



TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE TLAXIACO

SEGURIDAD Y VIRTUALIZACIÓN

Nombre de los Integrantes de equipo:

No. Control

Edwin López Santiago

21620123

Yanet González García

21620273

Tema:

Practica 2 : Autorización y Autenticación

Docente:

Ing. Osorio Salinas Edward

Carrera:

Ingeniería en Sistemas Computacionales

Grupo: 7US

Semestre: Séptimo.

Tlaxiaco, Oaxaca. A 05 de septiembre de 2024.



Índice

Introducción.....	3
Desarrollo.....	4
Práctica 2: Autorización y Autenticación	4
Instrucción:	4
1.- Crea una aplicación [web mobile escritorio] que permita loguearse con un usuario y contraseña.	4
2.- Implementa un mecanismo de autorización que permite o deniegue el acceso a ciertas rutas de la aplicación, en este caso la página de perfil y la página de administración si en dado caso el usuario no ha iniciado sesión o no tiene el rol de administrador.....	4
3.- Implemente un mecanismo de autenticación que permita a los usuarios registrarse, iniciar sesión y cerrar sesión.	4
4.- Implementa un mecanismo para cerrar sesión de un usuario si ha pasado un tiempo determinado sin actividad de 5 mins.....	4
PÁGINA WEB	5
MECANISMO DE AUTENTICACIÓN (REGISTRO, LOGIN Y CIERRE DE SESIÓN)	11
MECANISMO DE AUTORIZACIÓN.....	14
(ACCESO A CIERTAS RUTAS SEGÚN ROLES).....	14
MECANISMO DE CIERRE DE SESIÓN POR INACTIVIDAD	15
5.- Investiga y describe los siguientes servicios de autenticación:	20
o LDAP	20
o RADIUS	20
o TACACS+	20
o Kerberos.....	20
6.- Investiga y describe los siguientes servicios de autorización:.....	21
o ACL.....	21
o RBAC.....	21
o ABAC.....	21
o PBAC	21
Conclusión.....	23
Bibliografía.....	24



Introducción

En esta práctica, el objetivo es aprender sobre Autenticación y Autorización, dos conceptos clave en la seguridad de la información. La autenticación nos permite verificar la identidad de un usuario, y la autorización define qué acciones puede realizar ese usuario según su rol. En este apartado, se muestra como se ha desarrollado una página web donde los usuarios pueden registrarse, iniciar sesión y acceder a diferentes secciones según su nivel de permisos.

También se investigó servicios de autenticación y autorización para comprender mejor cómo funcionan y cómo se aplican a la seguridad de los sistemas. La seguridad de la información es un aspecto fundamental para proteger los datos sensibles y garantizar el acceso controlado a los sistemas. A continuación, se visualizará cada paso de la práctica solicitada, de igual forma, investigaciones del tema.



Desarrollo

Práctica 2: Autorización y Autenticación

Instrucción:

1.- Crea una aplicación [web|mobile|escritorio] que permita loguearse con un usuario y contraseña.

- La aplicación debe tener un formulario de inicio de sesión con los campos de usuario y contraseña.
- La aplicación debe tener un formulario de registro con los campos de usuario, contraseña y confirmación de contraseña.
- La aplicación debe decirme si la contraseña es segura o no (extra).
- La aplicación debe tener una página de inicio que sea accesible para cualquier usuario.
- La aplicación debe tener una página de perfil que solo sea accesible si el usuario ha iniciado sesión.
- La aplicación debe tener una página de administración que solo sea accesible si el usuario ha iniciado sesión y tiene un rol de administrador.

2.- Implementa un mecanismo de autorización que permite o deniegue el acceso a ciertas rutas de la aplicación, en este caso la página de perfil y la página de administración si en dado caso el usuario no ha iniciado sesión o no tiene el rol de administrador.

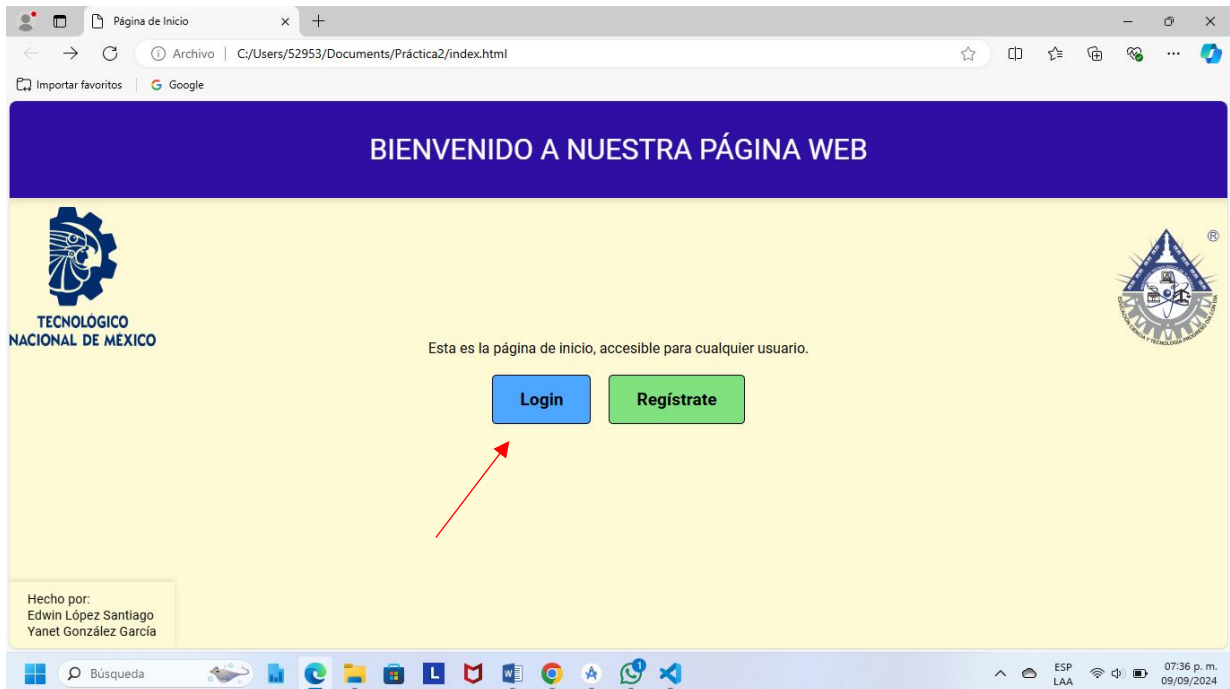
3.- Implemente un mecanismo de autenticación que permita a los usuarios registrarse, iniciar sesión y cerrar sesión.

4.- Implementa un mecanismo para cerrar sesión de un usuario si ha pasado un tiempo determinado sin actividad de 5 mins.

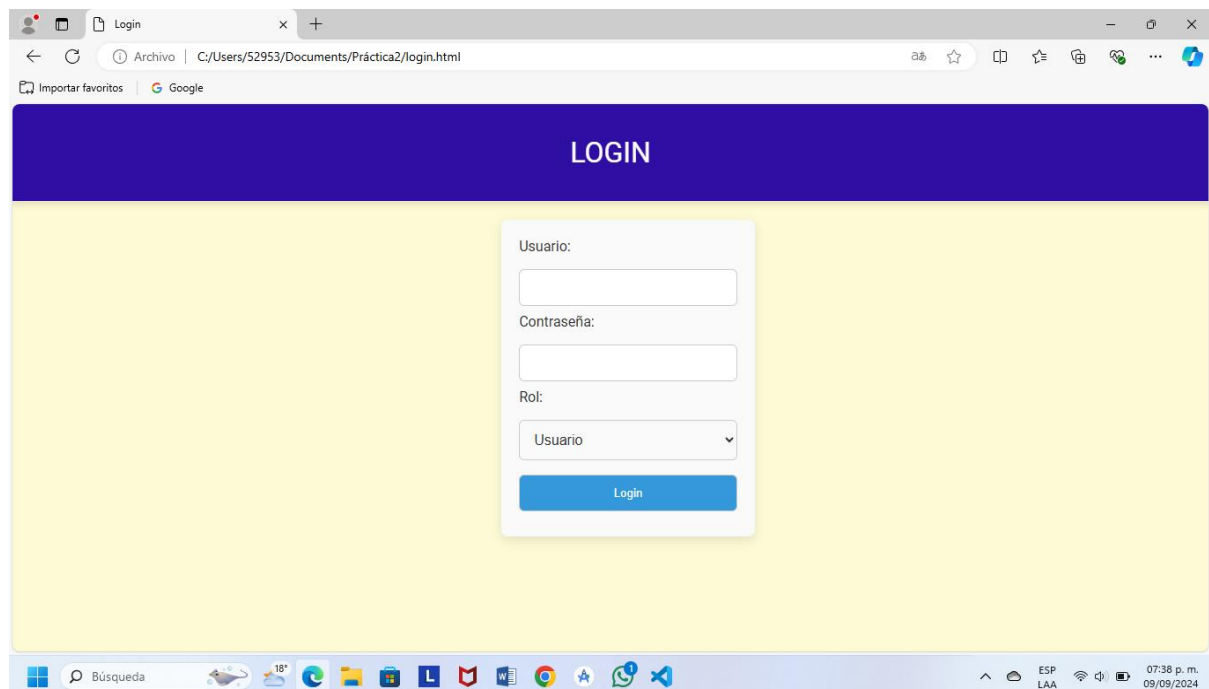
A continuación, se presenta desde el paso 1, 2, 3 y 4.

PÁGINA WEB

1.- La aplicación debe tener un formulario de **“login”** con los campos de usuario y contraseña. La página de inicio de la aplicación es la primera que los usuarios verán al acceder, y está diseñada para darles la bienvenida con un mensaje como "Bienvenido a nuestra página web."

