

U.T. 4: Desarrollo de Aplicaciones Web con PHP

Contenidos:

- Autenticación de usuarios y control de acceso
 - Mecanismos de autenticación
 - Incorporación de métodos de autenticación a una aplicación web
- Cookies
- Manejo de sesión
 - Configuración
 - Inicio y fin de una sesión
 - Gestión de la información de la sesión

1.- Autenticación de usuarios y control de acceso

Muchas veces es importante verificar la identidad de los dos extremos de una comunicación. En el caso de una comunicación web, existen métodos para identificar tanto al servidor en el que se aloja el sitio web, como al usuario del navegador que se encuentra en el otro extremo.

Los sitios web que necesitan emplear identificación del servidor, como las tiendas o los bancos, utilizan el protocolo HTTPS. Este protocolo requiere de un certificado válido, firmado por una autoridad confiable, que es verificado por el navegador cuando se accede al sitio web. Además, HTTPS utiliza métodos de cifrado para crear un canal seguro entre el navegador y el servidor, de tal forma que no se pueda interceptar la información que se transmite por el mismo.

Para identificar a los usuarios que visitan un sitio web, se pueden utilizar distintos métodos como el DNI digital o certificados digitales de usuario, pero el más extendido es solicitar al usuario cierta información que solo él conoce: la combinación de un nombre de usuario y una contraseña.

1.- Autenticación de usuarios y control de acceso

En la unidad anterior aprendiste a utilizar aplicaciones web para gestionar información almacenada en bases de datos. En la mayoría de los casos es importante implantar en este tipo de aplicaciones web, las que acceden a bases de datos, algún mecanismo de control de acceso que obligue al usuario a identificarse. Una vez identificado, se puede limitar el uso que puede hacer de la información.

Así, puede haber sitios web en los que los usuarios autenticados pueden utilizar sólo una parte de la información (como los bancos, que permiten a sus clientes acceder únicamente a la información relativa a sus cuentas). Otros sitios web necesitan separar en grupos a los usuarios autenticados, de tal forma que la información a la que accede un usuario depende del grupo en que éste se encuentre. Por ejemplo, una aplicación de gestión de una empresa puede tener un grupo de usuarios a los que permite visualizar la información, y otro grupo de usuarios que, además de visualizar la información, también la pueden modificar.

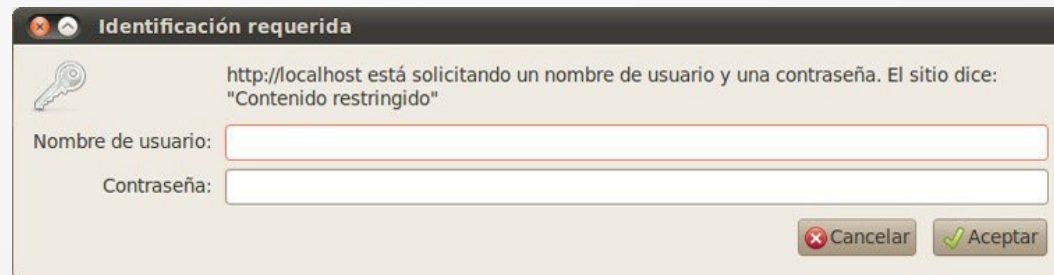
Debes distinguir la autenticación de los usuarios y el control de acceso, de la utilización de mecanismos para asegurar las comunicaciones entre el usuario del navegador y el servidor web. Aunque ambos aspectos suelen ir unidos, son independientes.

En los ejemplos de esta unidad, la información de autenticación (nombre y contraseña de los usuarios) se envía en texto plano desde el navegador hasta el servidor web. **Esta práctica es altamente insegura y nunca debe usarse sin un protocolo como HTTPS** que permita cifrar las comunicaciones con el servidor web. Sin embargo, la configuración de servidores web que permitan usar el protocolo HTTPS para cifrar la información que reciben y transmiten no forma parte de los contenidos de este módulo. Por este motivo, durante esta unidad utilizaremos únicamente el protocolo no seguro HTTP.

1.1.- Mecanismos de autenticación

El protocolo HTTP ofrece un método sencillo para autenticar a los usuarios. El proceso es el siguiente:

- ✓ El servidor web debe proveer algún método para definir los usuarios que se utilizarán y cómo se pueden autenticar. Además, se tendrán que definir los recursos a los que se restringe el acceso y qué lista de control de acceso (ACL) se aplica a cada uno.
- ✓ Cuando un usuario no autenticado intenta acceder a un recurso restringido, el servidor web responde con un error de "Acceso no autorizado" (código 401).
- ✓ El navegador recibe el error y abre una ventana para solicitar al usuario que se autentique mediante su nombre y contraseña.



- ✓ La información de autenticación del usuario se envía al servidor, que la verifica y decide si permite o no el acceso al recurso solicitado. Esta información se mantiene en el navegador para utilizarse en posteriores peticiones a ese servidor.

