



Reto 2

Ciberseguridad básica

Randy Villanueva Guzman
THINCRS

Contents

Administración de sesiones y perfiles web	2
Atacar por inyecciones y vulnerabilidades XSS	6
Inyecciones SQL	6
Vulnerabilidad XSS	7
Falsificar la identidad y explotar solicitudes entre sitios	7

Administración de sesiones y perfiles web

Para el manejo de sesiones utilizamos las siguientes herramientas PHP, PHPMyAdmin, MySQL y Apache2 para poder levantar un pequeño sitio web el cual cuenta con un login y tiene un sistema de validación de usuarios, que al ingresar las credenciales correctas te redirige al sitio de cliente, admin o en su defecto manda un error de autenticación.

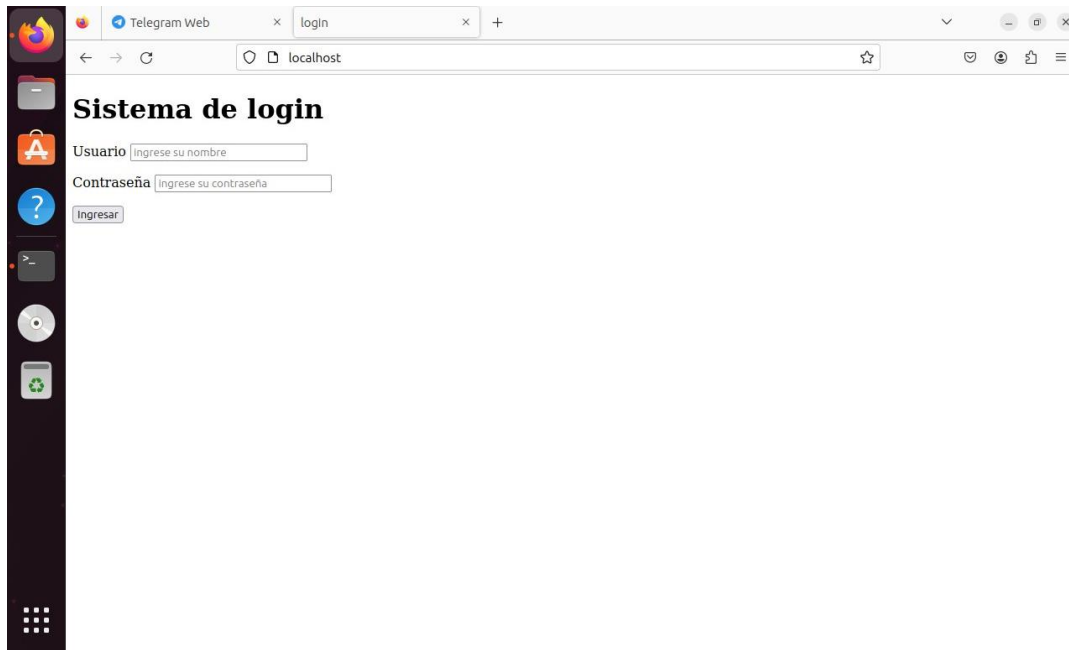


Figura 1. Pagina principal del sitio web

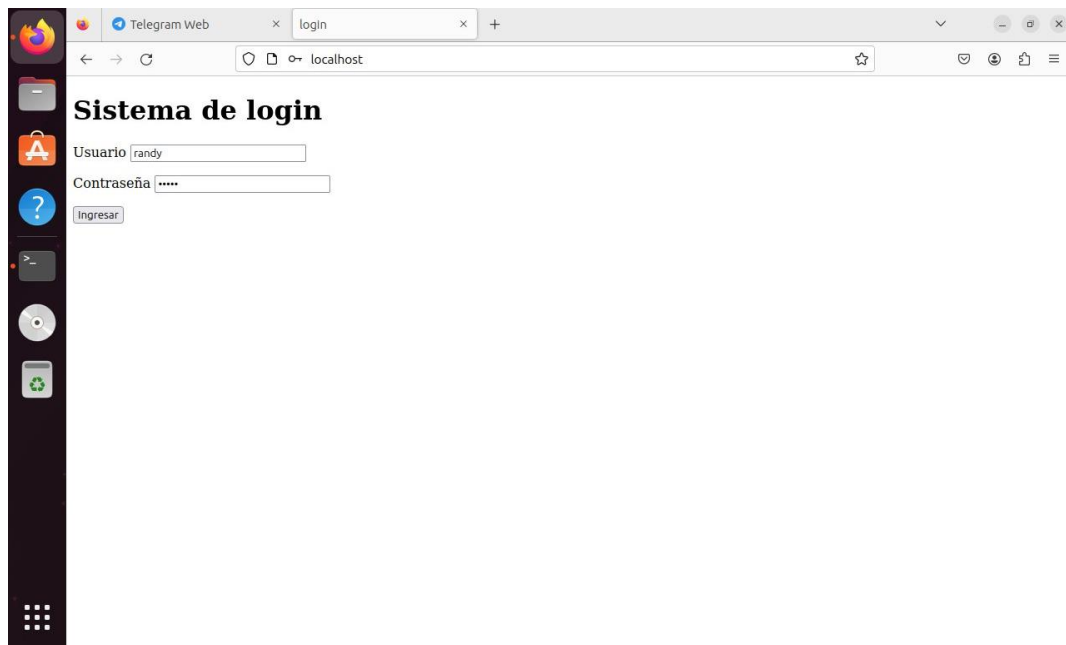


