

# Práctica 4. Creación y control de usuarios

Profesor: José M. Luna

Email: [jmluna@uco.es](mailto:jmluna@uco.es)

# Enunciado de prácticas

- Añade a la aplicación web un **sistema de control de acceso mediante cuentas de usuario**, de forma que se permita el acceso a ciertas partes de la aplicación web a usuarios anónimos pero que **el acceso a otras partes de la aplicación web se permita únicamente a usuarios identificados**. La aplicación deberá incluir las funcionalidades habituales en este tipo de sistemas, permitiendo que un visitante crea una cuenta de usuario y que los usuarios identificados puedan desconectarse (dejar de estar identificados) cuando lo deseen. La información relativa a las cuentas de usuario (nombre de usuario y contraseña) deberá almacenarse en la base de datos MySQL, usando algún tipo de encriptación que evite que las contraseñas sean directamente visibles en dicha base de datos.

# Enunciado de prácticas

## Biblioteca

[Listado de libros](#) [Listado de autores](#) [Listado de categorías](#) [Contacto](#) [Login](#)

### Login

Usuario

Contraseña

### Nuevo usuario

Usuario \*

Contraseña \*

Confirmar contraseña \*

Nombre \*

Apellidos

e-mail \*

Teléfono

# Enunciado de prácticas

## Biblioteca

[📖 Listado de libros](#)[👤 Listado de autores](#)[📁 Listado de categorías](#)[✉ Contacto](#)[🚪 Logout](#)

### Listado completo de libros de la biblioteca

Libro	Autor	Categoría	Año	ISBN	Disponible	
El retrato de Dorian Gray	Oscar Wilde	Ficcion clasica	1891	978-8-46-703393-9	No	<a href="#">i</a>
Los juegos del hambre	Suzanne Collins	Novela juvenil	2008	978-8-49-296680-6	No	<a href="#">i</a>
En llamas	Suzanne Collins	Novela juvenil	2009	978-8-49-296682-0	No	<a href="#">i</a>
Sinsajo	Suzanne Collins	Novela juvenil	2010	978-8-49-296681-3	No	<a href="#">i</a>
Romeo y Julieta	William Shakespeare	Teatro	1595	978-8-43-164140-5	No	<a href="#">i</a>
Hamlet	William Shakespeare	Teatro	1601	978-8-49-764539-3	Si	<a href="#">i</a>
Macbeth	William Shakespeare	Teatro	1606	978-8-41-597353-9	Si	<a href="#">i</a>

# Almacenar contraseñas

- El algoritmo de encriptación *md5* ha sido ampliamente recomendado para estas necesidades, pero a día de hoy se considera un algoritmo poco seguro.
- A la función hash de PHP se le pasa la cadena y el algoritmo de encriptación que queremos usar.
- Las versiones del algoritmo *ripemd* convierten la contraseña en una cadena hexadecimal de 32 caracteres.

# Almacenar contraseñas

- ¿Cómo comprobar que el usuario ha metido bien la contraseña?
  - Se compara el resultado de la contraseña metida con la cadena guardada en la base de datos. Usar el método hash

```
$token = hash('ripemd128', 'mypassword');  
> 7b694600c8a2a2b0897c719958713619
```

# Inicio de sesión

- En el fichero de login iniciamos la sesión. Para comenzar una sesión, hay que utilizar la función de php `session_start` antes de incluir ningún código html.

```
<?php  
session_start();  
?>
```

- Y si la contraseña es correcta, ponemos los datos de la sesión y el tiempo de duración de la sesión. Trascurrido ese tiempo, se hace un logout automático a menos que el usuario lo haga él con el botón logout. En ambos casos, hay que llamar a

```
session_destroy();
```

# Inicio de sesión

```
/*
password_Verify() function verify if the password entered by the user
match the password hash on the database. If everything is ok the session
is created for one minute. Change 1 on $_SESSION[start] to 5 for a 5 minutes session.
*/
if (password_verify($_POST['password'], $hash)) {

    $_SESSION['loggedin'] = true;
    $_SESSION['name'] = $row['Name'];
    $_SESSION['start'] = time();
    $_SESSION['expire'] = $_SESSION['start'] + (1 * 60) ;

    echo "<div class='alert alert-success' role='alert'><strong>Welcome!</strong> $row[Name]
    <p><a href='edit-profile.php'>Edit Profile</a></p>
    <p><a href='logout.php'>Logout</a></p></div>";

} else {
    echo "<div class='alert alert-danger' role='alert'>Email or Password are incorrects!
    <p><a href='login.html'><strong>Please try again!</strong></a></p></div>";
}
```



# Inicio de sesión

```
<?php
if (isset($_SESSION['loggedin']) && $_SESSION['loggedin'] == true)
{
} else {
    echo "<div class='alert alert-danger' role='alert'>
    <h4>You need to login to access this page.</h4>
    <p><a href='login.html'>Login Here!</a></p></div>";
    exit;
}

// checking the time now when home page starts
$now = time();
if ($now > $_SESSION['expire'] )
{
    session_destroy();
    echo "<div class='alert alert-danger' role='alert'>
    <h4>Your session has expire!</h4>
    <p><a href='login.html'>Login Here</a></p></div>";
    exit;
}
?>
```

# Inicio de sesión

- Una posibilidad es tener un fichero `session.php` que se incluya al principio de cada fichero php, antes de ningún código html y que obtenga la información del usuario si se encuentra logueado.

```
session_start();

if(isset($_SESSION['username'])) {
    $logged = true;
    $username = $_SESSION['username'];
    $name = $_SESSION['name'];
    $admin = $_SESSION['admin'];
}
else {
    $logged = false;
}
```