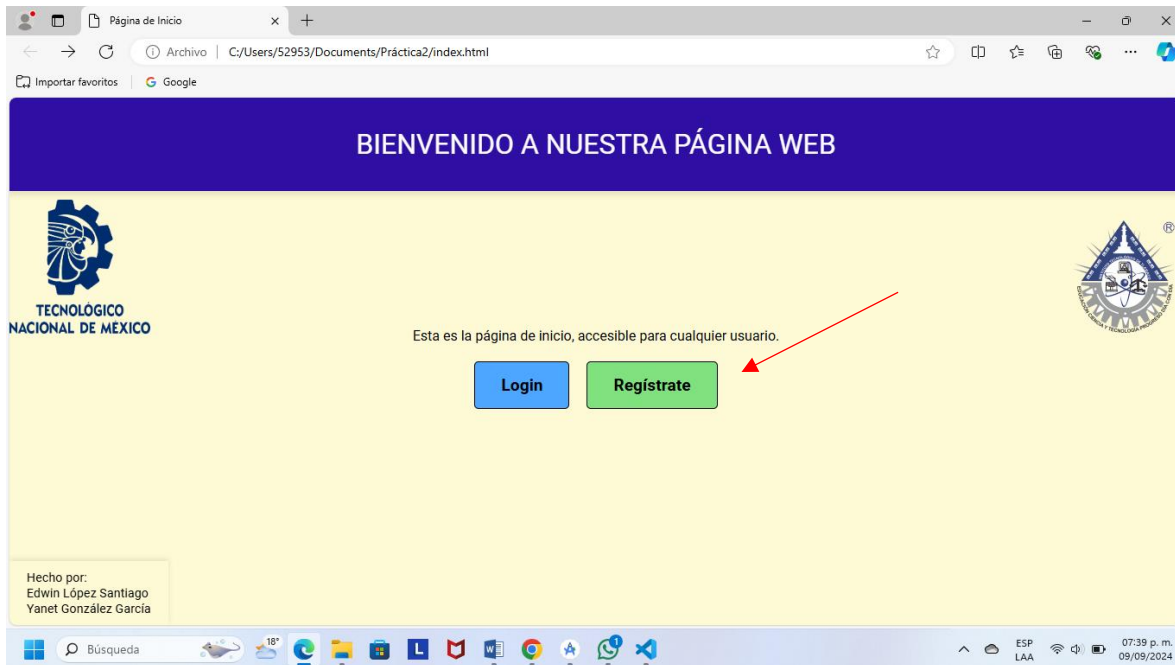


2.- Login con los campos de usuario y contraseña, en nuestro caso agregamos un campo más para el tipo de rol que tenemos.

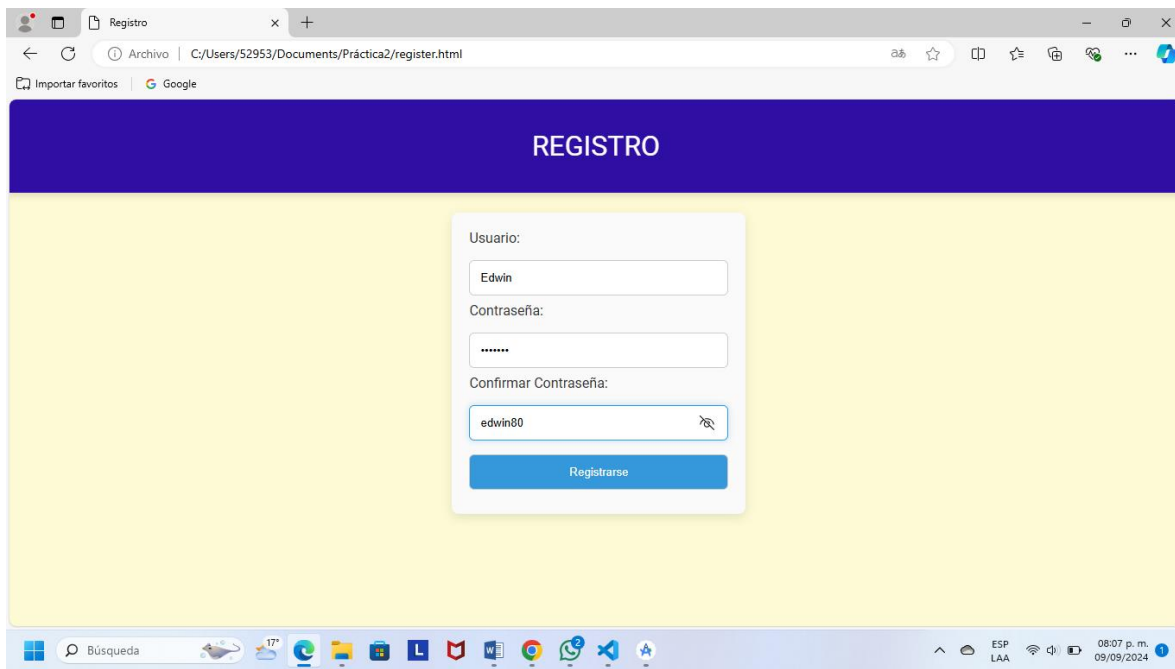




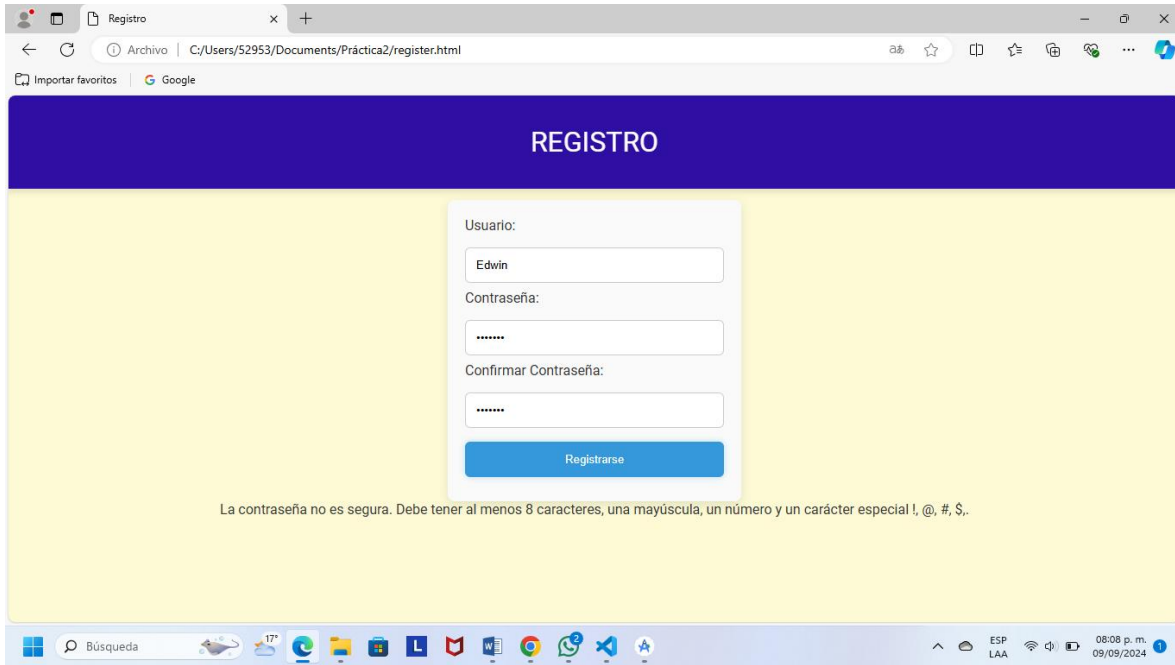
3.- La aplicación debe tener un formulario de **“registro”** con los campos de usuario, contraseña y confirmación de contraseña. La aplicación debe decirme si la contraseña es segura o no.



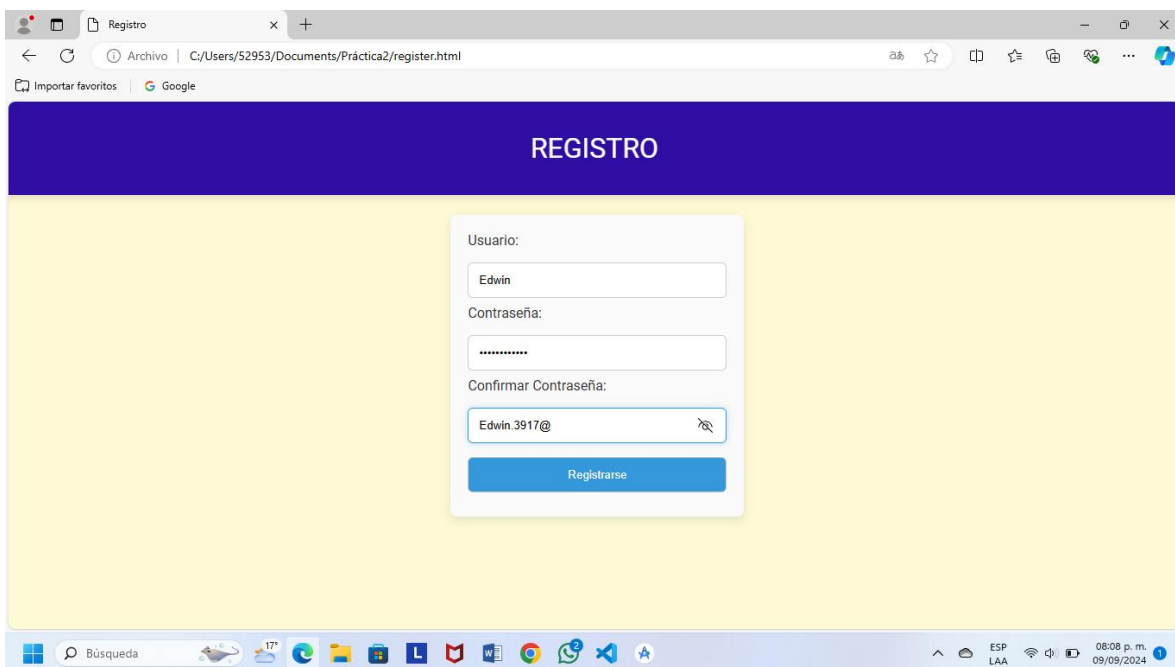
4.- Al darle clic al botón de registro nos arroja una ventana como aparece a continuación. En esta ventana vamos a rellenar lo que nos piden. En este caso se rellenó de la siguiente manera.