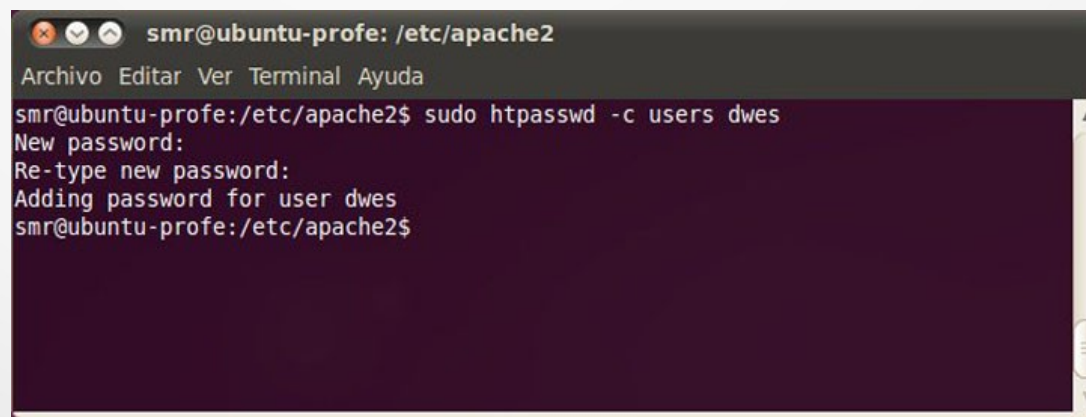
1.1.- Mecanismos de autenticación

En el servidor web Apache, el que has estado usando en anteriores unidades, existe una utilidad en línea de comandos, `htpasswd`, que permite almacenar en un fichero una lista de usuarios y sus respectivas contraseñas. La información relativa a las contraseñas se almacena cifrada; aun así, es conveniente crear este fichero en un lugar no accesible por los usuarios del servidor web.

Por ejemplo, para crear el fichero de usuario y añadirle el usuario "dwes", puedes hacer:

```
sudo htpasswd -c users dwes
```

e introducir la contraseña correspondiente a ese usuario.

A screenshot of a terminal window titled 'smr@ubuntu-profe: /etc/apache2'. The terminal shows the command 'sudo htpasswd -c users dwes' being executed. The output shows 'New password:', 'Re-type new password:', and 'Adding password for user dwes'. The prompt returns to 'smr@ubuntu-profe:/etc/apache2\$'.

```
smr@ubuntu-profe: /etc/apache2
Archivo Editar Ver Terminal Ayuda
smr@ubuntu-profe:/etc/apache2$ sudo htpasswd -c users dwes
New password:
Re-type new password:
Adding password for user dwes
smr@ubuntu-profe:/etc/apache2$
```

En el curso de Moodle encontrarás un enlace a `htpasswd` (PSM1)

1.1.- Mecanismos de autenticación

La opción `-c` indica que se debe crear el fichero, por lo que solo deberás usarla cuando introduzcas el primer usuario y contraseña. Fíjate que en el ejemplo anterior, el fichero se crea en la ruta `/etc/apache2/users` (la ruta desde la que se lanzó la instrucción), que en principio no es accesible vía web.

Si la consola indica que no encuentra el comando `htpasswd` puede deberse a que no esté instalado el paquete de utilidades de Apache, para ello sólo hay que ejecutar:

```
sudo apt-get install apache2-utils
```

Si se está trabajando en un entorno xampp de Windows la utilidad `htpasswd` se encontrará seguramente en `C:\xampp\apache\bin`

Para indicarle al servidor Apache qué recursos tienen acceso restringido, una opción es crear un fichero `.htaccess` en el directorio en que se encuentren, con las siguientes directivas:

```
AuthName "Contenido restringido"
```

```
AuthType Basic
```

```
AuthUserFile /etc/apache2/users
```

```
require valid-user
```

1.1.- Mecanismos de autenticación

El significado de cada una de las directivas anteriores es el siguiente:

Directivas de autenticación en Apache

Directiva	Significado
authName	Nombre de dominio que se usará en la autenticación. Si el cliente se autentifica correctamente, esa misma información de autenticación se utilizará automáticamente en el resto de las páginas del mismo dominio.
authType	Método de autenticación que se usará. Además del método Basic, Apache también permite utilizar el método Digest.
authUserFile	Ruta al archivo de credenciales que has creado con htpasswd.
require	Permite indicar que sólo puedan acceder algunos usuarios o grupos de usuarios concretos. Si indicamos "valid-user", podrán acceder todos los usuarios que se autentifiquen correctamente.

Además tendrás que asegurarte de que en la configuración de Apache se utiliza la directiva AllowOverride para que se aplique correctamente la configuración que figura en los ficheros .htaccess.

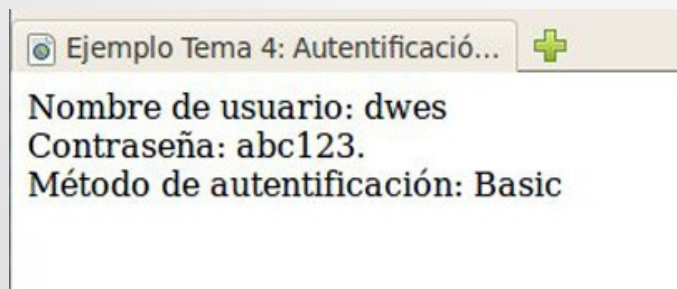
1.1.1.- Mecanismos de autenticación

Desde PHP puedes acceder a la información de autenticación HTTP que ha introducido el usuario utilizando el array superglobal `$_SERVER`.

