



EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA



TECNOLÓGICO
NACIONAL DE MÉXICO®

Instituto Tecnológico de Tlaxiaco

**TECNOLÓGICO NACIONAL DE MÉXICO
INSTITUTO TECNOLÓGICO DE TLAXIACO**

SEGURIDAD Y VIRTUALIZACIÓN

PRACTICA 2 - AUTORIZACIÓN Y AUTENTICACIÓN

INTEGRANTES:

SANDRA YOLOTZIN REYES GARCÍA	19620079
LUZ KARINA REYES LOPEZ	21620184
JERONIMA ROQUE CABALLERO	21620206

DOCENTE:

ING. OSORIO SALINAS EDWARD

CARRERA:

INGENIERÍA EN SISTEMAS COMPUTACIONALES

7US

Heroica Ciudad de Tlaxiaco, Oaxaca

INDICE

TABLA DE ILUSTRACIONES.....	2
INTRODUCCIÓN.....	3
LOGIN.....	4
INVESTIGACIÓN	11
CONCLUSIÓN.....	18
REFERENCIAS	19

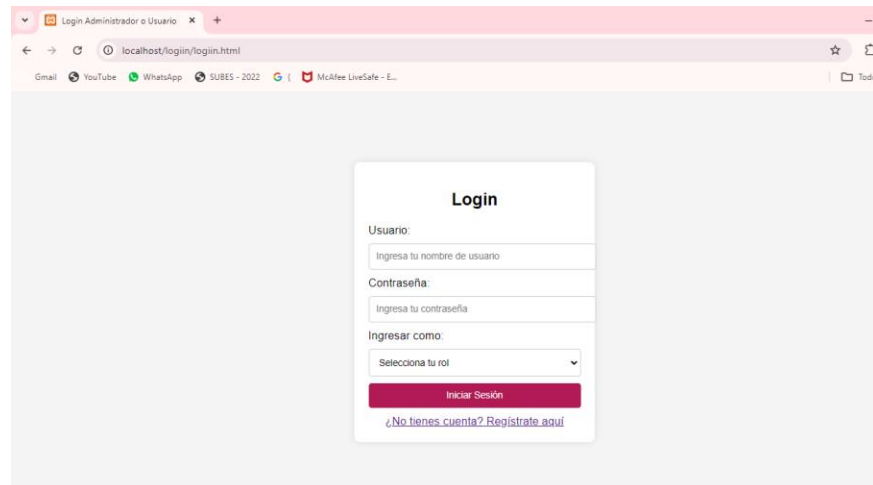
TABLA DE ILUSTRACIONES

Ilustración 1.....	4
Ilustración 2.....	4
Ilustración 3.....	5
Ilustración 4.....	5
Ilustración 5.....	6
Ilustración 6.....	6
Ilustración 7.....	7
Ilustración 8.....	8
Ilustración 9.....	8
Ilustración 10.....	9
Ilustración 11.....	9
Ilustración 12.....	10
Ilustración 13.....	10
Ilustración 14 LDAP.....	11
Ilustración 15 RADIUS.....	12
Ilustración 16 TACAS+.....	13
Ilustración 17 KERBEROS.....	14
Ilustración 18 ACL.....	15

INTRODUCCIÓN

En esta práctica, se desarrollará una página web que implementa funcionalidades básicas de autenticación y autorización, proporcionando una experiencia de usuario segura y controlada. El objetivo principal es gestionar el acceso a diferentes secciones de la página en función de si el usuario ha iniciado sesión y de su rol dentro del sistema. A través de un formulario de registro y un formulario de inicio de sesión, los usuarios podrán crear cuentas, verificar la seguridad de sus contraseñas, y acceder a páginas protegidas como el perfil y la administración, según los permisos correspondientes. Además, la página incluye un sistema para cerrar automáticamente la sesión de un usuario tras 5 minutos de inactividad, mejorando así la seguridad.

LOGIN

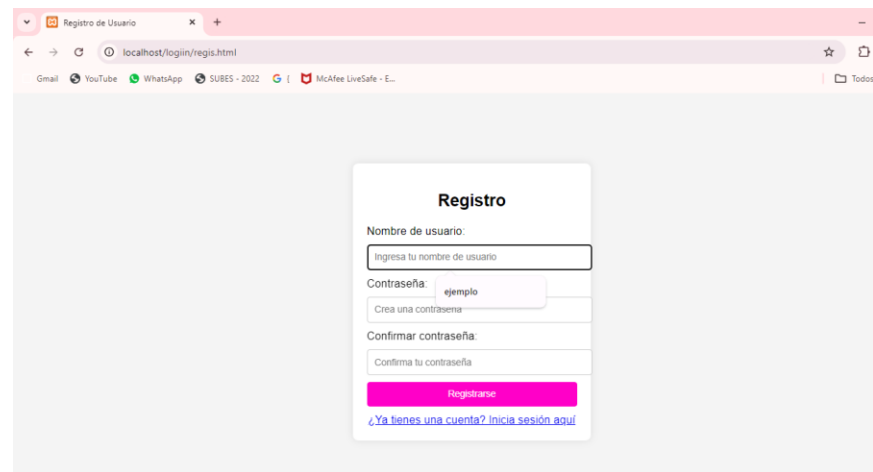


The screenshot shows a web browser window with the title 'Login Administrador o Usuario'. The address bar displays 'localhost/login/login.html'. The login form is centered on the page and contains the following elements:

- Titulo:** Login
- Usuario:** Ingresar tu nombre de usuario
- Contraseña:** Ingresar tu contraseña
- Ingresar como:** Selecciona tu rol (dropdown menu)
- Botón:** Iniciar Sesión
- Enlace:** ¿No tienes cuenta? Regístrate aquí

Ilustración 1

Al iniciar se muestra nuestro login para iniciar sesión, pero en caso de no tener una cuenta, se da clic en la parte debajo del botón de iniciar sesión que dice regístrate aquí, para que nos direcciona al formulario de registro.



The screenshot shows a web browser window with the title 'Registro de Usuario'. The address bar displays 'localhost/login/regist.html'. The registration form is centered on the page and contains the following elements:

- Titulo:** Registro
- Nombre de usuario:** Ingresar tu nombre de usuario
- Contraseña:** ejemplo (with a 'Crea una contraseña' button)
- Confirmar contraseña:** Confirma tu contraseña
- Botón:** Registrarse
- Enlace:** ¿Ya tienes una cuenta? Inicia sesión aquí

Ilustración 2

Para la parte de registro implementamos la validación de contraseñas para verificar que las contraseñas ingresadas coincidan y cumplan con los requisitos de seguridad. Todas las personas que se registren tendrán el rol de usuario, con el motivo de que no cualquier persona pueda ser administrador.

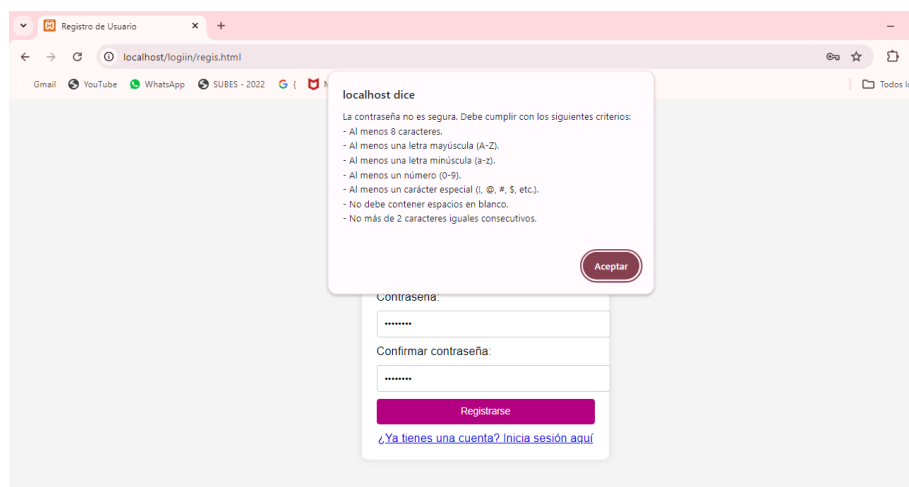


Ilustración 3

Por lo tanto, para registrarse correctamente se debe un nombre, una contraseña segura y confirmar la contraseña, si la contraseña escrita no es segura aparecerá un mensaje de alerta diciendo que la contraseña no es segura y que tiene que cumplir con algunos criterios, pero si la contraseña escrita es segura aparecerá un mensaje que dirá que la contraseña es segura y que el registro ha sido exitoso.

