

Práctica 4

Control de usuarios

Programación Web

3º Grado en Ingeniería Informática - Universidad de Córdoba

Jose María Moyano Murillo

jmoyano@uco.es

1. Almacenar contraseñas

Práctica 4 – Control de usuarios

Almacenar contraseñas

- Obviamente, los nombres de usuario y contraseñas de los usuarios estarán almacenadas en MySQL.
- Sin embargo, no queremos almacenar las contraseñas como texto plano, ya que pueden quedar expuestas si alguien consigue acceder a las bases de datos de nuestra aplicación web.
- En lugar de eso, usaremos una *función de único sentido*.

Almacenar contraseñas

- Estas funciones convierten una cadena de texto en una cadena aparentemente aleatoria.
- Dada su naturaleza de un solo sentido, estas funciones son virtualmente imposibles de revertir, por lo que su salida puede ser almacenada con seguridad en una base de datos, sabiendo que nadie que consiga robarla podrá obtener la contraseña.

Almacenar contraseñas

Función hash

- 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.

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

<http://www.md5calc.com/ripemd128>

Almacenar contraseñas

Salting

- Sin embargo, los *hash* pueden no ser suficiente para proteger las contraseñas en la base de datos, ya que son susceptibles de sufrir un ataque de fuerza bruta que use otra base de datos de tokens de 32 caracteres conocidos.
- Podemos hacerlo un poco más difícil modificando (*salting*) las contraseñas antes de pasárselas a la función de *hash*, almacenando en la base de datos el *hash* de la contraseña modificada.
- El *salting* se basa simplemente en añadir algo de texto que solo nosotros conocemos a la cadena que queremos *hashear*.

Almacenar contraseñas

Salting

- En el siguiente ejemplo, el texto "saltstring" se añade al principio de la cadena antes de obtener su *hash*.

```
$token = hash('ripemd128', 'saltstringmypassword');
```

- En el siguiente ejemplo, varios caracteres aleatorios se añaden tanto antes como después de la contraseña. Así, dada solo la base de datos y sin tener acceso al código php, será prácticamente imposible obtener las contraseñas.

```
$token = hash('ripemd128', 'hqb%$tmypasswordcg*1');
```

Almacenar contraseñas

Salting

- Para verificar que la contraseña introducida es la correcta, deberemos:
 - 1) Añadir los *saltings* a la cadena de la contraseña introducida por el usuario.
 - 2) Generar el *hash* con la contraseña modificada.
 - 3) Comparar con el *hash* almacenado en la base de datos.

```
$salt1 = "qm&h*";  
$salt2 = "pg!@";  
$username = "jose";  
$password = "josePWD";  
  
$token = hash('ripemd128', '$salt1$password$salt2');  
  
checkUser($conn, $username, $token);
```


2. Sesiones de usuario

Práctica 4 – Control de usuarios

Sesiones de usuario

Cookies

- Las *cookies* son un ítem de datos que el servidor web almacena en el disco duro a través del navegador.
- Puede contener cualquier información alfanumérica (hasta 4KB) y puede obtenerse del ordenador para devolverlo al servidor cuando este lo requiera.
- Usos comunes: mantener información de sesiones, mantener datos a través de diferentes vistas o páginas, mantener datos del carrito de la compra, almacenar datos de login, etc.

Sesiones de usuario

Sesiones

- Para saber las variables que se definieron en otros programas o ficheros, resulta necesario rastrear qué hacen los usuarios en su paso de una web a otra.
- Las sesiones son grupos de variables que se almacenan en el servidor, pero relativas solo al usuario actual.
- Para ello, php almacena una nueva *cookie* en el navegador del usuario para identificarlo.

Sesiones de usuario

Empezando una sesión

- Para comenzar una sesión, hay que utilizar la función de php `session_start` antes de incluir ningún código html.
- Para empezar a guardar variables en la sesión, simplemente se le asigna como parte del array asociativo `$_SESSION`.

```
$_SESSION['variable'] = $value;
```

- Posteriormente, se pueden leer los valores de este array como:

```
$variable = $_SESSION['variable'];
```

Sesiones de usuario

session.php

- Ejemplo: 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;
}
```

Sesiones de usuario

Cerrar sesión

- Para cerrar una sesión, se hace con la función `session_destroy()`.