Valores del array `$_SERVER` relacionados con la autenticación HTTP

Valor	Contenido
<code>\$_SERVER['PHP_AUTH_USER']</code>	Nombre de usuario que se ha introducido.
<code>\$_SERVER['PHP_AUTH_PW']</code>	Contraseña introducida.
<code>\$_SERVER['AUTH_TYPE']</code>	Método HTTP usado para autenticar. Puede ser Basic o Digest.

Es decir, que si creas una página web que muestre los valores de estas variables, y preparas el servidor web para utilizar autenticación HTTP, cuando accedas a esa página con el usuario "dwes" obtendrás algo como lo siguiente:



En el curso de Moodle encontrarás el código de la página web del ejemplo (ER1)

1.1.1.- Mecanismos de autenticación

Si no introduces un usuario/contraseña válidos, el navegador te mostrará el error 401.

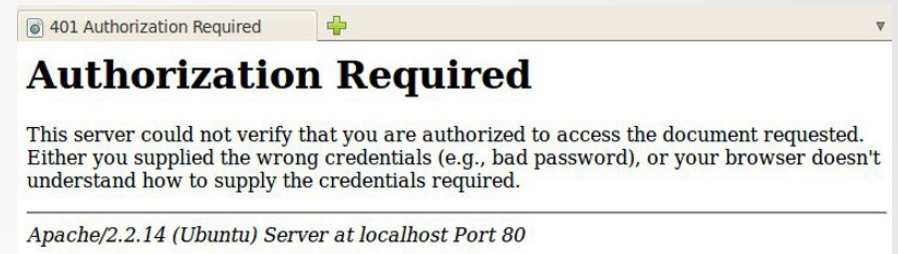
Recuerda que debes tener creado el fichero .htaccess en la ubicación donde ejecutas este ejemplo, para que solicite la autenticación.

Además, en PHP puedes usar la función header para forzar a que el servidor envíe un error de "Acceso no autorizado" (código 401). De

esta forma no es necesario utilizar ficheros .htaccess para indicarle a Apache qué recursos están restringidos. En su lugar, puedes añadir las siguientes líneas en tus páginas PHP:

```
if (!isset($_SERVER['PHP_AUTH_USER'])) {  
    header('WWW-Authenticate: Basic Realm="Contenido restringido");  
    header('HTTP/1.0 401 Unauthorized');  
    echo "Usuario no reconocido!";  
    exit;  
}  
?>
```

Con el código anterior, la página envía un error 401, lo que fuerza al navegador a solicitar las credenciales de acceso (nombre de usuario y contraseña). Si se introducen, se ejecuta el resto de la página y se muestra su contenido. En este caso, habría que añadir algún código para comprobar que el nombre de usuario y contraseña son válidos, tal y como veremos a continuación. Si se pulsa el botón "Cancelar", se muestra el mensaje de error que se indica.



En el curso encontrarás un enlace a la función header (DC1) y a un ejemplo resuelto (ER2)

1.2.- Incorporación de métodos de autenticación a una aplicación web

Si utilizas la función header para forzar al navegador a solicitar credenciales HTTP, el usuario introducirá un nombre y una contraseña. Pero el servidor no verificará esta información; deberás ser tú quien provea un método para comprobar que las credenciales que ha introducido el usuario son correctas.

El método más simple es incluir en el código PHP de tu página las sentencias necesarias para comparar los datos introducidos con otros datos fijos. Por ejemplo, para permitir el acceso a un usuario "dwes" con contraseña "abc123.", puedes hacer:

```
if ($_SERVER['PHP_AUTH_USER'] != 'dwes' || $_SERVER['PHP_AUTH_PW'] != 'abc123.') {  
    header('WWW-Authenticate: Basic Realm="Contenido restringido"');  
    header('HTTP/1.0 401 Unauthorized');  
    echo "Usuario no reconocido!";  
    exit;  
}  
?>
```

Recuerda que el código PHP no se envía al navegador, por lo que la información de autenticación que introduzcas en el código no será visible por el usuario. Sin embargo, esto hará tu código menos portable. Si necesitas modificar el nombre de usuario o la contraseña, tendrás que hacer modificaciones en el código. Además, no podrás permitir al usuario introducir su propia contraseña.

1.2.- Incorporación de métodos de autenticación a una aplicación web

Una solución mejor es utilizar un almacenamiento externo para los nombres de usuario y sus contraseñas. Para esto podrías emplear un fichero de texto, o mejor aún, una base de datos. La información de autenticación podrá estar aislada en su propia base de datos, o compartir espacio de almacenamiento con los datos que utilice tu aplicación web.