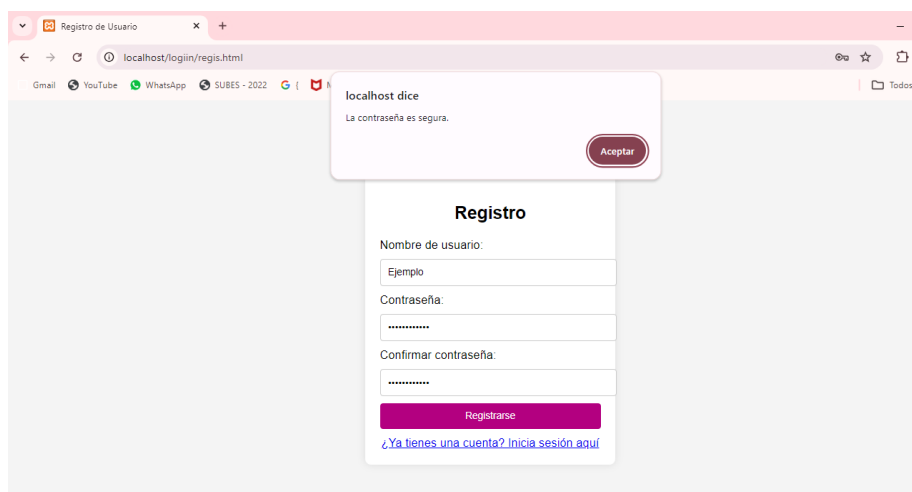


Ilustración 4

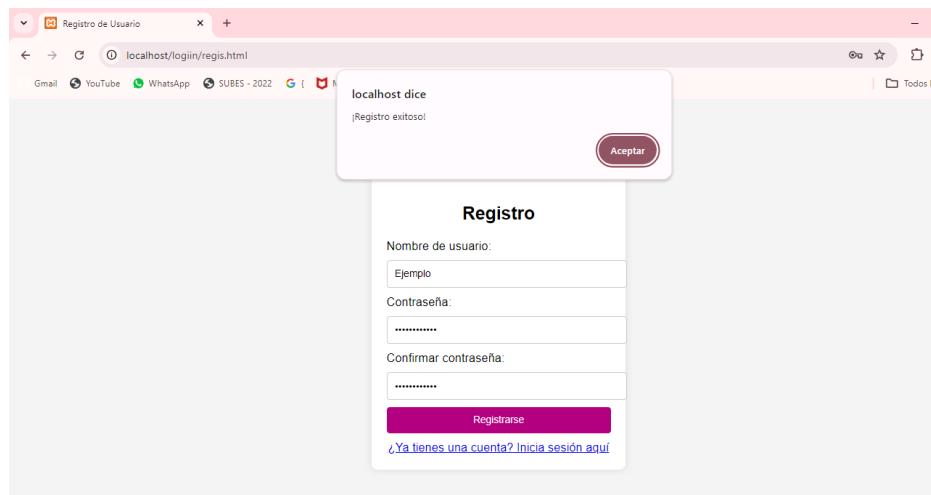


Ilustración 5

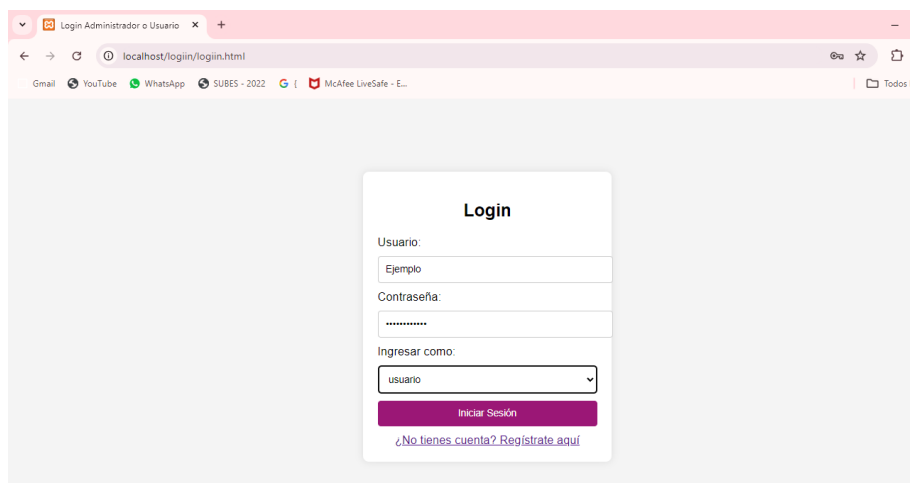
El código PHP que aparece en la imagen es parte del registro de usuarios con la base de datos. Se verifica la conexión y que las dos contraseñas ingresadas por el usuario coincidan y cumplan con los criterios de una contraseña segura

```

registro.php
1  <?php
2  // Configuración de la base de datos
3  $host = "localhost";
4  $dbname = "dbseguridad";
5  $username = "root"; // Usuario por defecto de XAMPP
6  $password = ""; // La contraseña por defecto de XAMPP es vacía
7
8  // Crear la conexión
9  $conn = new mysqli($host, $username, $password, $dbname);
10
11 // Verificar la conexión
12 if ($conn->connect_error) {
13     die("Conexión fallida: " . $conn->connect_error);
14 }
15
16 // Obtener los datos del formulario
17 $newUsername = $_POST['newUsername'];
18 $newPassword = $_POST['newPassword'];
19 $confirmPassword = $_POST['confirmPassword'];
20 $rol = $_POST['rol']; // Obtener el valor del rol
21
22 // Verificar si las contraseñas coinciden
23 if ($newPassword !== $confirmPassword) {
24     echo "Las contraseñas no coinciden.";
25     exit();
26 }
27
28 // Validar que la contraseña sea segura
29 if (strlen($newPassword) < 8 ||
30     !preg_match("/[A-Z]/", $newPassword) ||
31     !preg_match("/[a-z]/", $newPassword) ||
  
```

Ilustración 6

Después de un registro exitoso, el usuario es redirigido a la página de inicio de sesión que es el login. Aquí, el usuario introduce su nombre de usuario y contraseña previamente registrados, selecciona su rol (usuario) y luego inicia sesión, posteriormente se mostrará una página que dice bienvenido usuario, como se puede observar en las siguientes imágenes.