5.- Al dar clic al botón de registrarse aparece el siguiente mensaje **“La contraseña no es segura. ¡Debe tener al menos 8 caracteres, una mayúscula, un número y un carácter especial !, @, #, \$,.”** Esto se debe que tenemos validado la contraseña para que tenga una contraseña segura y con las características que debe tener.



6.- Al volver nuevamente a escribir **“Edwin.3917@”** y darle en registrarse nos aparecerá la siguiente ventana.





7.- Al dar clic en “**registrarse**” nos aparece el siguiente mensaje, la cual ya cumple con los requisitos indicados para poder hacer un registro de un nuevo usuario.

Registro

Archivo | C:/Users/52953/Documents/Práctica2/register.html

Importar favoritos | Google

REGISTRO

Usuario:

Edwin

Contraseña:

Confirmar Contraseña:

Registrarse

Registro exitoso.

Búsqueda 17° ESP LAA 08:09 p. m. 09/09/2024


8.- La aplicación debe tener una página de inicio que sea accesible para cualquier usuario. Nuestra página principal es esta donde se encuentran las opciones de login y registrarse.


Página de Inicio

Archivo | C:/Users/52953/Documents/Práctica2/index.html

Importar favoritos | Google

BIENVENIDO A NUESTRA PÁGINA WEB

 **TECNOLÓGICO NACIONAL DE MÉXICO**



Esta es la página de inicio, accesible para cualquier usuario.

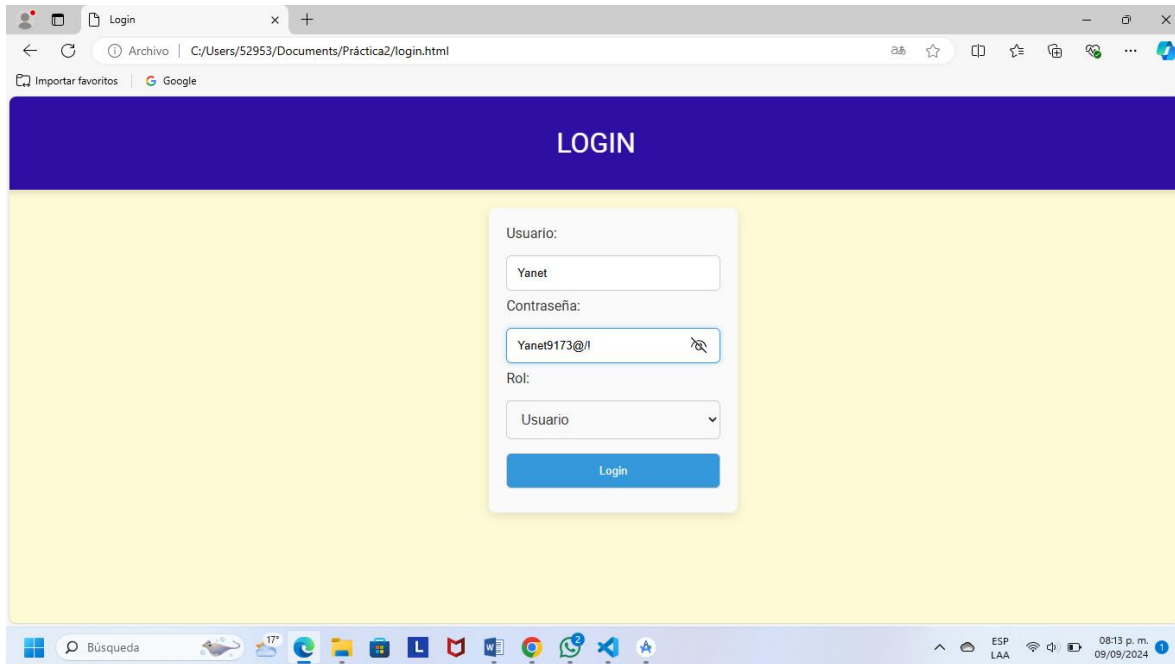
Login Registrarse

Hecho por:
Edwin López Santiago
Yanet González García

Búsqueda 17° ESP LAA 08:10 p. m. 09/09/2024

9.- La aplicación debe tener una página de perfil que solo sea accesible si el usuario ha iniciado sesión. Para realizar dicho punto tenemos que iniciar sesión desde el login y rellenar los campos que nos piden.

Nota: Como es para iniciar sesión debemos de seleccionar el rol de usuario.

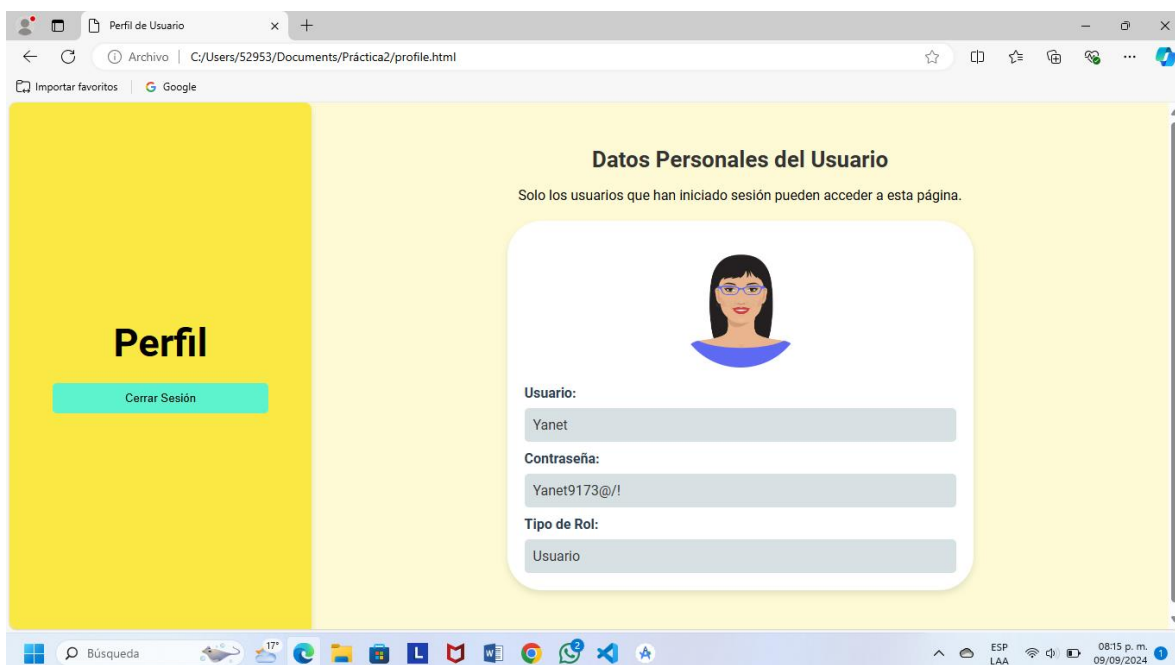


La imagen muestra una ventana de navegador con la pestaña "Login". La URL es "C:/Users/52953/Documents/Práctica2/login.html". El formulario de login tiene un encabezado azul con el texto "LOGIN". El formulario está centrado en un fondo amarillo y contiene los siguientes campos:

- Usuario:
- Contraseña:
- Rol:
- Botón "Login" en azul.

La barra de tareas de Windows muestra la hora 08:13 p.m. del 09/09/2024.

10.- Una vez que hemos accedido esta es la página para nuestro usuario. Esta página está diseñada para que solo los usuarios autenticados puedan acceder a ella, proporcionando un espacio seguro y personalizado para cada usuario registrado.



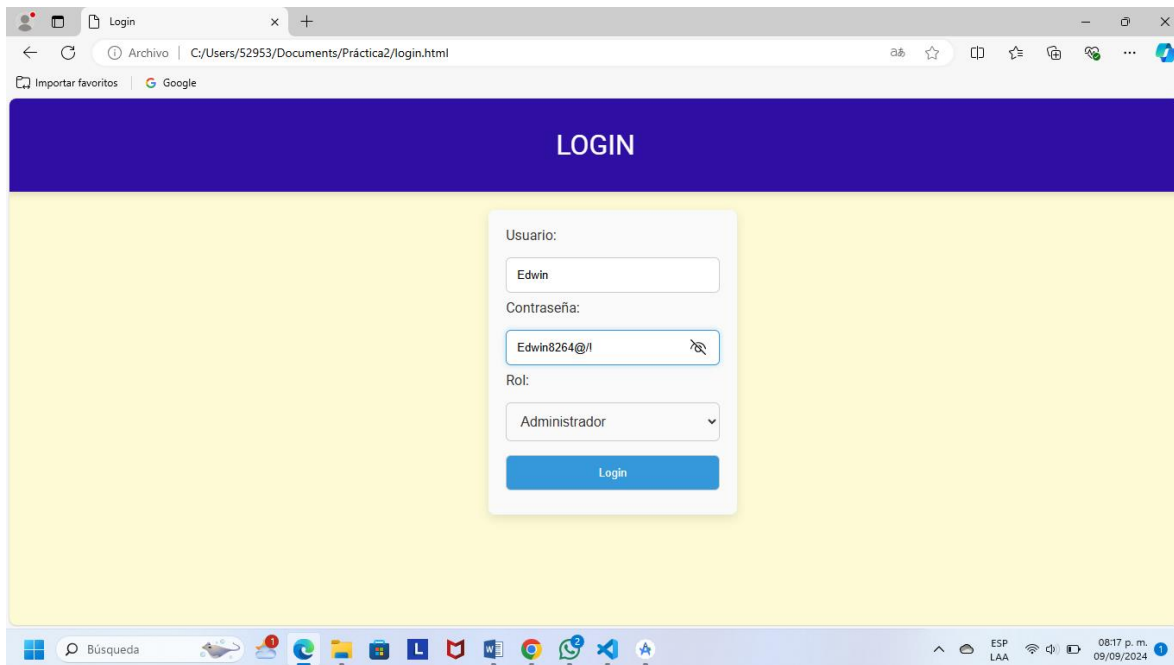
La imagen muestra una ventana de navegador con la pestaña "Perfil de Usuario". La URL es "C:/Users/52953/Documents/Práctica2/profile.html". La página tiene un fondo amarillo y un sidebar izquierdo con el título "Perfil" y un botón "Cerrar Sesión". El contenido principal muestra "Datos Personales del Usuario" con el mensaje "Solo los usuarios que han iniciado sesión pueden acceder a esta página." y un formulario de perfil con un avatar de una mujer y los siguientes campos:

- Usuario:
- Contraseña:
- Tipo de Rol:

La barra de tareas de Windows muestra la hora 08:15 p.m. del 09/09/2024.