Si quieres almacenar la información de los usuarios en la base de datos "dwes", tienes que crear una nueva tabla en su estructura. Para ello, revisa y ejecuta estas sentencias SQL:

```
USE dwes;
```

```
-- Creamos la tabla
```

```
CREATE TABLE usuarios (  
usuario VARCHAR(20) NOT NULL PRIMARY KEY,  
contrasena VARCHAR(32) NOT NULL  
) ENGINE = INNODB;
```

```
-- Creamos el usuario dwes
```

```
INSERT INTO usuarios (usuario, contrasena) VALUES  
( 'dwes', 'e8dc8ccd5e5f9e3a54f07350ce8a2d3d');
```

Aunque se podrían almacenar las contraseñas en texto plano, es mejor hacerlo en formato encriptado. En el ejemplo anterior, para el usuario "dwes" se almacena el hash MD5 correspondiente a la contraseña "abc123.". En PHP puedes usar la función md5 para calcular el hash MD5 de una cadena de texto (en el curso de Moodle encontrarás un enlace a esta función, PSM2)

En el curso de Moodle encontrarás un ejercicio resuelto donde se utiliza la extensión MySQLi (ER3)

2.- Cookies

Una cookie es un fichero de texto que un sitio web guarda en el entorno del usuario del navegador. Su uso más típico es el almacenamiento de las preferencias del usuario (por ejemplo, el idioma en que se deben mostrar las páginas), para que no tenga que volver a indicarlo la próxima vez que visite el sitio.

Si utilizas Firefox como navegador, puedes consultar las cookies almacenadas en el mismo con el Inspector (Menú Desarrollador Web)

En PHP, para almacenar una cookie en el navegador del usuario, puedes utilizar la función *setcookie*. El único parámetro obligatorio que tienes que usar es el nombre de la cookie, pero admite varios parámetros más opcionales.

En el curso encontrarás un enlace a la función *setcookie* (DC2)

2.- Cookies

Por ejemplo, si quieres almacenar en una cookie el nombre de usuario que se transmitió en las credenciales HTTP (es solo un ejemplo, no es en absoluto aconsejable almacenar información relativa a la seguridad en las cookies), puedes hacer:

```
setcookie("nombre_usuario", $_SERVER['PHP_AUTH_USER'], time()+3600);
```

Los dos primeros parámetros son el nombre de la cookie y su valor. El tercero es la fecha de caducidad de la misma (una hora desde el momento en que se ejecute). En caso de no figurar este parámetro, la cookie se eliminará cuando se cierre el navegador. Ten en cuenta que también se pueden aplicar restricciones a las páginas del sitio que pueden acceder a una cookie en función de la ruta. Si una vez almacenada una cookie en el navegador quieres eliminarla antes de que expire, puedes utilizar la misma función setcookie pero indicando una fecha de caducidad anterior a la actual.

Las cookies se transmiten entre el navegador y el servidor web de la misma forma que las credenciales que acabas de ver; utilizando los encabezados del protocolo HTTP. Por ello, las sentencias setcookie deben enviarse antes de que el navegador muestre información alguna en pantalla.

El proceso de recuperación de la información que almacena una cookie es muy simple. Cuando accedes a un sitio web, el navegador le envía de forma automática todo el contenido de las cookies que almacene relativas a ese sitio en concreto. Desde PHP puedes acceder a esta información por medio del array \$_COOKIE.

Siempre que utilices cookies en una aplicación web, debes tener en cuenta que en última instancia su disponibilidad está controlada por el cliente. Por ejemplo, algunos usuarios deshabilitan las cookies en el navegador porque piensan que la información que almacenan puede suponer un potencial problema de seguridad. O la información que almacenan puede llegar a perderse porque el usuario decide formatear el equipo o simplemente eliminarlas de su sistema.

En el curso de Moodle encontrarás un ejercicio resuelto sobre cookies (ER4)

3.- Manejo de sesiones

Como acabas de ver, una forma para guardar información particular de cada usuario es utilizar cookies. Sin embargo, existen diversos problemas asociados a las cookies, como el número de ellas que admite el navegador, o su tamaño máximo. Para solventar estos inconvenientes, existen las sesiones. El término sesión hace referencia al conjunto de información relativa a un usuario concreto. Esta información puede ser tan simple como el nombre del propio usuario, o más compleja, como los artículos que ha depositado en la cesta de compra de una tienda online.

Cada usuario distinto de un sitio web tiene su propia información de sesión. Para distinguir una sesión de otra se usan los identificadores de sesión (SID). Un SID es un atributo que se asigna a cada uno de los visitantes de un sitio web y lo identifica. De esta forma, si el servidor web conoce el SID de un usuario, puede relacionarlo con toda la información que posee sobre él, que se mantiene en la sesión del usuario. Esa información se almacena en el servidor web, generalmente en ficheros aunque también se pueden utilizar otros mecanismos de almacenamiento como bases de datos.

