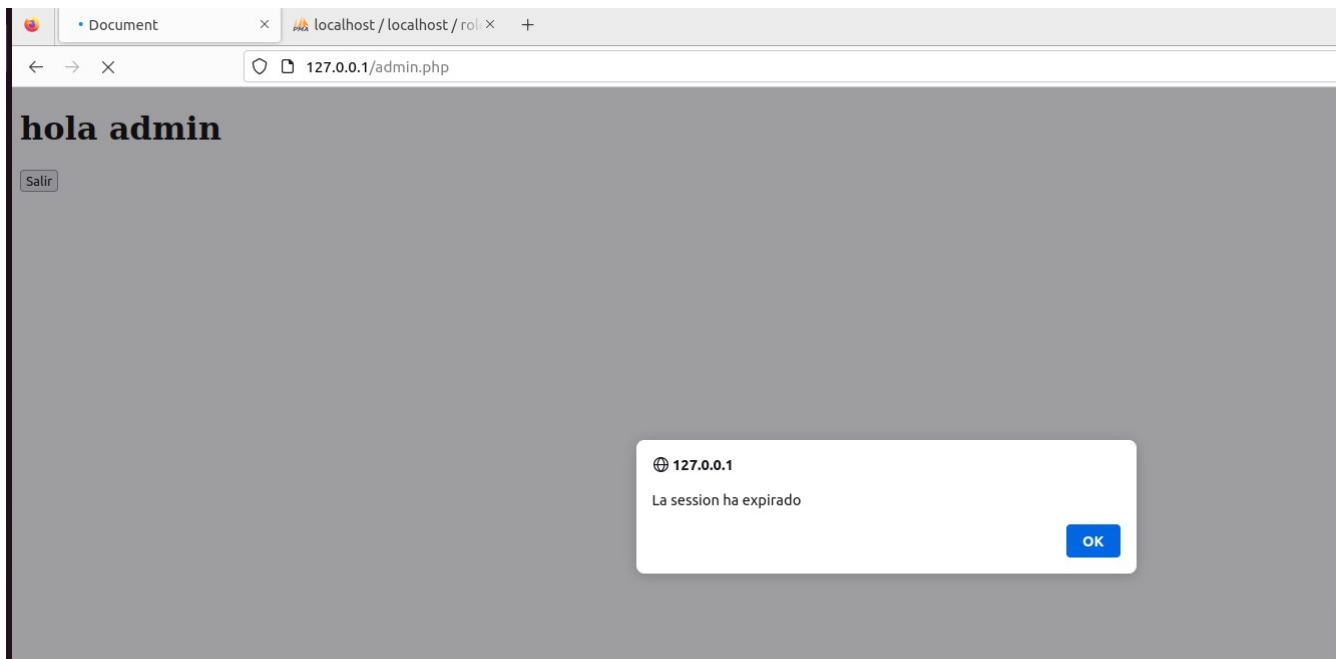
Usuario

Contraseña

ERROR EN LA AUTENTIFICACION

//

Otra cosa importante a considerar es que el sistema debiera terminar una sesión de usuario al cabo de un tiempo, esto para evitar que una persona no autorizada entre al sistema con las credenciales de otro usuario.



Vulnerabilidades XSS

Para este apartado se utilizo la plataforma de portswinger para realizar algunos ejercicios de inyección SQL:

Please enter your email address and password to log in.

Email address

Password

[Forgot your password?](#)

☐ Remember me on this computer

[Log in](#)

[Create account](#)

SQL injection

LAB

APPRENTICE

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data >>

✓ Solved

LAB

APPRENTICE

SQL injection vulnerability allowing login bypass >>

✓ Solved

LAB

PRACTITIONER






SQL injection UNION attack, determining the number of columns returned by the query >>

✓ Solved

Cross site scripting:

Al igual que para las inyecciones sql, utilizamos la misma herramienta para hacer las practicas.

Cross-site scripting

 LAB	APPRENTICE Reflected XSS into HTML context with nothing encoded »	✓ Solved
 LAB	APPRENTICE Stored XSS into HTML context with nothing encoded »	✓ Solved
 LAB	APPRENTICE DOM XSS in <code>document.write</code> sink using source <code>location.search</code> »	✓ Solved
 LAB	APPRENTICE DOM XSS in <code>innerHTML</code> sink using source <code>location.search</code> »	✓ Solved
 LAB	APPRENTICE DOM XSS in jQuery anchor <code>href</code> attribute sink using <code>location.search</code> source »	✓ Solved