11.- La aplicación debe tener una página de administración que solo sea accesible si el usuario ha iniciado sesión y tiene un rol de administrador. Para realizar dicho punto tenemos que iniciar sesión desde el login y rellenar los campos que nos piden.

Nota: como es para iniciar sesión debemos de seleccionar el rol de administrador y utilizaremos otro tipo de usuario con el rol de administrador.

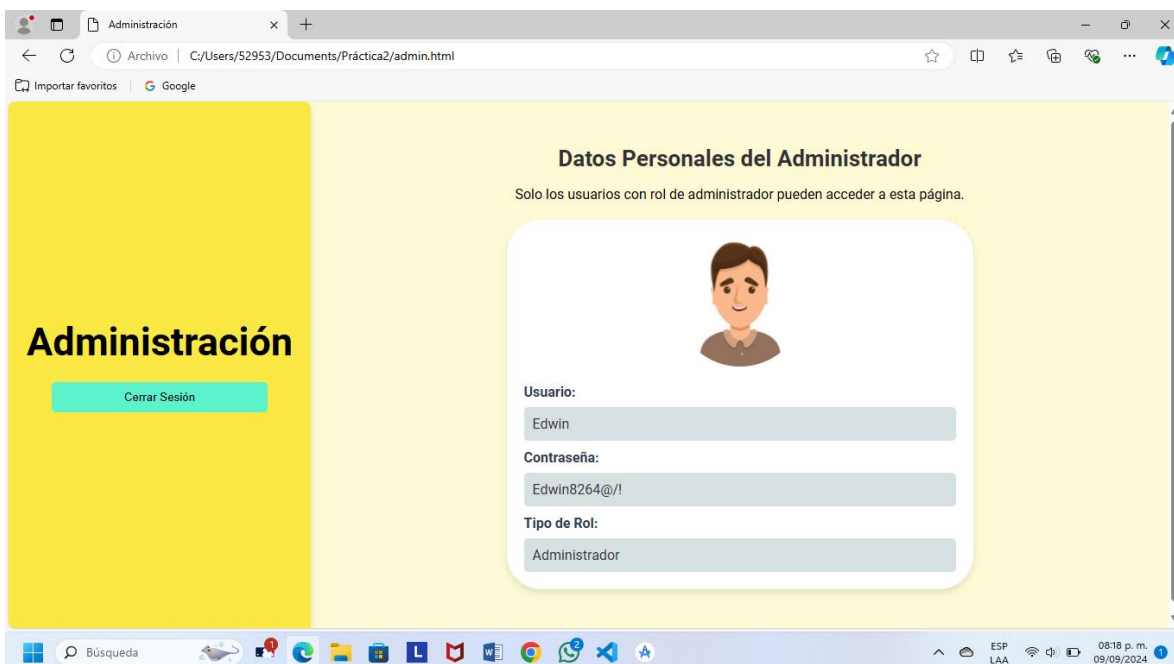


La imagen muestra una ventana de navegador con la URL `C:/Users/52953/Documents/Práctica2/login.html`. El título de la página es "LOGIN". El formulario de login contiene los siguientes campos:

- Usuario: Edwin
- Contraseña: Edwin8264@/l
- Rol: Administrador
- Botón: Login

La barra de tareas en la parte inferior muestra la hora como 08:17 p. m. el 09/09/2024.

12.- Una vez que hemos accedido este es el diseño de nuestra página para nuestro administrador. En esta página, el administrador puede ver información relevante relacionada con su cuenta, como su nombre de usuario, detalles de perfil.



La imagen muestra una ventana de navegador con la URL `C:/Users/52953/Documents/Práctica2/admin.html`. El título de la página es "Administración". El formulario de administración contiene los siguientes campos:

- Usuario: Edwin
- Contraseña: Edwin8264@/l
- Tipo de Rol: Administrador

La barra de tareas en la parte inferior muestra la hora como 08:18 p. m. el 09/09/2024.

13.- Implementa un mecanismo de autorización que permita o deniegue el acceso a ciertas rutas de la aplicación, en este caso la página de perfil y la página de administración si en dado caso el usuario no ha iniciado sesión o no tiene el rol de administrador.

MECANISMO DE AUTENTICACIÓN (REGISTRO, LOGIN Y CIERRE DE SESIÓN)

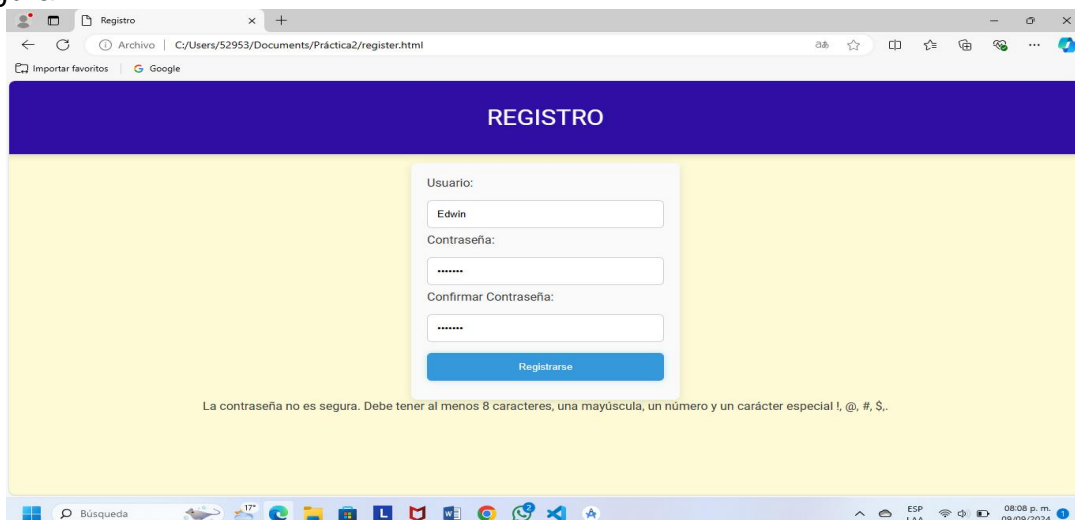
Registro: La parte de registro está en el bloque de código que escucha el evento del formulario registerForm.

```
document.getElementById('registerForm')?.addEventListener('submit', function (e) {
    e.preventDefault();
    const username = document.getElementById('newUsername').value;
    const password = document.getElementById('newPassword').value;
    const confirmPassword = document.getElementById('confirmPassword').value;
    const msgDiv = document.getElementById('passwordMsg');

    const passwordSecurityMessage = isPasswordSecure(password);

    if (passwordSecurityMessage !== "La contraseña es segura.") {
        msgDiv.textContent = passwordSecurityMessage;
    } else if (password !== confirmPassword) {
        msgDiv.textContent = "Las contraseñas no coinciden.";
    } else {
        msgDiv.textContent = "Registro exitoso.";
        // Guardar el nuevo usuario (simulación)
        users.push({ username, password, role: "user" });
    }
});
```

14.- En este apartado se ingresó una contraseña cualquiera, no cumple con todos los requisitos, no cumple con ningún carácter. Este es un breve ejemplo, la cual se debe ingresar una contraseña que cumpla con los requisitos solicitados y sea segura.



La imagen muestra una interfaz web de registro en un navegador. El título de la página es "REGISTRO". El formulario contiene tres campos de texto: "Usuario:" con el valor "Edwin", "Contraseña:" con caracteres ocultos por puntos, y "Confirmar Contraseña:" también con caracteres ocultos. Debajo de los campos hay un botón azul que dice "Registrarse". En la parte inferior del formulario, hay un mensaje de error en rojo que dice: "La contraseña no es segura. Debe tener al menos 8 caracteres, una mayúscula, un número y un carácter especial !, @, #, \$, ..". La barra de direcciones del navegador muestra la ruta "C:/Users/52953/Documents/Práctica2/register.html".