Como ya habrás supuesto, la cuestión ahora es: ¿y dónde se almacena ese SID, el identificador de la sesión, que es único para cada usuario? Pues existen dos maneras de mantener el SID entre las páginas de un sitio web que visita el usuario:

- ✓ Utilizando cookies, tal y como ya viste.
- ✓ Propagando el SID en un parámetro de la URL. El SID se añade como una parte más de la URL, de la forma:

<http://www.misitioweb.com/tienda/listado.php&PHPSESSID=34534fg4ffg34ty>

3.- Manejo de sesiones

Ninguna de las dos maneras es perfecta. Ya sabes los problemas que tiene la utilización de cookies. Pese a ello, es el mejor método y el más utilizado. Propagar el SID como parte de la URL conlleva mayores desventajas, como la imposibilidad de mantener el SID entre distintas sesiones, o el hecho de que compartir la URL con otra persona implica compartir también el identificador de sesión.

La buena noticia, es que el proceso de manejo de sesiones en PHP está automatizado en gran medida. Cuando un usuario visita un sitio web, no es necesario programar un procedimiento para ver si existe un SID previo y cargar los datos asociados con el mismo. Tampoco tienes que utilizar la función setcookie si quieres almacenar los SID en cookies, o ir pasando el SID entre las páginas web de tu sitio si te decides por propagarlo. Todo esto PHP lo hace automáticamente.

A la información que se almacena en la sesión de un usuario también se le conoce como cookies del lado del servidor (server side cookies). Debes tener en cuenta que aunque esta información no viaja entre el cliente y el servidor, sí lo hace el SID, bien como parte de la URL o en un encabezado HTTP si se guarda en una cookie. En ambos casos, esto plantea un posible problema de seguridad. El SID puede ser conseguido por otra persona, y a partir del mismo obtener la información de la sesión del usuario. La manera más segura de utilizar sesiones es almacenando los SID en cookies y utilizar HTTPS para encriptar la información que se transmite entre el servidor web y el cliente.

3.1.- Configuración

Por defecto, PHP incluye soporte de sesiones incorporado. Sin embargo, antes de utilizar sesiones en tu sitio web, debes configurar correctamente PHP utilizando las siguientes directivas en el fichero php.ini según corresponda:

Directivas de configuración de PHP relacionadas con el manejo de sesiones

Directiva	Significado
session.use_cookies	Indica si se deben usar cookies (1) o propagación en la URL (0) para almacenar el SID
session.use_only_cookies	Se debe activar (1) cuando utilizas cookies para almacenar los SID, y además no quieres que se reconozcan los SID que se puedan pasar como parte de la URL (este método se puede usar para usurpar el identificador de otro usuario).
session.save_handler	Se utiliza para indicar a PHP cómo debe almacenar los datos de la sesión del usuario. Existen cuatro opciones: en ficheros (files), en memoria (mm), en una base de datos SQLite (sqlite) o utilizando para ello funciones que debe definir el programador (user). El valor por defecto (files) funcionará sin problemas en la mayoría de los casos.
session.name	Determina el nombre de la cookie que se utilizará para guardar el SID. Su valor por defecto es PHPSESSID.
session.auto_start	Su valor por defecto es 0, y en este caso deberás usar la función session_start para gestionar el inicio de las sesiones. Si usas sesiones en el sitio web, puede ser buena idea cambiar su valor a 1 para que PHP active de forma automática el manejo de sesiones.
session.cookie_lifetime	Si utilizas la URL para propagar el SID, éste se perderá cuando cierres tu navegador. Sin embargo, si utilizas cookies, el SID se mantendrá mientras no se destruya la cookie. En su valor por defecto (0), las cookies se destruyen cuando se cierra el navegador. Si quieres que se mantenga el SID durante más tiempo, debes indicar en esta directiva ese tiempo en segundos.
session.gc_maxlifetime	Indica el tiempo en segundos que se debe mantener activa la sesión, aunque no haya ninguna actividad por parte del usuario. Su valor por defecto es 1440. Es decir, pasados 24 minutos desde la última actividad por parte del usuario, se cierra su sesión automáticamente.

3.1.- Configuración

La función `phpinfo`, de la que ya hablamos con anterioridad, te ofrece información sobre la configuración actual de las directivas de sesión.

En el curso de Moodle tienes un enlace con información sobre las directivas que permiten configurar el manejo de sesiones (PSM3)

session

Session Support	enabled
Registered save handlers	files user sqlite
Registered serializer handlers	php php_binary wddx

Directive	Local Value	Master Value
session.auto_start	Off	Off
session.bug_compat_42	On	On
session.bug_compat_warn	On	On
session.cache_expire	180	180
session.cache_limiter	nocache	nocache
session.cookie_domain	<i>no value</i>	<i>no value</i>
session.cookie_httponly	Off	Off
session.cookie_lifetime	0	0
session.cookie_path	/	/
session.cookie_secure	Off	Off
session.entropy_file	<i>no value</i>	<i>no value</i>
session.entropy_length	0	0
session.gc_divisor	100	100
session.gc_maxlifetime	1440	1440
session.gc_probability	1	1
session.hash_bits_per_character	5	5
session.hash_function	0	0
session.name	PHPSESSID	PHPSESSID
session.referer_check	<i>no value</i>	<i>no value</i>
session.save_handler	files	files
session.save_path	\xampplite\tmp	\xampplite\tmp
session.serialize_handler	php	php
session.use_cookies	On	On
session.use_only_cookies	Off	Off
session.use_trans_sid	0	0

3.2.- Inicio y fin de una sesión

El inicio de una sesión puede tener lugar de dos formas. Si has activado la directiva `session.auto_start` en la configuración de PHP, la sesión comenzará automáticamente en cuanto un usuario se conecte a tu sitio web. En caso de que ese usuario ya haya abierto una sesión con anterioridad, y esta no se haya eliminado, en lugar de abrir una nueva sesión se reanudará la anterior. Para ello se utilizará el SID anterior, que estará almacenado en una cookie (recuerda que si usas propagación del SID, no podrás restaurar sesiones anteriores; el SID figura en la URL y se pierde cuando cierras el navegador).