The image shows a web browser window with the address bar displaying 'localhost/login/login.html'. The browser's taskbar at the top includes icons for Gmail, YouTube, WhatsApp, SUBES - 2022, and McAfee LiveSafe - E... The login form itself is centered on a light gray background. It has a title 'Login' in bold. Below the title are three input fields: 'Usuario:' with the placeholder text 'Ejemplo', 'Contraseña:' with masked characters '*****', and 'Ingresar como:' with a dropdown menu showing 'usuario'. A red button labeled 'Iniciar Sesión' is positioned below these fields. At the bottom of the form, there is a link that reads '¿No tienes cuenta? Regístrate aquí'.

Ilustración 7

En la parte de la esquina superior de la página se encuentra un botón color rojo el cual nos sirve para cerrar sesión manualmente, pero en caso de inactividad durante dos minutos se cerrará automáticamente la sesión y mostrará el login para la autenticación.

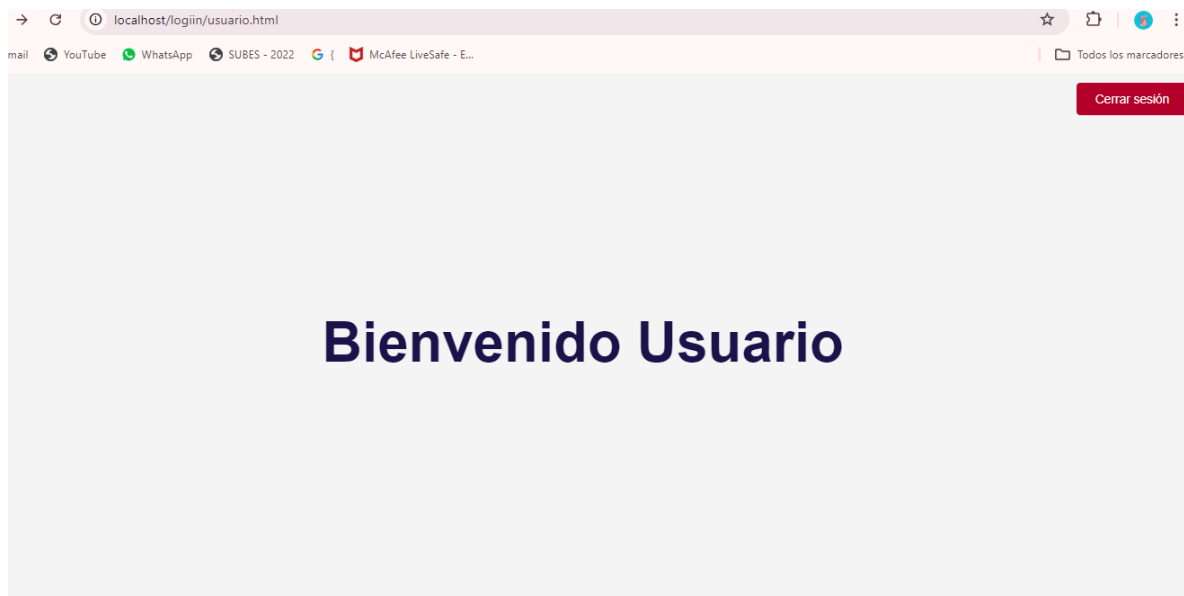


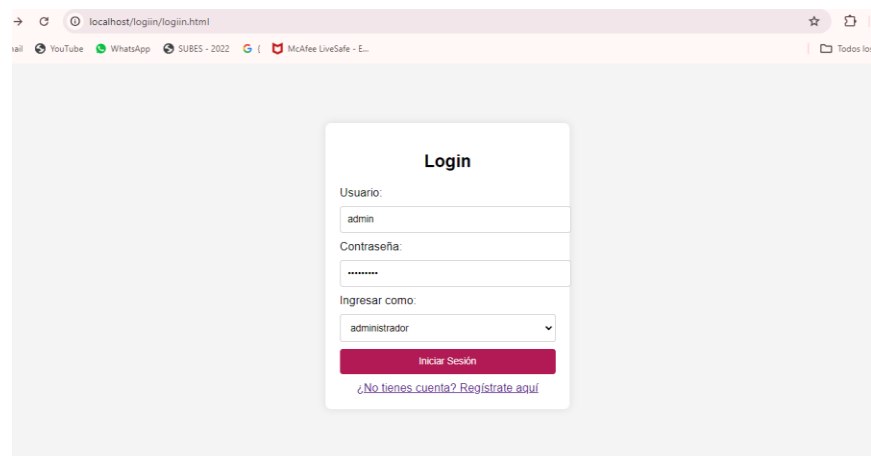
Ilustración 8

La primera parte del código define una función llamada `logout ()` cuyo objetivo es redireccionar al usuario a la página de inicio de sesión (`login.html`) cuando la sesión se cierra. Este mecanismo es útil para cuando el sistema quiere asegurar que el usuario vuelva a autenticarse después de ser desconectado, ya sea manualmente o por inactividad.

```
login.php
1 // Verificar si el formulario ha sido enviado
2
3 if ($_SERVER['REQUEST_METHOD'] === 'POST') {
4     $usuario = $_POST['usuario'];
5     $contraseña = $_POST['contraseña'];
6
7     // Consultar el usuario en la base de datos
8     $sql = "SELECT * FROM usuarios WHERE usuario = ?";
9     $stmt = $conn->prepare($sql);
10    $stmt->bind_param("s", $usuario);
11    $stmt->execute();
12    $resultado = $stmt->get_result();
13
14    // Verificar si se encontró un usuario
15    if ($resultado->num_rows > 0) {
16        $fila = $resultado->fetch_assoc();
17
18        // Verificar la contraseña encriptada
19        if (password_verify($contraseña, $fila['contraseña'])) {
20            $rol = $fila['rol'];
21
22            // Redirigir según el rol
23            if ($rol == 'usuario') {
24                header("Location: usuario.html");
25            } elseif ($rol == 'administrador') {
26                header("Location: administrador.html");
27            } else {
28                echo "Rol desconocido.";
29            }
30        } else {
31            echo "Contraseña incorrecta.";
32        }
33    }
34 }
```

Ilustración 9

En caso de iniciar sesión como administrador, se mostrará la siguiente página que dice bienvenido administrador.