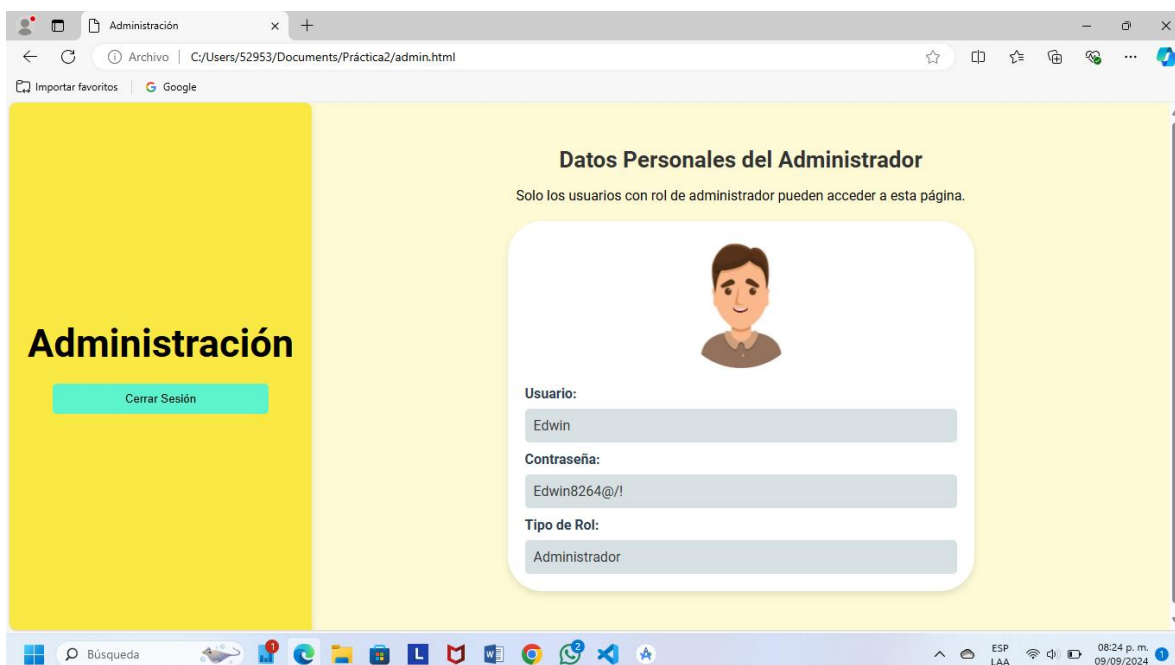
15.- Login: El proceso de inicio de sesión se maneja cuando el usuario envía el formulario loginForm. Se valida si el usuario existe en el arreglo users, y si las credenciales coinciden, se guarda la sesión en el localStorage mediante la función setSession.

```
document.getElementById('loginForm')?.addEventListener('submit', function (e) {
  e.preventDefault();
  const username = document.getElementById('username').value;
  const password = document.getElementById('password').value;
  const errorMsg = document.getElementById('errorMsg');

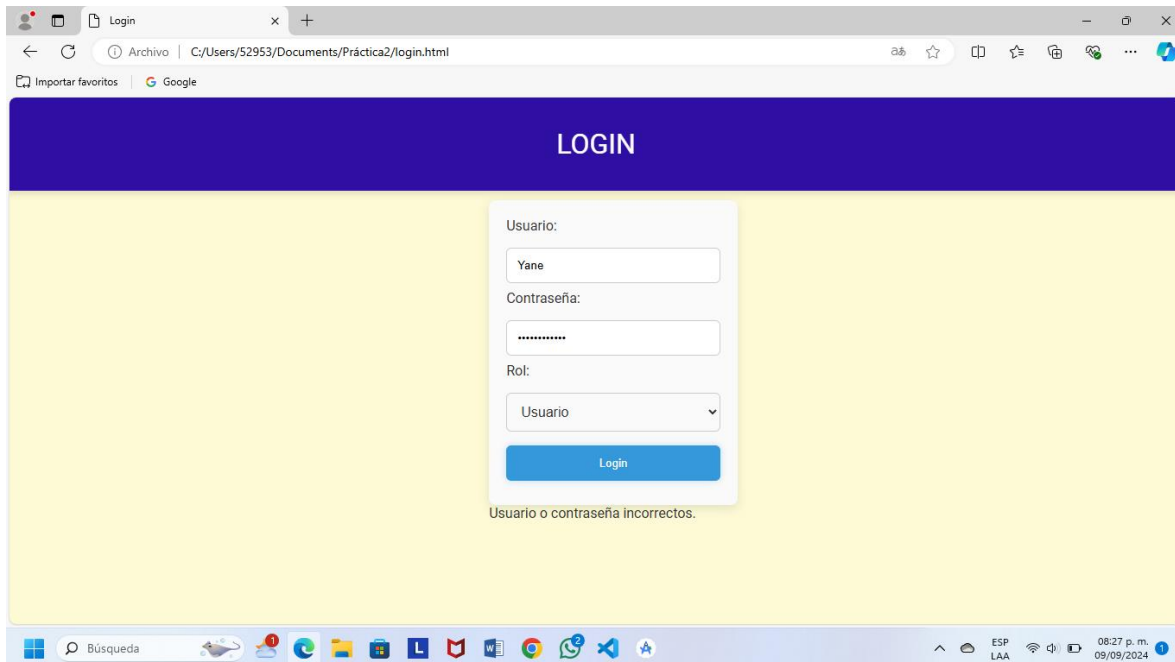
  const user = users.find(u => u.username === username && u.password === password);

  if (user) {
    errorMsg.textContent = "";
    setSession(user); // Establecer la sesión
    if (user.role === "admin") {
      window.location.href = "admin.html";
    } else {
      window.location.href = "profile.html";
    }
  } else {
    errorMsg.textContent = "Usuario o contraseña incorrectos.";
  }
});
```

16.- Cuando se validan las credenciales del login podemos acceder a la página del administrador o usuario y nos dirige a la página de usuario o administrador.



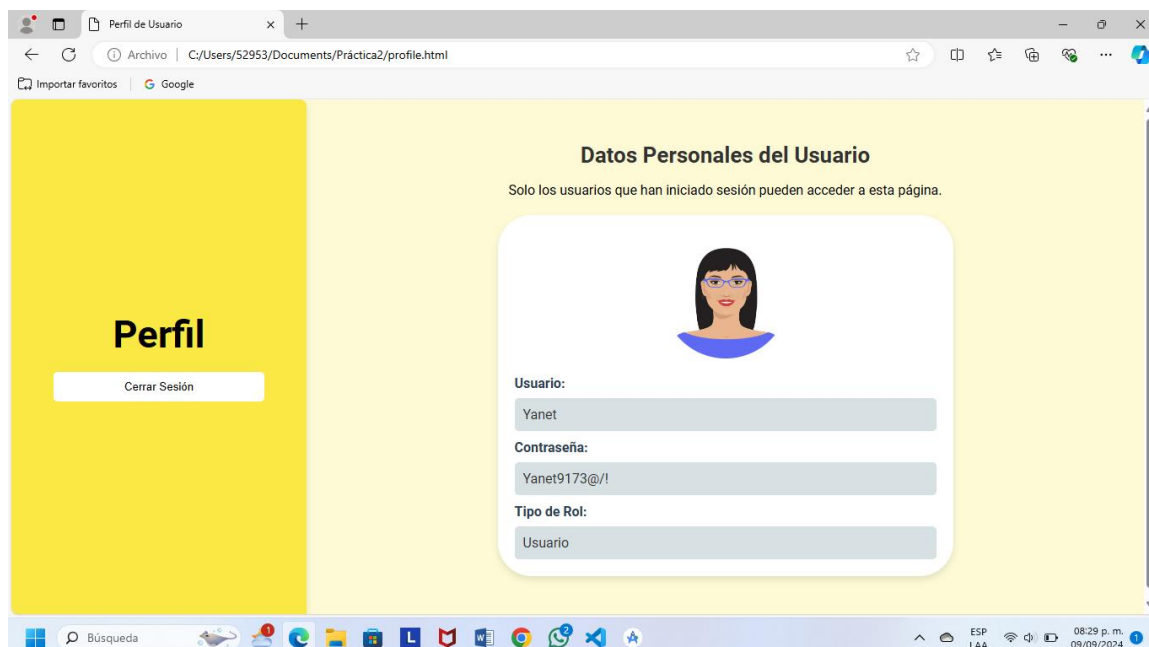
17.- De igual forma pasa si no anotamos bien al usuario nos mandara al siguiente mensaje.



18.- **Cierre de Sesión:** Para cerrar sesión manualmente, se elimina la sesión del localStorage y se redirige al usuario a la página de inicio de sesión.

```
document.getElementById('logoutButton')?.addEventListener('click', function  
( ) {  
    clearSession();  
});
```

19.- Para el cierre de sesión tenemos implementado un botón llamado “Cerrar sesión”.



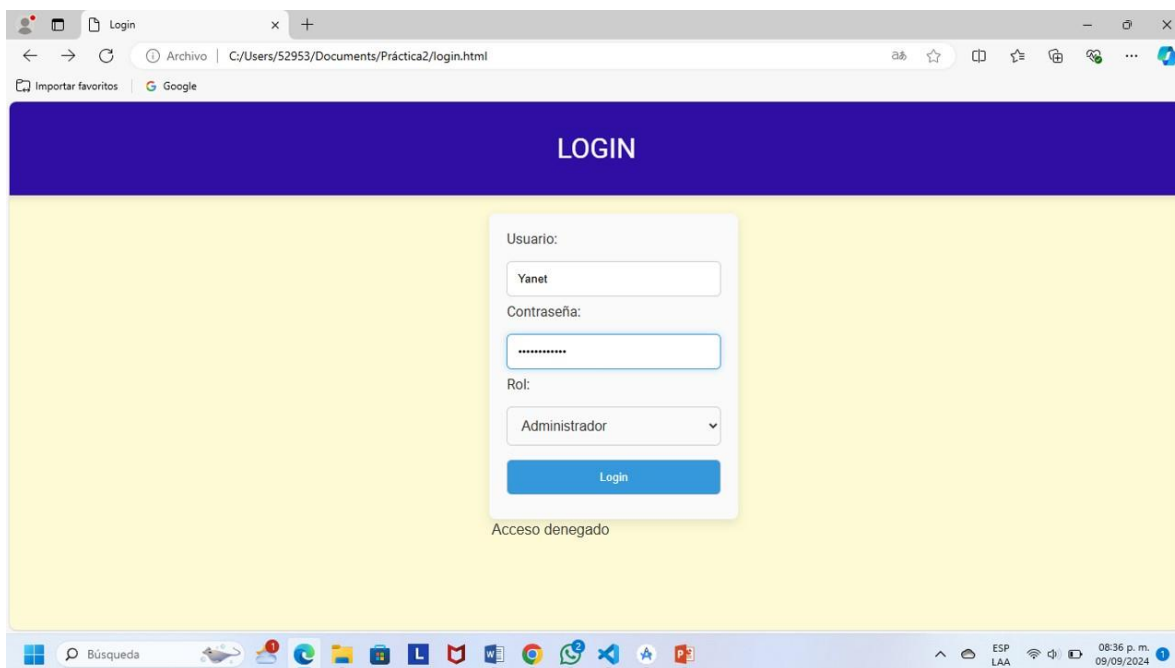
20.- Implementa un mecanismo de autenticación que permita a los usuarios registrarse, iniciar sesión y cerrar sesión.