Si por el contrario, decides no utilizar el inicio automático de sesiones, deberás ejecutar la función `session_start` para indicar a PHP que inicie una nueva sesión o reanude la anterior. Aunque anteriormente esta función devolvía siempre `true`, a partir de la versión 5.3.0 de PHP su comportamiento es más coherente: devuelve `false` en caso de no poder iniciar o restaurar la sesión.

Como el inicio de sesión requiere utilizar cookies, y éstas se transmiten en los encabezados HTTP, debes tener en cuenta que para poder iniciar una sesión utilizando `session_start`, tendrás que hacer las llamadas a esta función antes de que la página web muestre información en el navegador.

Además, todas las páginas que necesiten utilizar la información almacenada en la sesión, deberán ejecutar la función `session_start`.

3.2.- Inicio y fin de una sesión

Mientras la sesión permanece abierta, puedes utilizar la variable superglobal `$_SESSION` para añadir información a la sesión del usuario, o para acceder a la información almacenada en la sesión. Por ejemplo, para contar el número de veces que el usuario visita la página, puedes hacer:

```
// Iniciamos la sesión o recuperamos la anterior sesión existente
session_start();
// Comprobamos si la variable ya existe
if (isset($_SESSION['visitas']))
    $_SESSION['visitas']++;
else
    $_SESSION['visitas'] = 0;
?>
```

Si en lugar del número de visitas, quisieras almacenar el instante en que se produce cada una, la variable de sesión "visitas" deberá ser un array y por tanto tendrás que cambiar el código anterior por:

```
// Iniciamos la sesión o recuperamos la anterior sesión existente
session_start();
// En cada visita añadimos un valor al array "visitas"
$_SESSION['visitas'][] = mktime();
?>
```

3.2.- Inicio y fin de una sesión

Aunque como ya viste, puedes configurar PHP para que elimine de forma automática los datos de una sesión pasado cierto tiempo, en ocasiones puede ser necesario cerrarla de forma manual en un momento determinado. Por ejemplo, si utilizas sesiones para recordar la información de autenticación, deberás darle al usuario del sitio web la posibilidad de cerrar la sesión cuando lo crea conveniente.

En PHP tienes dos funciones para eliminar la información almacenada en la sesión:

- ✓ **session_unset.** Elimina las variables almacenadas en la sesión actual, pero no elimina la información de la sesión del dispositivo de almacenamiento usado.
- ✓ **session_destroy.** Elimina completamente la información de la sesión del dispositivo de almacenamiento.

En el curso de Moodle tiene un ejercicio resuelto sobre almacenar visitas de usuarios utilizando sesiones (ER5)

3.3.- Gestión de la información de la sesión

En este punto vas a ver paso a paso un ejemplo de utilización de sesiones para almacenar la información del usuario. Utilizarás la base de datos "dwes", creada anteriormente, para crear un prototipo de una tienda web dedicada a la venta de productos de informática.

Las páginas de que constará tu tienda online son las siguientes:

- ✓ Login (login.php). Su función es autenticar al usuario de la aplicación web. Todos los usuarios de la aplicación deberán autenticarse utilizando esta página antes de poder acceder al resto de páginas.
- ✓ Listado de productos (productos.php). Presenta un listado de los productos de la tienda, y permite al usuario seleccionar aquellos que va a comprar.
- ✓ Cesta de compra (cesta.php). Muestra un resumen de los productos escogidos por el usuario para su compra y da acceso a la página de pago.
- ✓ Pagar (pagar.php). Una vez confirmada la compra, la última página debería ser la que permitiera al usuario escoger el método de pago y la forma de envío. En este ejemplo no la vas a implementar como tal. Simplemente mostrará un mensaje de tipo "Gracias por su compra" y ofrecerá un enlace para comenzar una nueva compra.
- ✓ Logoff (logoff.php). Esta página desconecta al usuario de la aplicación y redirige al usuario de forma automática a la pantalla de autenticación. No muestra ninguna información en pantalla, por lo que no es visible para el usuario.

Recuerda poner a las páginas los nombres que aquí figuran, almacenando todas en la misma carpeta. Si cambias algún nombre o mueves alguna página de lugar, los enlaces internos no funcionarán.