The screenshot shows a web browser window with the address bar displaying 'localhost/login/login.html'. The browser's taskbar at the top includes icons for 'nail', 'YouTube', 'WhatsApp', 'SUBES - 2022', and 'McAfee LiveSafe - E...'. The main content area features a light gray background with a white login form in the center. The form is titled 'Login' and contains the following fields: 'Usuario:' with the text 'admin' entered, 'Contraseña:' with masked characters '*****', and 'Ingresar como:' with a dropdown menu showing 'administrador'. Below these fields is a red button labeled 'Iniciar Sesión'. At the bottom of the form, there is a link that reads '¿No tienes cuenta? Regístrate aquí'.

Ilustración 10

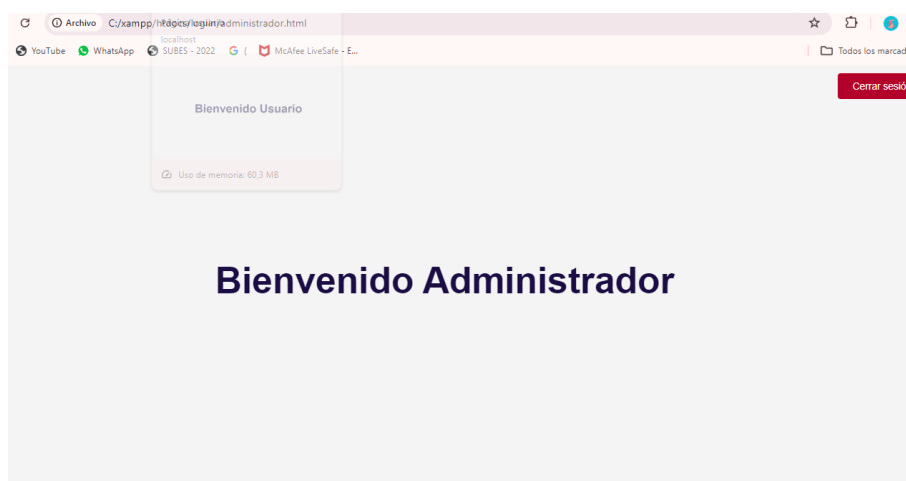


Ilustración 11

La segunda parte del código introduce una variable global llamada timeout. Esta variable será utilizada para almacenar el identificador del temporizador que va a controlar la inactividad del usuario.

La función startTimer() es una de las partes más importantes del código. Su objetivo es iniciar un temporizador que ejecuta la función logout() después de dos minutos (120,000 milisegundos) de inactividad. El método setTimeout es el que permite retrasar la ejecución de una función específica después de un tiempo determinado. En este caso, si el temporizador no es interrumpido, después de dos minutos, el usuario será redirigido a la página de inicio de sesión. Esto es muy útil en aplicaciones donde se requiere una capa adicional de seguridad, asegurando que un usuario no autorizado no pueda acceder a la sesión si el usuario deja la página abierta sin supervisión.

Este código ayuda a garantizar que una sesión de usuario se cierre automáticamente si no se detecta actividad durante un período prolongado.

```
<script>
// Función para cerrar sesión
function logout() {
    // Redirigir a la página de inicio de sesión
    window.location.href = "login.html";
}

// Temporizador para inactividad
let timeout;

// Función para cerrar sesión después de 2 minutos (120000 ms) de inactividad
function startTimer() {
    timeout = setTimeout(logout, 120000); // 2 minutos
}

// Resetear el temporizador al detectar actividad
function resetTimer() {
    clearTimeout(timeout);
    startTimer(); // Reiniciar el temporizador
}

// Escuchar eventos de interacción del usuario
window.onload = startTimer;
document.onmousemove = resetTimer; // Movimiento del ratón
document.onkeypress = resetTimer; // Teclas presionadas
</script>
```

Ilustración 12

También para poder realizar el login creamos una base de datos en phpmyadmin llamada seguridad donde se almacena la información de los usuarios registrados, incluyendo su nombre de usuario, contraseña y rol.