MECANISMO DE AUTORIZACIÓN (ACCESO A CIERTAS RUTAS SEGÚN ROLES)

Autorización para Rutas: La función `checkAuth` se utiliza para verificar si el usuario tiene acceso a ciertas páginas. Se verifica si el usuario ha iniciado sesión y si tiene el rol adecuado para acceder a páginas específicas como el perfil o la administración. Si el usuario no está autenticado o no tiene el rol adecuado, se redirige a la página de inicio de sesión.

```
// Redirigir si no está autenticado o no tiene el rol adecuado
function checkAuth(role = null) {
  const user = getSession();
  if (!user || (role && user.role !== role)) {
    alert("Acceso denegado");
    window.location.href = 'login.html';
  }
}
```

21.- Si el usuario quiere iniciar un acceso con el rol del administrar se denegará el acceso ya que solamente los verdaderos administradores pueden acceder a ella.



La imagen muestra una interfaz web de login en un navegador. El título de la página es "LOGIN". El formulario de login contiene los siguientes campos:

- Usuario:
- Contraseña:
- Rol: - Botón: Login

Debajo del formulario, se muestra el mensaje "Acceso denegado". La barra de direcciones del navegador indica la URL: `C:/Users/52953/Documents/Práctica2/login.html`. La barra de tareas en la parte inferior muestra la hora: 08:36 p. m. 09/09/2024.

22.- Este código implementa un mecanismo para cerrar sesión de un usuario si ha pasado un tiempo determinado sin actividad de 5 mins.

MECANISMO DE CIERRE DE SESIÓN POR INACTIVIDAD

Temporizador de Inactividad: Se resetea el temporizador de inactividad cada vez que el usuario interactúa con la página (moviendo el mouse o presionando teclas). Si pasan 5 minutos sin actividad, se cierra la sesión automáticamente.

```
// Tiempo máximo de inactividad (5 minutos en milisegundos)
const MAX_INACTIVITY_TIME = 5 * 60 * 1000;

// Variables para controlar la sesión y el tiempo de inactividad
let inactivityTimer;

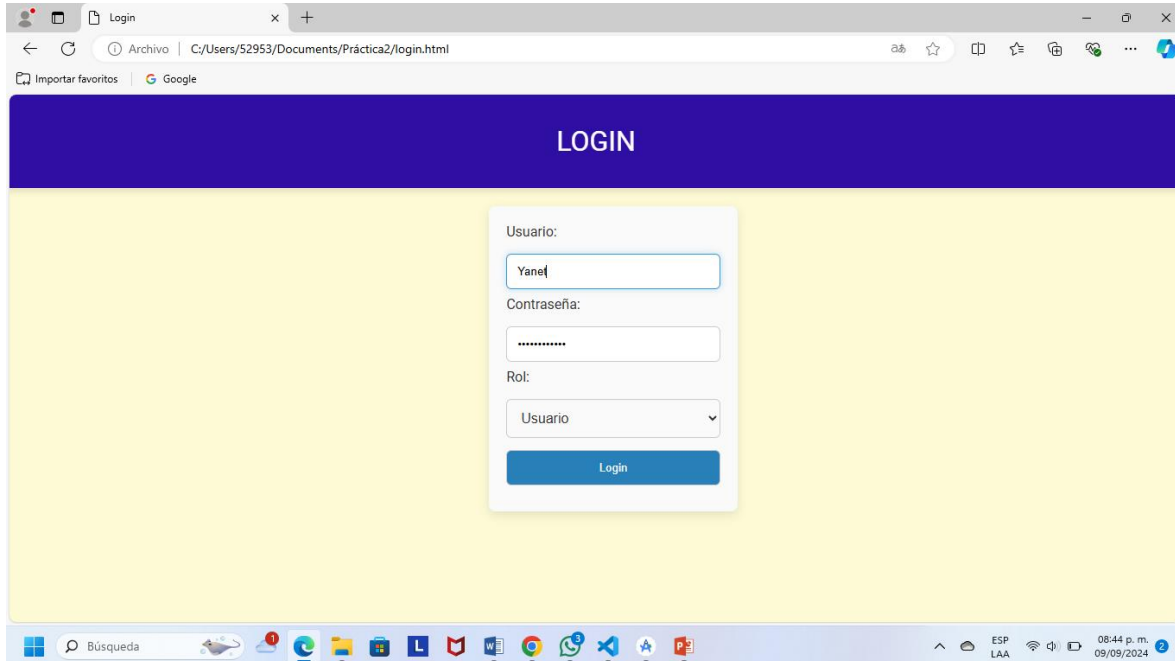
// Guardar sesión en localStorage
function setSession(user) {
  localStorage.setItem('currentUser', JSON.stringify(user));
  resetInactivityTimer(); // Resetea el contador de inactividad
}

// Eliminar sesión (Cerrar sesión)
function clearSession() {
  localStorage.removeItem('currentUser');
  window.location.href = 'index.html';
}

// Resetea el temporizador de inactividad
function resetInactivityTimer() {
  if (inactivityTimer) {
    clearTimeout(inactivityTimer);
  }
  inactivityTimer = setTimeout(() => {
    alert("Sesión expirada por inactividad.");
    clearSession();
  }, MAX_INACTIVITY_TIME);
}

// Control de inactividad: resetea el temporizador con cualquier interacción
window.onload = resetInactivityTimer;
window.onmousemove = resetInactivityTimer;
window.onkeypress = resetInactivityTimer;
```

23.- Para hacer este punto lo haremos iniciando sesión con el login para acceder a la página de cualquier rol y si no hacemos un movimiento con el mouse o el teclado se expira nuestra sesión esto está habilitado para las sesiones de usuario y administrador.



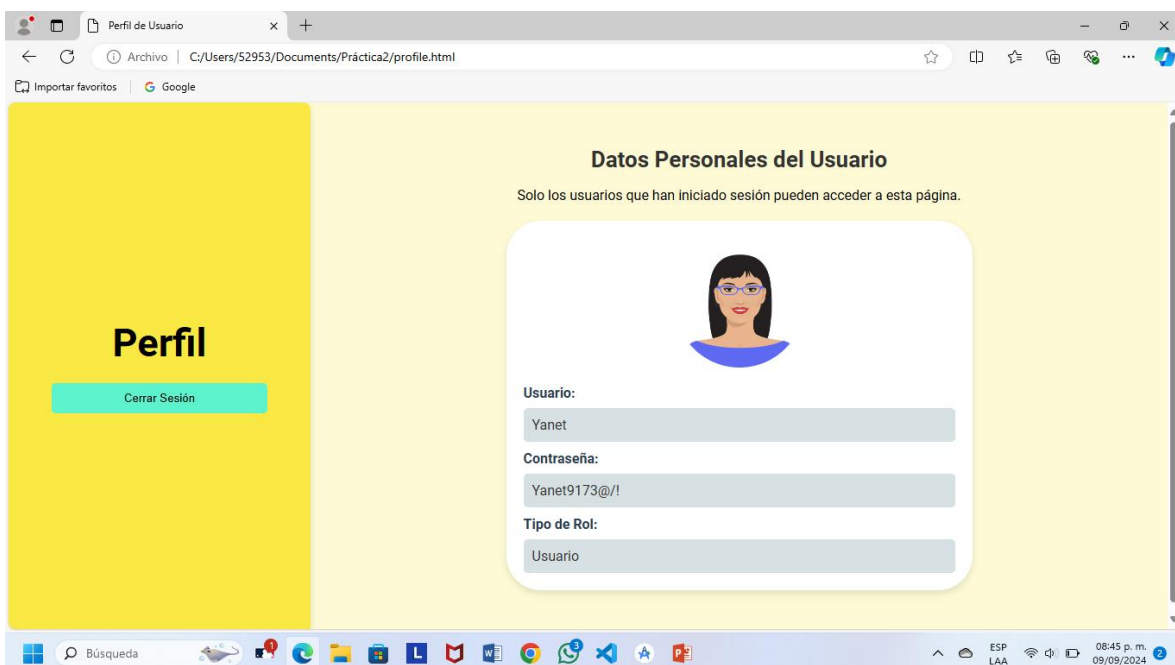
La imagen muestra una ventana de navegador con la URL `C:/Users/52953/Documents/Práctica2/login.html`. El título de la página es "LOGIN". El formulario de login contiene los siguientes campos:

- Usuario:
- Contraseña:
- Rol:

Hay un botón "Login" debajo de los campos. La barra de tareas en la parte inferior muestra la hora como 08:44 p. m. el 09/09/2024.

24.- Ya estamos en la sesión del **usuario** y no haremos ningún movimiento por 5 minutos y vamos a esperar a que expire nuestra sesión.