3.3.- Gestión de la información de la sesión

Aunque el aspecto de la aplicación no es importante para nuestro objetivo, utilizaremos una hoja de estilos, tienda.css, común a todas las páginas para ofrecer un interface más amigable. (puede descargarla del curso de Moodle)

Antes de comenzar ten en cuenta que la aplicación que vas a desarrollar no es completamente funcional. Además de no desarrollar la página con la información de pago, habrá algunas opciones que no tendrás en cuenta para simplificar el código. Por ejemplo:

- ✓ No tendrás en cuenta la posibilidad de que el usuario compre varias unidades de un mismo producto.
- ✓ Una vez añadido un producto a la cesta de compra, no se podrá retirar de la misma. La única posibilidad será vaciar toda la cesta y comenzar de nuevo añadiendo productos.
- ✓ No se mostrarán imágenes de los productos, ni será posible ver el total de la compra hasta que ésta haya finalizado.
- ✓ Se muestran todos los productos en una única página. Sería preferible filtrarlos por familia y mostrarlos en varias páginas, limitando a 10 o 20 productos el número máximo de cada página.

Recomendación: Aunque reduzcamos en este ejemplo la funcionalidad de la tienda, te animamos a que una vez finalizado el mismo, añadas por tu cuenta todas aquellas opciones que quieras. Recuerda que la mejor forma de aprender programación es... ¡programando!

3.3.1.- Gestión de la información de la sesión

La primera página que vas a programar es la de autenticación del usuario (login.php). Para variar, utilizarás las capacidades de manejo de sesiones de PHP para almacenar la identificación de los usuarios. Además, utilizaremos la información de la tabla "usuarios" en la base de datos "dwes", accediendo mediante PDO en lugar de MySQLi.

Vas a crear en la página un formulario con dos campos, uno de tipo text para el usuario, y otro de tipo password para la contraseña. Al pulsar el botón Enviar, el formulario se enviará a esta misma página, donde se compararán las credenciales proporcionadas por el usuario con las almacenadas en la base de datos. Si los datos son correctos, se iniciará una nueva sesión y se almacenará en ella el nombre del usuario que se acaba de conectar.

3.3.1.- Gestión de la información de la sesión

Vamos por pasos. El código HTML para crear el formulario, que irá dentro del cuerpo de la página (entre las etiquetas < body>) será el siguiente:

```
<div id='login'>
<form action='<?php echo $_SERVER['PHP_SELF'];?>' method='post'>
<fieldset >
  <legend>Login</legend>
  <div><span class='error'><?php if (isset($error)) echo $error; ?></span></div>
  <div class='campo'>
    <label for='usuario' >Usuario:</label><br/>
    <input type='text' name='usuario' id='usuario' maxlength="50" /><br/>
  </div>
  <div class='campo'>
    <label for='password' >Contraseña:</label><br/>
    <input type='password' name='password' id='password' maxlength="50" /><br/>
  </div>

  <div class='campo'>
    <input type='submit' name='enviar' value='Enviar' />
  </div>
</fieldset>
</form>
</div>
```

Fíjate que existe un espacio para poner los posibles mensajes de error que se produzcan, como la falta de algún dato necesario, o un error de credenciales erróneas.

3.3.1.- Gestión de la información de la sesión

El código PHP que debe figurar al comienzo de esta misma página (antes de que se muestre cualquier texto), se encargará de:

Comprobar que se han introducido tanto el nombre de usuario como la contraseña.

```
if (isset($_POST['enviar'])) {  
    $usuario = $_POST['usuario'];  
    $password = $_POST['password'];  
  
    if (empty($usuario) || empty($password))  
        $error = "Debes introducir un nombre de usuario y una contraseña";  
    Else {
```

Conectarse a la base de datos.

```
try {  
    $opc = array(PDO::MYSQL_ATTR_INIT_COMMAND => "SET NAMES utf8");  
    $dsn = "mysql:host=localhost;dbname=dwes";  
    $dwes = new PDO($dsn, "dwes", "abc123.", $opc);  
}  
catch (PDOException $e) {  
    die("Error: " . $e->getMessage());  
}
```

3.3.1.- Gestión de la información de la sesión

Comprobar las credenciales.

```
$sql = "SELECT usuario FROM usuarios WHERE usuario='$usuario' " .  
      "AND contrasena=" . md5($password) . "";
```

```
if($resultado = $dwes->query($sql)) {  
    $fila = $resultado->fetch();  
    if ($fila != null) {
```

Iniciar la sesión y almacenar en la variable de sesión \$_SESSION['usuario'] el nombre de usuario.

```
session_start();  
$_SESSION['usuario']=$usuario;
```

Redirigir a la página del listado de productos.

```
header("Location: productos.php");
```

Revisa el código completo de la página login.php y comprueba su funcionamiento antes de seguir con las demás, está disponible en el curso de Moodle.

3.3.2.- Gestión de la información de la sesión

Cuando un usuario proporciona unas credenciales de inicio de sesión correctas (recuerda que tú ya habías añadido el usuario "dwes" con contraseña "abc123."), se le redirige de forma automática a la página del listado de productos (productos.php) para que pueda empezar a hacer la compra.