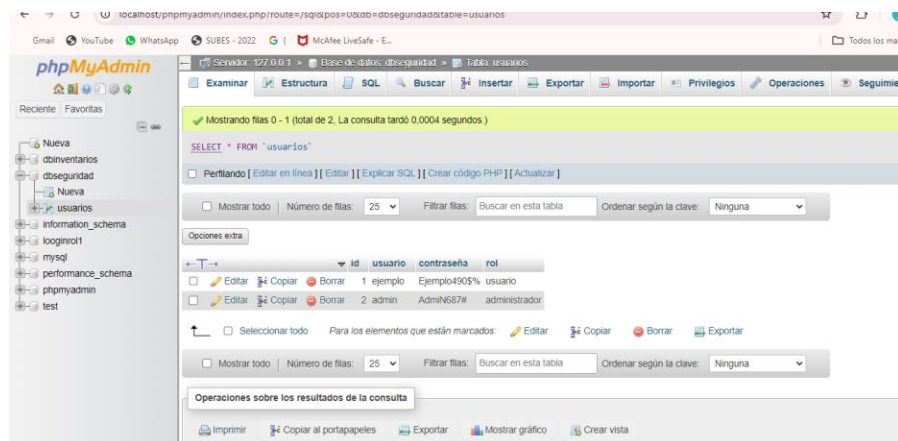


Ilustración 13

INVESTIGACIÓN

SERVICIOS DE AUTENTICACIÓN

LDAP (Lightweight Directory Access Protocol)

¿Qué es LDAP?

LDAP es un protocolo independiente del producto que las aplicaciones pueden usar para acceder y administrar datos extensos a gran velocidad en directorios distribuidos. El directorio activo es un ejemplo de servicios de directorio con los que se puede utilizar este protocolo para comunicarse. El protocolo puede consultar la información del usuario en los directorios, leerla y realizar modificaciones.

Este protocolo, que a menudo se usa en Linux y otros entornos similares a UNIX, ha encontrado numerosas aplicaciones en la industria de las telecomunicaciones, donde admite aplicaciones de operadores inalámbricos telefónicos. Estas aplicaciones normalmente atienden millones de solicitudes de suscriptores de redes telefónicas. También se usa comúnmente en la industria de las aerolíneas.

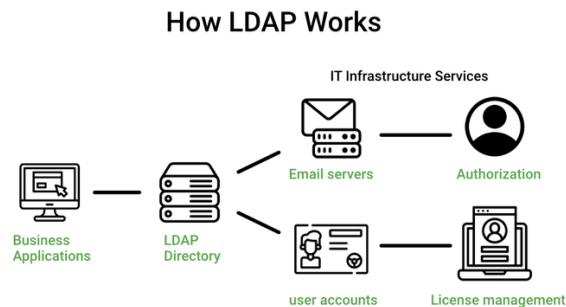


Ilustración 14 LDAP

LDAP se destaca en diferentes áreas, incluida la lectura y modificación rápida de datos, la autenticación de usuarios y la búsqueda. La forma más simple de autenticación LDAP implica verificar la información en un servidor de directorio con la ingresada por el usuario durante el inicio de sesión. Si la información coincide, el usuario está autorizado.

La autenticación en LDAP implica vincularse a un servicio. Durante una operación de vinculación, la aplicación puede consultar los servidores de directorio con la entrada del usuario para su validación. La autenticación LDAP avanzada también podría incluir certificados de cliente y token Kerberos.

RADIUS (Remote Authentication Dial-In User Service)

¿Qué es RADIUS?

RADIUS (Remote Authentication Dial-In User Service) es un protocolo cliente/servidor que gestiona la autenticación, autorización y contabilidad (AAA) en redes. Permite que un servidor de acceso a la red (NAS) autentique usuarios y autorice su acceso a recursos específicos, transmitiendo datos mediante UDP para garantizar rapidez y fiabilidad. RADIUS es ampliamente compatible y asegura que solo usuarios autorizados puedan acceder a una red, siendo uno de los protocolos más utilizados para este propósito.



Ilustración 15 RADIUS

¿Por qué necesitamos RADIUS?

RADIUS (Remote Authentication Dial-In User Service) es un protocolo que proporciona autenticación, autorización y contabilidad (AAA) en redes, protegiéndolas contra accesos no autorizados. Es el más utilizado para gestionar el acceso remoto, permitiendo que un servidor de acceso a la red (NAS) autentique usuarios y transmita la información necesaria a un servidor RADIUS. Esto asegura que solo usuarios autorizados accedan a los recursos de la red, garantizando seguridad y eficiencia mediante el uso del protocolo UDP para una transmisión rápida.

¿Cuáles son las características de RADIUS?

- Estructura cliente/servidor.
- Mecanismo seguro de intercambio de información.
- Buena escalabilidad.

TACACS+ (Terminal Access Controller Access-Control System Plus)

¿QUÉ ES LA AUTENTICACIÓN TACACS+?