Nota: En mi reloj son a las 8:45 por default nos tiene que expirar la sesión a las 8:50 minutos.

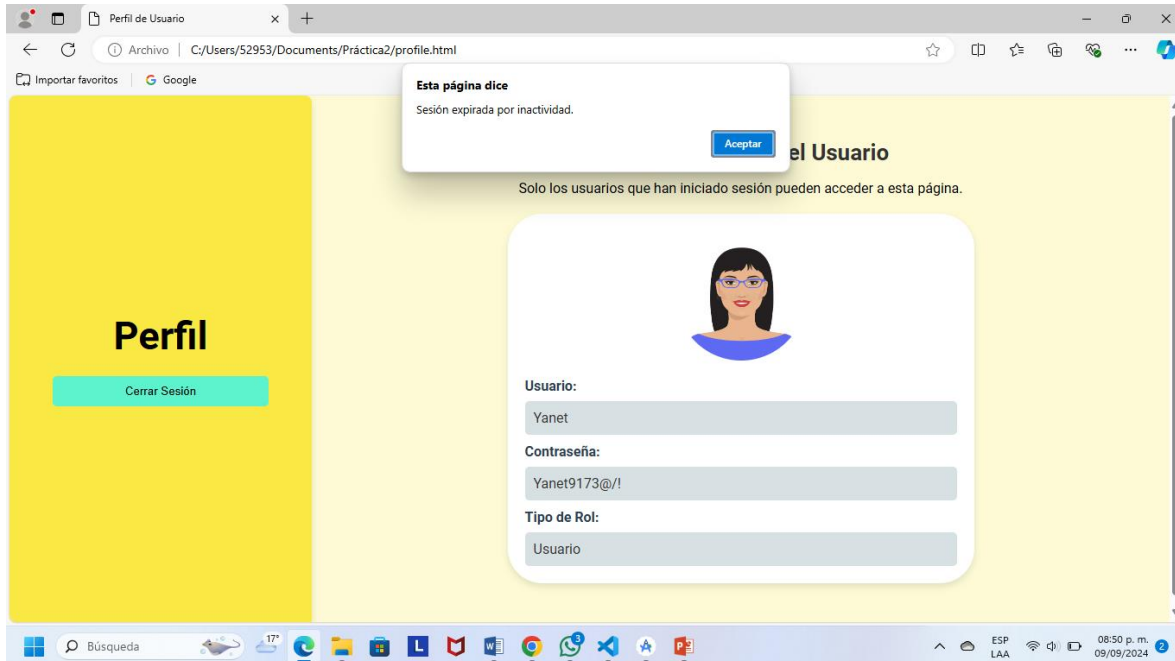


La imagen muestra una ventana de navegador con la URL `C:/Users/52953/Documents/Práctica2/profile.html`. El título de la página es "Perfil de Usuario". El contenido principal muestra:

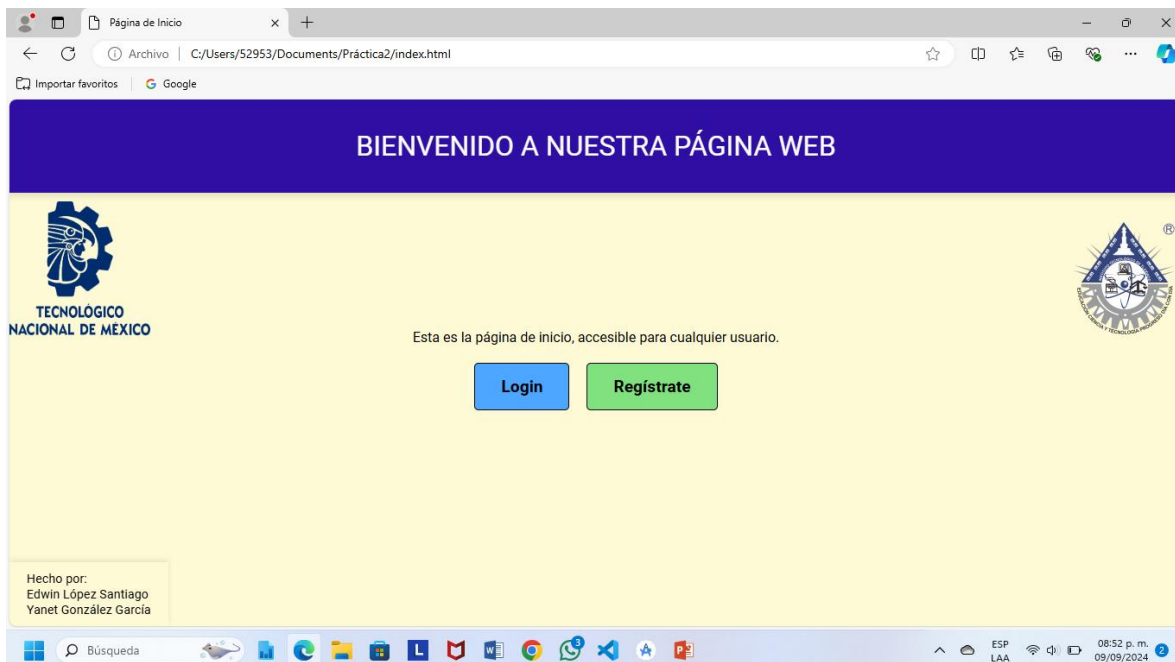
- Datos Personales del Usuario**
- Solo los usuarios que han iniciado sesión pueden acceder a esta página.
- Un avatar de una mujer con gafas y cabello negro.
- Un formulario con los siguientes campos: Usuario (Yanet), Contraseña (Yanet9173@/!), Tipo de Rol (Usuario).

En la barra lateral izquierda, hay un botón "Cerrar Sesión". La barra de tareas en la parte inferior muestra la hora como 08:45 p. m. el 09/09/2024.

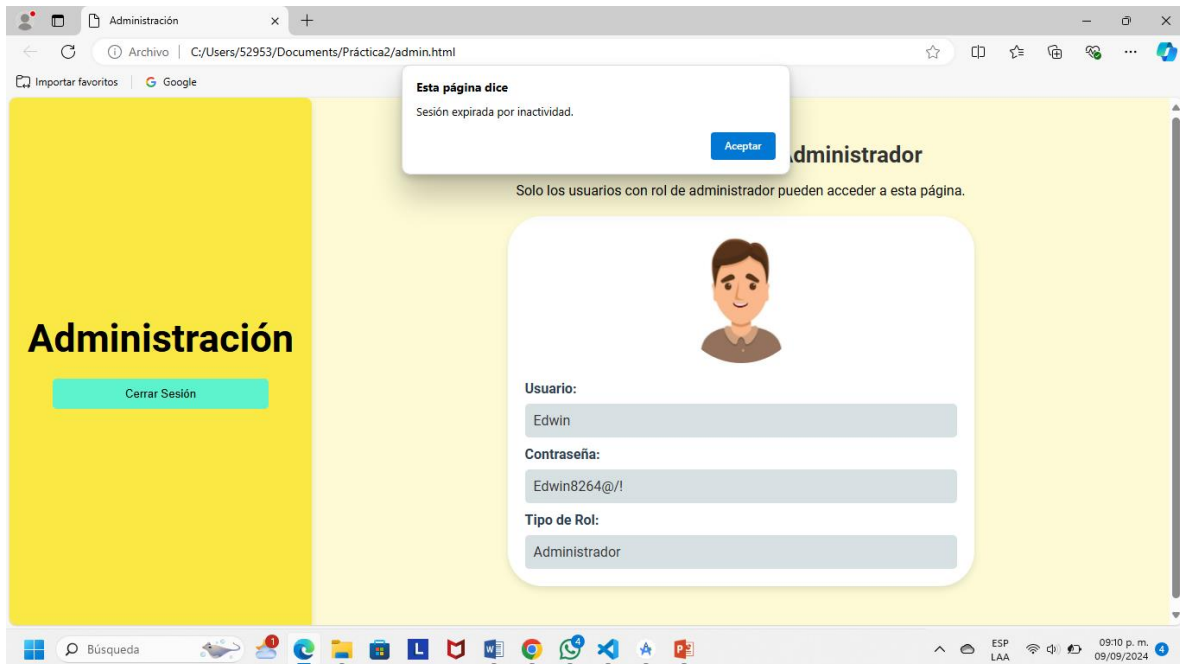
25.- Como lo mencione siendo a las 8:50 nuestra sesión ha sido expirada y nos manda la ventana emergente con el siguiente mensaje de “Esta página dice: Sesión expirada por inactividad” y nos da la opción de aceptar la cual tenemos que aceptar por defecto.