Figura 2. Ingresando credenciales incorrectas

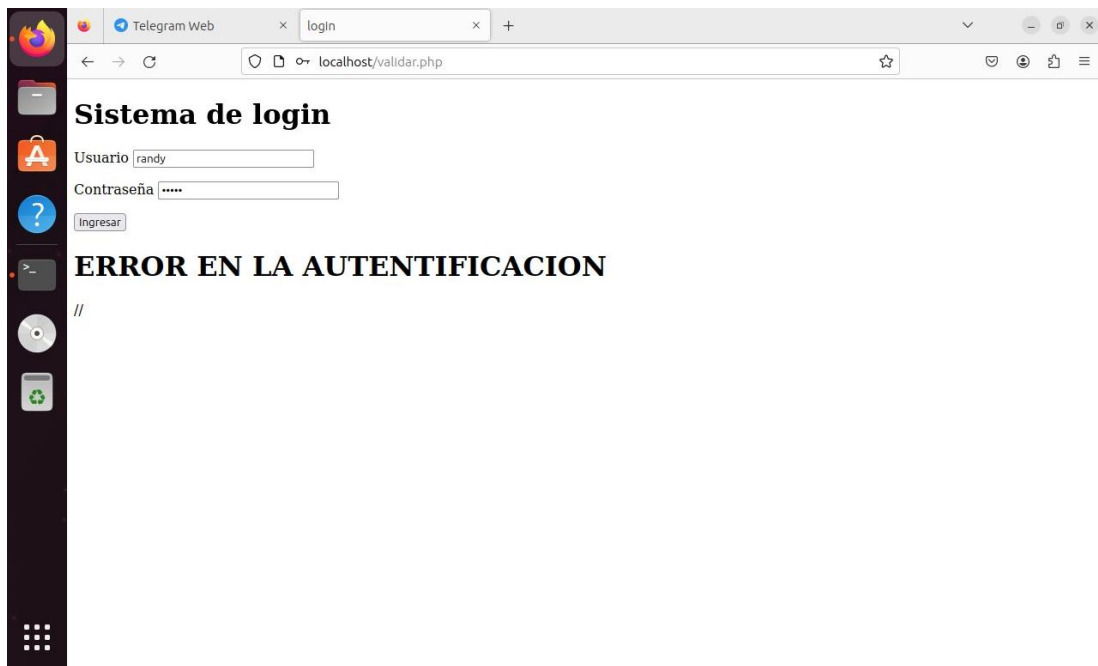


Figura 3. Mensaje de error de autenticación

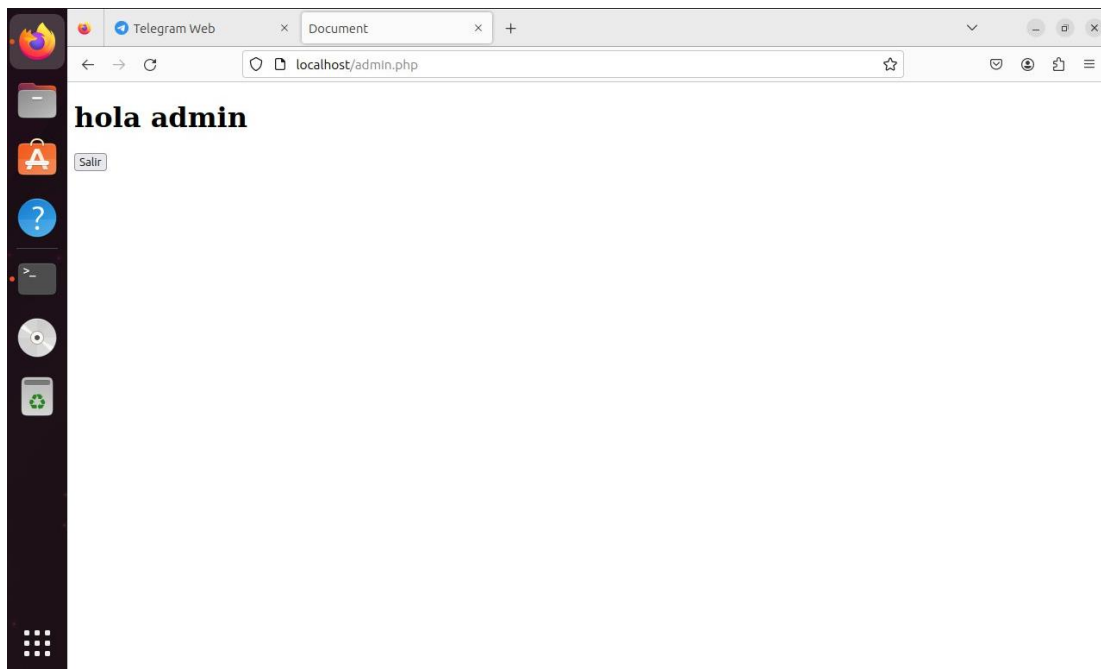


Figura 4. Sitio principal del Administrador

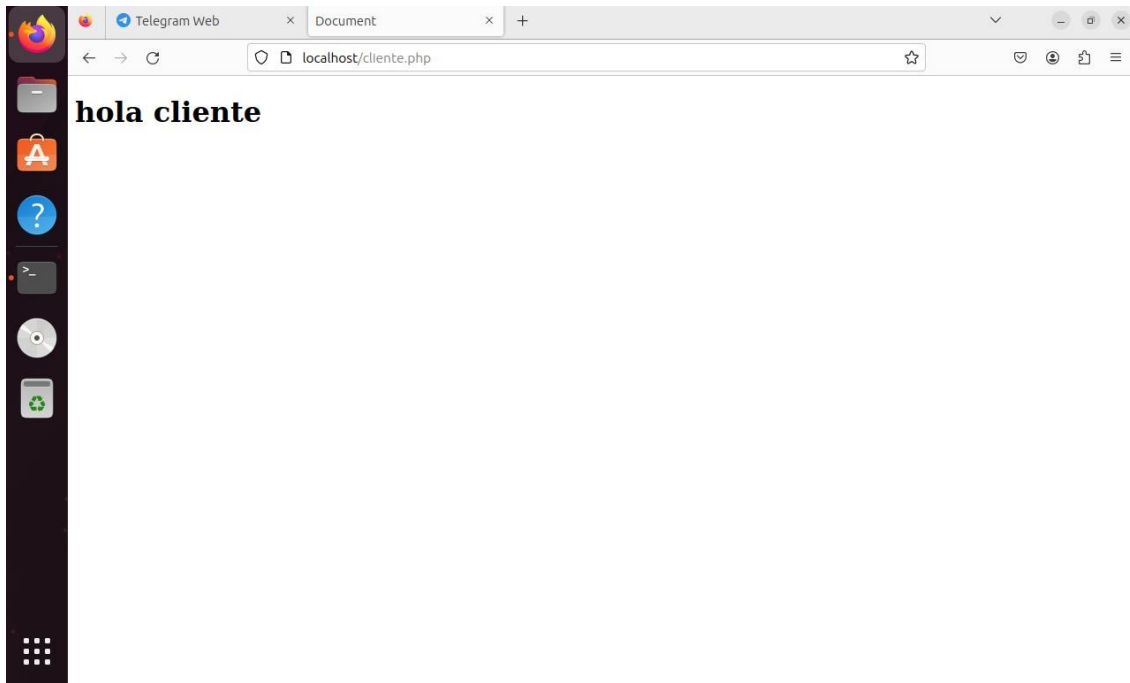


Figura 5. Sitio principal del Cliente

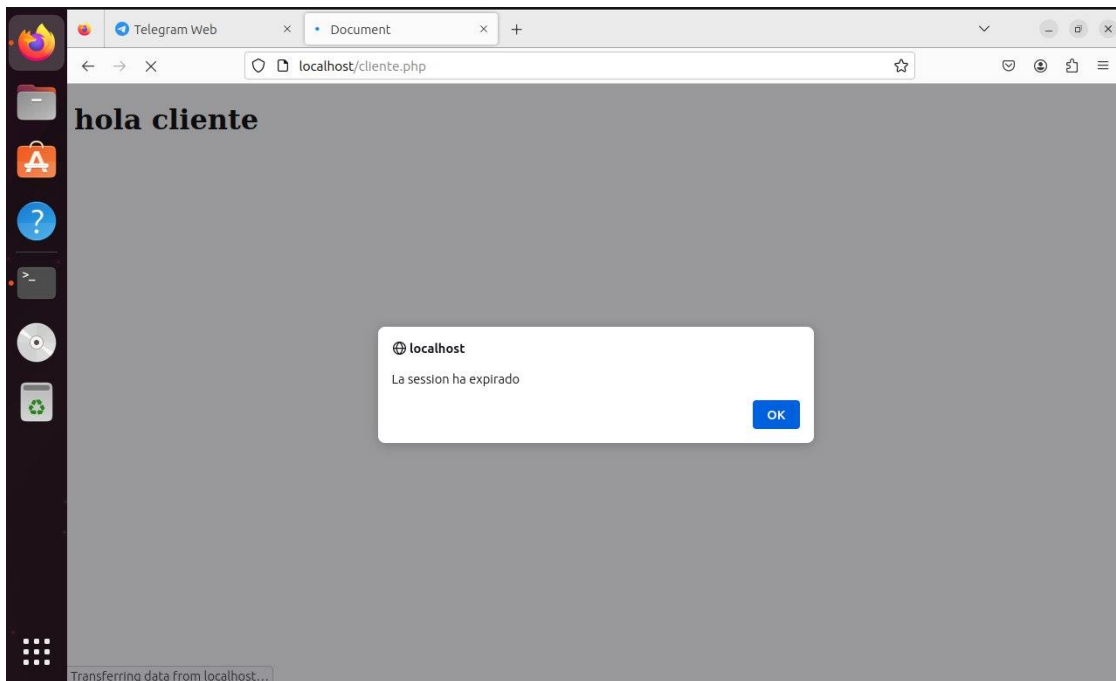


Figura 6. Cerrando sesión del cliente por falta de actividad

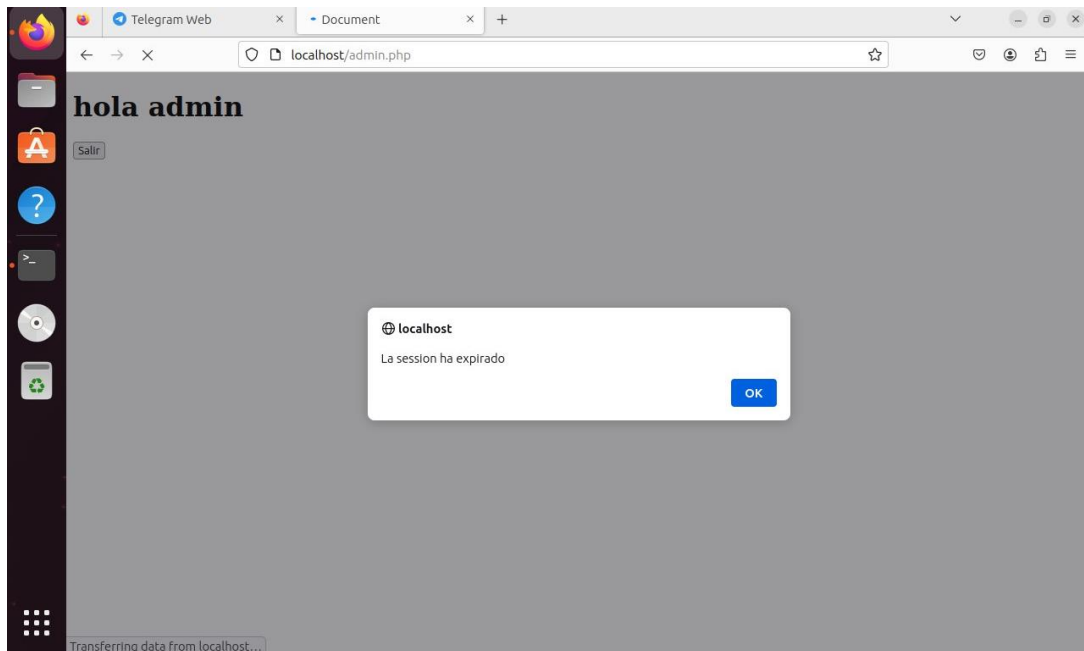


Figura 7. Cerrando sesión del admin por falta de actividad

Por último, el manejo de las sesiones se realizó en PHP, donde se valida que si no hay ninguna solicitud durante 5 segundos, se cierra la sesión y se redirige hacia la pantalla principal.

```
<?php
    $inactive = 5;
    ini_set('session.gc_maxlifetime', $inactive);