```
function destroySession()  
{  
    //Iniciar la sesión para poder acceder al array $_SESSION  
    session_start();  
    //Inicializar $_SESSION a un array vacío  
    $_SESSION = array();  
    //Finalizar la sesión  
    session_destroy();  
}
```

Sesiones de usuario


Pantalla de inicio de sesión

- Normalmente incluye dos apartados: inicio de sesión y crear nuevo usuario.
 - Un formulario de inicio de sesión que pida el nombre de usuario y la contraseña, que valide en el servidor si el nombre de usuario existe en la base de datos y la contraseña coincide con la correspondiente.
 - Un formulario de creación de un nuevo usuario que al menos pida el nombre de usuario y contraseña (por duplicado, comprobando que coinciden). Suele pedir más información acerca del usuario que también se almacenará.
 - En el caso de diferenciar entre usuarios administradores y no administradores, en principio, solo un usuario administrador podrá crear otro usuario administrador; si no, por defecto se crea un usuario no administrador.

Sesiones de usuario

Pantalla de inicio de sesión

```
if (isset($_POST['login'])) {  
    if (...) { //Check if cancel button has been selected  
    }  
    else {  
        //Get the username and password of the login form  
        $username = $_POST['username'];  
        $password = $_POST['password'];  
  
        //Check if user and password match with the ones  
        in the database  
        $checkLogin = login($username, $password);  
  
        if ($checkLogin) {  
            header('Location: /index.php');  
        }  
        else {  
            header('Location: /authenticate.php?auth=false');  
        }  
    }  
}
```

- 
- 1) Comprobar que las longitudes sean > 0
 - 2) checkUserAndPassword()
 - 3) session_start()
 - 4) Obtener más info del usuario si es necesario
 - 5) \$_SESSION['username'] = \$username
 - 6) \$_SESSION[] ...

3. Objetivos Práctica 4

Práctica 4 – Control de usuarios

Objetivos Práctica 4

- Ampliar la práctica anterior haciendo uso de sesiones de usuario.
- Se necesitará una nueva tabla en la base de datos con la información de los usuarios.
 - Nombre de usuario
 - Contraseña (encriptada)
 - Admin (bool)
- Incluir una nueva página para realizar el inicio de sesión y crear usuarios.

Objetivos Práctica 4

Escenarios

- Un usuario sin registrar o un usuario normal únicamente podrán acceder al listado y a más información de cada uno de los registros.
- Los usuarios administradores, además, podrán añadir, modificar y eliminar registros de la base de datos.
- Si el usuario no está registrado habrá un botón/enlace a la página de inicio de sesión; y si está registrado, uno para cerrar la sesión.

Objetivos Práctica 4

Escenarios

- Controlar que a las páginas restringidas para cierto tipo de usuarios no pueda acceder un usuario no permitido a través de su enlace.
- Controlar que no se añadan dos usuarios iguales.
- Debe haber una página de inicio de sesión y otra para añadir usuarios, o una con ambas funcionalidades.
- Los campos de contraseña no deben mostrar los caracteres que se introducen.
- Tener al menos un usuario normal y otro administrador para poder probar los distintos escenarios.

Objetivos Práctica 4

Biblioteca – books.php



Biblioteca

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

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
Los juegos del hambre	Suzanne Collins	Novela juvenil	2008	978-8-49-296680-6	No
En llamas	Suzanne Collins	Novela juvenil	2009	978-8-49-296682-0	No
Sinsajo	Suzanne Collins	Novela juvenil	2010	978-8-49-296681-3	No
Romeo y Julieta	William Shakespeare	Teatro	1595	978-8-43-164140-5	No
Hamlet	William Shakespeare	Teatro	1601	978-8-49-764539-3	Si
Macbeth	William Shakespeare	Teatro	1606	978-8-41-597353-9	Si

Esta página ha sido creada por Jose M. Moyano. Contacto: jmoyano@uco.es

Objetivos Práctica 4

Biblioteca – login.php



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

Objetivos Práctica 4

Biblioteca – books.php



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	i
Los juegos del hambre	Suzanne Collins	Novela juvenil	2008	978-8-49-296680-6	No	i
En llamas	Suzanne Collins	Novela juvenil	2009	978-8-49-296682-0	No	i
Sinsajo	Suzanne Collins	Novela juvenil	2010	978-8-49-296681-3	No	i
Romeo y Julieta	William Shakespeare	Teatro	1595	978-8-43-164140-5	No	i
Hamlet	William Shakespeare	Teatro	1601	978-8-49-764539-3	Si	i
Macbeth	William Shakespeare	Teatro	1606	978-8-41-597353-9	Si	i

Esta página ha sido creada por Jose M. Moyano. Contacto: jmoyano@uco.es

Objetivos Práctica 4

Biblioteca – books.php



Biblioteca

[Listado de libros](#) [Listado de autores](#) [Listado de categorías](#) [Contacto](#) [Añadir usuario](#) [Logout](#)

Listado completo de libros de la biblioteca

[+ Añadir nuevo libro](#)

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

Esta página ha sido creada por Jose M. Moyano. Contacto: jmoyano@uco.es

Práctica 4

Control de usuarios

Programación Web

3º Grado en Ingeniería Informática - Universidad de Córdoba

Jose María Moyano Murillo

jmoyano@uco.es