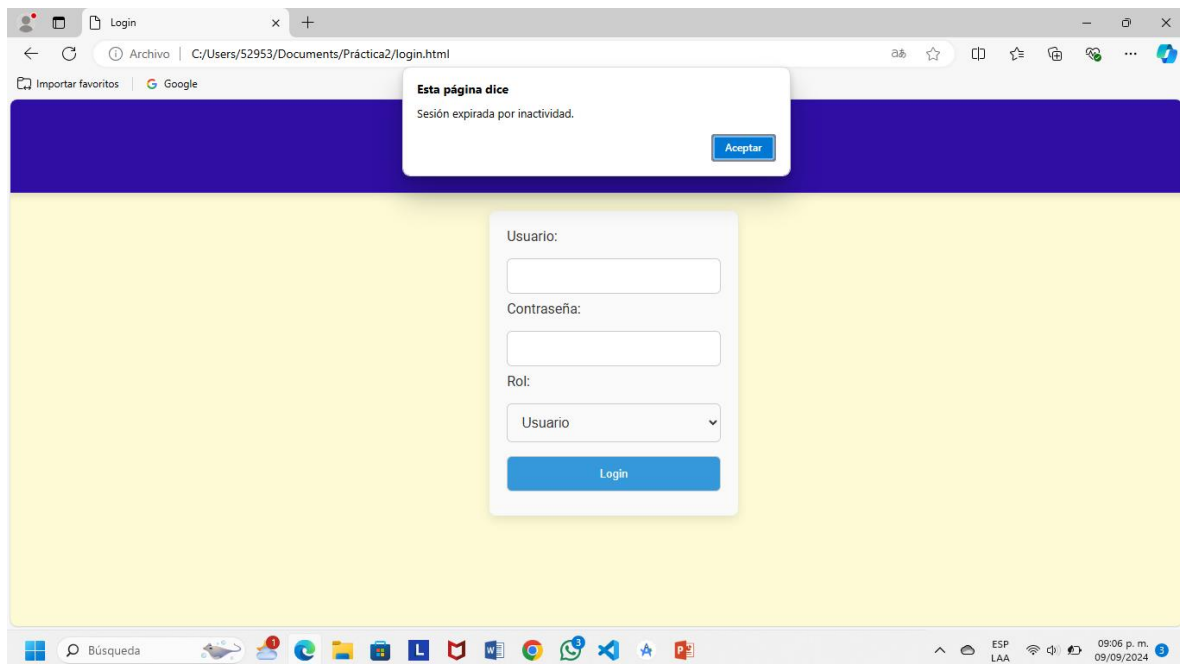
26.- Al presionar el botón de **Aceptar** nos regresa a la página principal donde cualquier usuario puede acceder.



27.- El mismo mecanismo tiene el **rol del administrador** si no se hace ningún movimiento se expira la página en 5 minutos.



28.- El mismo mecanismo tiene en el **Login** si no se hace ningún movimiento se expira la página en 5 minutos.





29.- El mismo mecanismo tiene en la “**página de Registro**” si no se hace ningún movimiento se expira la página en 5 minutos.

En todas las páginas dice el mismo mensaje y la misma opción, dicha opción los manda hasta el inicio donde cualquier usuario puede acceder.

Registro

Archivo | C:/Users/52953/Documents/Práctica2/register.html

Importar favoritos | Google

Esta página dice
Sesión expirada por inactividad.
Aceptar

Usuario:

Contraseña:

Confirmar Contraseña:

Registrarse

Búsqueda

ESP LAA 09:03 p. m. 09/09/2024

5.- Investiga y describe los siguientes servicios de autenticación:

- LDAP
- RADIUS
- TACACS+
- Kerberos

LDAP (Lightweight Directory Access Protocol): Es un protocolo utilizado para acceder y mantener servicios de directorio distribuidos sobre una red IP. LDAP almacena y organiza la información en una jerarquía, permitiendo que los administradores gestionen usuarios, grupos y recursos dentro de una red. Es ampliamente utilizado para la autenticación en aplicaciones empresariales, ya que permite a los sistemas validar credenciales contra un repositorio centralizado. Es compatible con varios sistemas operativos y puede integrarse con otros servicios como Active Directory.

RADIUS (Remote Authentication Dial-In User Service): Es un protocolo de red que proporciona autenticación centralizada, autorización y contabilidad (AAA) para usuarios que se conectan y usan un servicio de red. RADIUS es comúnmente utilizado por proveedores de servicios de Internet y redes empresariales para autenticar usuarios en conexiones inalámbricas o VPNs. Funciona como intermediario entre los servidores de autenticación y los puntos de acceso, verificando las credenciales del usuario antes de permitir el acceso.

TACACS+ (Terminal Access Controller Access-Control System Plus): Es un protocolo que proporciona servicios AAA, especialmente en redes empresariales y grandes infraestructuras. TACACS+ separa los procesos de autenticación, autorización y contabilidad, lo que ofrece un mayor control y flexibilidad para los administradores de redes. Se utiliza principalmente en dispositivos de red como routers y switches para controlar el acceso de los usuarios administrativos a los recursos del sistema.

Kerberos: Es un protocolo de autenticación diseñado para funcionar en redes abiertas y de cliente-servidor, proporcionando un método seguro para que los usuarios se autentifiquen entre sí. Kerberos utiliza criptografía de clave simétrica y un sistema de "tickets" para permitir que los usuarios se autentifiquen de manera segura sin enviar contraseñas en texto plano. Es muy utilizado en sistemas operativos como Windows y en redes empresariales donde se requiere una autenticación fuerte y centralizada.

6.- Investiga y describe los siguientes servicios de autorización:

- ACL
- RBAC
- ABAC
- PBAC

ACL (Listas de Control de Acceso): Es un mecanismo de autorización que especifica qué usuarios o sistemas tienen permisos para acceder a ciertos recursos en una red o sistema. Las listas de control de acceso contienen una lista de entradas donde cada una define un permiso para un usuario o grupo específico. Estos permisos pueden incluir lectura, escritura, ejecución, etc. LCA es una forma directa y sencilla de controlar el acceso, aunque su administración puede volverse complicada a medida que crece el número de usuarios y recursos.

Características:

- **Simplicidad:** Las listas de control de acceso (LCA) son simples de entender y usar, ya que asignan permisos directamente a usuarios o grupos específicos.
- **Permisos Específicos:** Cada entrada en la lista define qué tipo de acceso tiene un usuario o grupo a un recurso (lectura, escritura, ejecución, etc.).
- **Administración:** Puede volverse compleja a medida que aumenta el número de usuarios y recursos, requiriendo una gestión constante para mantener las listas actualizadas.
- **Granularidad:** Ofrece un control de acceso detallado, pero cada cambio requiere una actualización manual de la lista.

RBAC (Role-Based Access Control): Es un modelo de control de acceso basado en roles, donde los permisos para realizar operaciones están asociados con roles específicos dentro de una organización. En lugar de asignar permisos directamente a los usuarios, se les asignan roles, y cada rol tiene un conjunto de permisos predefinidos. Esto facilita la administración, ya que los permisos no se asignan individualmente, sino en función de los roles que desempeñan los usuarios, lo que mejora la eficiencia y seguridad en sistemas grandes.

Características:

- **Basado en Roles:** Los permisos se asignan a roles en lugar de a usuarios individuales. Los usuarios obtienen permisos al ser asignados a uno o más roles.
- **Escalabilidad:** Facilita la administración en grandes organizaciones, ya que los permisos se gestionan a nivel de rol y no de usuario individual.

ABAC (Attribute-Based Access Control): Es un modelo de autorización en el que los permisos se otorgan en función de atributos de los usuarios, los recursos y el entorno. Los atributos pueden ser cualquier cosa, desde la ubicación del usuario, la hora del día, el tipo de dispositivo que está utilizando o cualquier característica del usuario o recurso. Esto permite un control de acceso más granular y flexible en comparación con RBAC, ya que las decisiones de acceso pueden basarse en una combinación de múltiples atributos.

Características:

- **Basado en Atributos:** Los permisos se basan en una combinación de atributos de usuarios, recursos y contexto (como hora del día, ubicación, tipo de dispositivo).
- **Flexibilidad:** Permite un control de acceso más granular y adaptativo al considerar múltiples factores al tomar decisiones de acceso.
- **Políticas Complejas:** Utiliza políticas basadas en atributos para decidir el acceso, lo que puede permitir configuraciones más complejas.
- **Dinamismo:** Permite adaptaciones en tiempo real basadas en cambios en los atributos o contexto.

PBAC (Policy-Based Access Control): Este modelo de autorización está basado en políticas específicas definidas por una organización. Las políticas determinan las reglas de acceso basadas en diferentes condiciones y atributos, que pueden incluir roles, atributos de usuarios y otros factores contextuales. PBAC es similar a ABAC, pero se enfoca más en la definición y aplicación de políticas específicas que gestionan quién puede acceder a qué y bajo qué condiciones.

Características:

- **Basado en Políticas:** La autorización se gestiona mediante políticas definidas por la organización, que especifican las reglas y condiciones para el acceso.
- **Definición de Reglas:** Las políticas pueden incluir una combinación de roles, atributos y otros factores contextuales para determinar el acceso.
- **Flexibilidad en Políticas:** Permite una amplia personalización de reglas y condiciones de acceso, adaptándose a las necesidades específicas de la organización.
- **Centralización:** La administración de acceso se basa en la definición y aplicación de políticas, lo que puede simplificar la gestión en entornos complejos.



Conclusión

En esta práctica, se aplicó de manera práctica los conceptos de autenticación y autorización, que son fundamentales para garantizar la seguridad en aplicaciones web. Desarrollar la página web con formularios de registro e inicio de sesión me permitió entender cómo proteger el acceso a diferentes secciones, dependiendo de si el usuario está autenticado y su rol en el sistema.

Implementar estas funcionalidades no solo nos ayudó a comprender la importancia de controlar quién puede acceder a qué, sino también a explorar servicios de autenticación y autorización como LDAP, RADIUS, TACACS+, Kerberos, ACL, RBAC, ABAC y PBAC. Conocer estos servicios es esencial para aplicar medidas de seguridad más avanzadas en aplicaciones reales. Este trabajo fue muy útil para reforzar nuestros conocimientos y habilidades en seguridad de la información, logrando una aplicación segura y funcional. Fue una experiencia muy enriquecedora y práctica.



Bibliografía

<https://jumpcloud.com/es/blog/what-is-ldap-authentication>

<https://www.redeszone.net/tutoriales/servidores/que-es-servidor-radius-funcionamiento/>

https://www.cisco.com/c/es_mx/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html

<https://www.ibm.com/docs/es/aix/7.3?topic=network-kerberos>

<https://cloud.google.com/storage/docs/access-control/lists?hl=es-419>

<https://www.entrust.com/es/resources/learn/what-is-role-based-access-control>

<https://www.safepaas.com/es/articles/why-pbac-is-the-new-rbac/>