TACACS + (Terminal Access Controller Access Control System) es un protocolo de seguridad que proporciona una validación centralizada de los usuarios que intentan obtener acceso a un enrutador o NAS. **TACACS+** proporciona servicios independientes de autenticación, autorización y contabilidad (**AAA**).

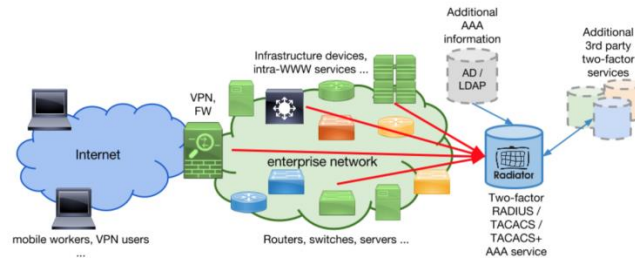


Ilustración 16 TACACS+

¿CÓMO FUNCIONA EL PROTOCOLO TACACS+?

El cliente del TACACS+ se llama Dispositivo de acceso a la red (Nad) o Servidor de acceso a la red (NAS). El dispositivo de acceso a la red se comunicará con el servidor TACACS+ para obtener un aviso de nombre de usuario a través del mensaje "Continuar".

Luego el usuario ingresa un nombre de usuario y el dispositivo de acceso a la red nuevamente se comunica con el servidor TACACS+ para obtener una solicitud de contraseña (mensaje Continuar) que muestra la solicitud de contraseña al usuario, el usuario ingresa una contraseña y luego la contraseña se envía al servidor TACACS+.

Para la contabilidad, el cliente enviará un mensaje de Solicitud al servidor TACACS+ para lo cual el servidor responde con un mensaje de Respuesta indicando que se recibió el registro.

KERBEROS

¿QUÉ ES KERBEROS?

En mitología, Kerberos (también conocido como Cerberus) es un perro grande de tres cabezas que protege las puertas del inframundo para evitar que las almas escapen. En nuestro mundo, Kerberos es el protocolo de autenticación de red informática desarrollado inicialmente en la década de 1980 por científicos informáticos del Massachusetts Institute of Technology (MIT). La idea detrás de Kerberos es autenticar a los usuarios y evitar que las contraseñas se envíen por Internet.



Ilustración 17 KERBEROS

BENEFICIOS DE LA AUTENTICACIÓN DE KERBEROS

El uso de Kerberos como servicio de autenticación tiene algunas ventajas clave.

CONTROL DE ACCESO

El protocolo de autenticación de Kerberos permite un control de acceso efectivo. Los usuarios se benefician de un solo punto para llevar un registro de todos los inicios de sesión y la aplicación de políticas de seguridad.

AUTENTICACIÓN MUTUA

La autenticación de Kerberos permite que los sistemas de servicio y los usuarios se autenticuen entre sí. Durante todos los pasos del proceso, el usuario y el servidor sabrán que las contrapartes con las que interactúan son auténticas.

SERVICIOS DE AUTORIZACIÓN

ACL (Access Control List)

¿Qué es una lista de control de acceso (ACL)?

Una lista de control de acceso, a menudo abreviada como ACL, es una lista que puede definirse como un conjunto de reglas. Estas reglas están diseñadas para proporcionar un cierto nivel de control sobre el acceso a una red o sistema. Básicamente, una ACL dicta quién puede acceder a qué recursos, y qué operaciones pueden realizar en esos recursos. Esta lista puede contener usuarios, grupos o entidades computacionales como procesos o dispositivos.

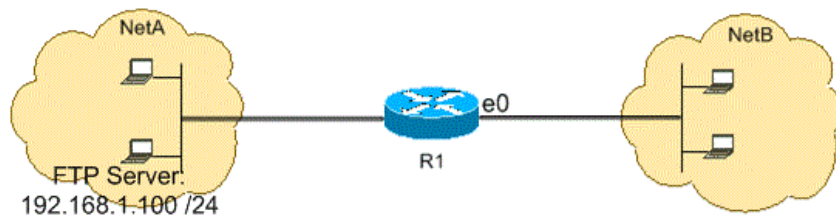


Ilustración 18 ACL

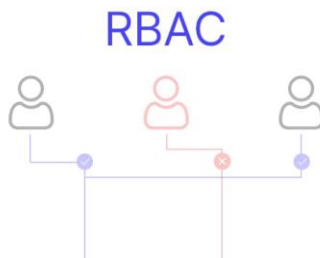
¿Cómo funciona la lista de control de acceso?

El mecanismo de funcionamiento de una ACL es relativamente sencillo. Cuando un usuario o entidad intenta acceder a un recurso, se comprueba la ACL. Si la lista contiene una regla que permite el acceso, se procede a la operación. Por el contrario, si la ACL contiene una regla que deniega el acceso, o si no existe ninguna regla relativa al usuario o entidad, el acceso se deniega. De este modo, una ACL funciona como un gatekeeper, regulando el acceso en función de reglas predefinidas.

RBAC (Role-Based Access Control)

¿QUÉ ES EL CONTROL DE ACCESO BASADO EN ROLES (RBAC)?