La página se divide en varias zonas, cada una definida por una etiqueta < div> en el código HTML:

- ✓ encabezado. Contiene únicamente el título de la página.
- ✓ productos. Contiene el listado de todos los productos tal y como figuran en la base de datos. Cada producto figura en una línea (nombre y precio).

Se crea un formulario por cada producto, con un botón "Añadir" que envía a esta misma página los datos código, nombre y precio del producto. Cuando se abre la página, se comprueba si se ha enviado este formulario, y si fuera así se añade un elemento al array asociativo \$_SESSION['cesta'] con los datos del nuevo producto.

```
// Comprobamos si se ha enviado el formulario de añadir
if (isset($_POST['enviar'])) {
    // Creamos un array con los datos del nuevo producto
    $producto['nombre'] = $_POST['nombre'];
    $producto['precio'] = $_POST['precio'];
    // y lo añadimos
    $_SESSION['cesta'][$_POST['producto']] = $producto;
}
```

El array \$_SESSION['cesta'] es la variable de sesión en la que guardaremos los datos de todos los productos que va a comprar el usuario. Fíjate que los datos del nuevo producto se incluyen a su vez como un array con dos elementos, el precio y el nombre.

3.3.2.- Gestión de la información de la sesión

- ✓ cesta. Muestra el código de los productos que se van añadiendo a la cesta.

```
// Si la cesta está vacía, mostramos un mensaje
$cesta_vacia = true;
if (count($_SESSION['cesta'])==0) {
    print "Cesta vacía";
}
// Si no está vacía, mostrar su contenido
else {
    foreach ($_SESSION['cesta'] as $codigo => $producto)
        print "$codigo";
    $cesta_vacia = false;
}
```

Contiene dos formularios. Uno para vaciar la cesta (botón "Vaciar Cesta"), dirigido a esta misma página, y otro para realizar la compra (botón "Comprar"), que dirige a la página cesta.php. Para vaciar la cesta, se incluye en la página el siguiente código:

```
// Comprobamos si se ha enviado el formulario de vaciar la cesta
if (isset($_POST['vaciar'])) {
    unset($_SESSION['cesta']);
}
```

3.3.2.- Gestión de la información de la sesión

- ✓ pie. Contiene un botón para desconectar al usuario actual. Llama a la página `logout.php`, que borra la sesión actual.

Además, tanto en esta página como en todas las demás, es necesario comprobar la variable de sesión `$_SESSION['usuario']` para verificar que el usuario se ha autenticado correctamente. Para ello, debes incluir el siguiente código al inicio de la página.

```
// Recuperamos la información de la sesión
session_start();

// Y comprobamos que el usuario se haya autenticado
if (!isset($_SESSION['usuario'])) {
    die("Error - debe identificarse.");
}
?>
```

Si el usuario no se ha autenticado, se muestra un mensaje de error junto con un enlace a la página `login.php`.

3.3.3.- Gestión de la información de la sesión

Si desde la página del listado de productos, el usuario pulsa sobre el botón "Comprar", se le dirige a la página de la Cesta de la compra (cesta.php), en la que se le muestra un resumen de los productos que ha seleccionado junto al importe total de los mismos.

En la página figuran dos formularios que simplemente redirigen a otras páginas. El que contiene el botón "Pagar", que redirige a la página pagar.php, que en nuestro caso lo único que debe hacer es eliminar la sesión del usuario. Y el que contiene el botón de desconexión, que es similar al que figuraba en la página productos.php, y dirige a la página logoff.php, que cierra la sesión del usuario.

Cesta de la compra		
SMSN150101LD	Samsung N150 10.1LED N450 1GB 250GB BAT6 BT W7 R	260.60
KSTMSDHC8GB	Kingston MicroSDHC 8GB	10.20
IXUS115HSAZ	Canon Ixus 115HS azul	196.70
Precio total: 467.5 €		
<input type="button" value="Pagar"/>		
<input type="button" value="Desconectar usuario dwes"/>		

3.3.3.- Gestión de la información de la sesión

Los datos que figuran en la página se obtienen todos de la información almacenada en la sesión del usuario. No es necesario establecer conexiones con la base de datos. El código que sirve para mostrar el listado de los productos seleccionados es el siguiente:

```
$total = 0;
foreach($_SESSION['cesta'] as $codigo => $producto) {
    echo "$codigo";
    echo "${producto['nombre']}";
    echo "${producto['precio']}";
    $total += $producto['precio'];
}
?>
```

Precio total: €

Recuerda que al principio de esta página, también será necesario verificar la variable de sesión `$_SESSION['usuario']` para comprobar que el usuario se ha autenticado correctamente.

3.3.3.- Gestión de la información de la sesión

Tanto desde esta página como desde la página del listado de productos, se le ofrece al usuario la posibilidad de cerrar la sesión. Para ello se le dirige a la página `logoff.php`, que no muestra nada en pantalla. Su código es el siguiente:

```
// Recuperamos la información de la sesión
session_start();

// Y la eliminamos
session_unset();
session_destroy();
header("Location: login.php");
?>
```

Tras eliminar la sesión, redirige al usuario a la página de autenticación donde puede iniciar una nueva sesión con el mismo o con otro usuario distinto.