    session_start();

    //Time Validation
    if (isset($_SESSION['LAST_ACTIVITY']) && (time() - $_SESSION['LAST_ACTIVITY'] > 10)) {
        // last request was more than 5 seconds ago
        session_unset(); // unset $_SESSION variable for the run-time
        session_destroy(); // destroy session data in storage

        // Send message to user and redirect
        echo '<script language="javascript">';
        echo 'alert("La session ha expirado"); window.location.href="index.html";';
        echo '</script>';
    }
    $_SESSION['LAST_ACTIVITY'] = time(); // update last activity time stamp
?>
```

Figura 8. Manejo de sesión en PHP

Atacar por inyecciones y vulnerabilidades XSS

Para practicar las inyecciones y vulnerabilidades XSS se utilizó la plataforma PortSwigger que es un entorno seguro el cual nos permite poner a prueba las vulnerabilidades básicas de cada uno.

Inyecciones SQL

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
 LAB	PRACTITIONER SQL injection UNION attack, finding a column containing text »	✓ Solved
 LAB	PRACTITIONER SQL injection UNION attack, retrieving data from other tables »	✓ Solved
 LAB	PRACTITIONER SQL injection UNION attack, retrieving multiple values in a single column »	✓ Solved

Figura 9. Todos los laboratorios resueltos en clase

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

Figura 10. Todos los laboratorios resueltos en clase

Falsificar la identidad y explotar solicitudes entre sitios

Las formas principales de Cross Site Scripting son las siguientes:

- Cross Site Scripting puede ocurrir en el script malicioso ejecutado en el lado del cliente.
- Página o formulario falso que se muestra al usuario (donde la víctima escribe credenciales o hace clic en un enlace malicioso).
- En los sitios web con anuncios mostrados.
- Correos electrónicos maliciosos enviados a la víctima.

Este ataque ocurre cuando el usuario malintencionado encuentra las partes vulnerables del sitio web y lo envía como entrada maliciosa apropiada. Se inyecta un script malicioso en el código y luego se envía como salida al usuario final.

FASES DEL ATAQUE CSRF



EXPLOTACIÓN DE SOLICITUDES EN EL SITIO (CSRF)

Figura 11. Explicación 1 del ataque CSRF

FASES DEL ATAQUE CSRF



EXPLOTACIÓN DE SOLICITUDES EN EL SITIO (CSRF)

Figura 12. Explicación 2 del ataque CSRF 2