El control de acceso basado en roles (RBAC) es un mecanismo de control de acceso que define los roles y los privilegios para determinar si a un usuario se le debe dar acceso a un recurso. Los roles se definen en función de características como la ubicación, el departamento, la antigüedad o las funciones de un usuario.



¿Cuál es la función del RBAC?

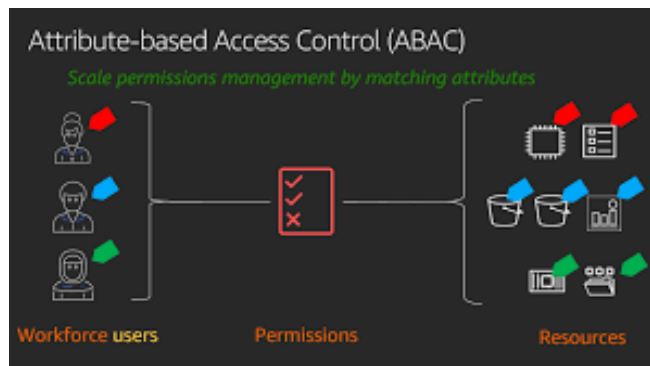
Compromiso con el “principio de mínimo privilegio”: El RBAC ayuda a lograr la seguridad de Zero Trust al asignar la menor cantidad de permisos de acceso a un usuario en función de sus roles. El rol define el conjunto de permisos que necesita el usuario para realizar las tareas comerciales asociadas con su función laboral.

Reducción de la carga administrativa: Utilice el RBAC para agregar y cambiar los roles rápidamente e implementarlos globalmente en todos los sistemas operativos, plataformas y aplicaciones. Además, reduzca la posibilidad de error al asignar permisos de usuario. El RBAC también integra fácilmente a los usuarios de terceros en su red.

Separación de tareas: Como los roles están separados, en teoría, ningún usuario individual puede causar una infracción significativa, ya que un hacker estaría limitado a los recursos a los que se le permitió acceder a esa cuenta.

Cumplimiento mejorado: El RBAC ayuda a las organizaciones a cumplir con las normas de cumplimiento para la protección de datos y la privacidad, así como con los requisitos legales impuestos por los organismos gubernamentales regionales y locales. Esto es posible ya que los departamentos de TI y los ejecutivos pueden gestionar los permisos de acceso a los datos según los roles de los usuarios.

ABAC (Attribute-Based Access Control):



El control de acceso basado en atributos (ABAC) utiliza atributos de usuarios, recursos y el entorno para determinar el acceso. Este enfoque permite una granularidad más alta en las decisiones de autorización, considerando múltiples factores, como la ubicación del usuario, la hora del día y otros contextos relevantes. ABAC es flexible y se adapta bien a entornos dinámicos.

PBAC (Policy-Based Access Control):



El control de acceso basado en políticas (PBAC) utiliza políticas definidas para gestionar el acceso a recursos. Estas políticas pueden basarse en una combinación de reglas que involucran roles, atributos y otros contextos. PBAC permite una gestión más dinámica y adaptativa del acceso, facilitando la implementación de políticas complejas según las necesidades de la organización.

CONCLUSIÓN

En conclusión, al finalizar esta práctica, se habrá creado una página funcional que permite el registro y autenticación de usuarios, así como el control de acceso mediante mecanismos de autorización basados en roles. Se han implementado buenas prácticas de seguridad, como la verificación de contraseñas seguras y el cierre de sesión tras un periodo de inactividad. Estas características son esenciales para asegurar la integridad de los datos y garantizar que solo los usuarios autorizados puedan acceder a secciones sensibles del sistema, como el perfil personal o la página de administración. La experiencia adquirida en esta práctica es clave para desarrollar página web seguras y eficientes.

REFERENCIAS

<https://www.sgrwin.com/es/ldap-o-active-directory-descubre-las-caracteristicas-y-diferencias-de-cada-uno/>

<https://forum.huawei.com/enterprise/es/%C2%BFqu%C3%A9-es-radius-conceptos-b%C3%A1sicos-ciberseguridad/thread/765146523923865600-667212881550258176>

<https://forum.huawei.com/enterprise/es/protocolo-tacacs/thread/667235082160717824-667212882523336704>

<https://www.fortinet.com/lat/resources/cyberglossary/kerberos-authentication#:~:text=Un%20Kerberos%20es%20un%20sistema,web%20que%20visitan%20en%20l%C3%ADnea.>

<https://www.ninjaone.com/es/it-hub/endpoint-management/lista-de-control-de-acceso-acl/>

[https://www.entrust.com/es/resources/learn/what-is-role-based-access-control#:~:text=El%20control%20de%20acceso%20basado%20en%20roles%20\(RBAC\)%20es%20un,las%20funciones%20de%20un%20usuario.](https://www.entrust.com/es/resources/learn/what-is-role-based-access-control#:~:text=El%20control%20de%20acceso%20basado%20en%20roles%20(RBAC)%20es%20un,las%20funciones%20de%20un%20usuario.)