Programación Avanzada
Ingeniería Informática en Sistemas de Información - Curso 2017/2018
ENSEÑANZAS PRÁCTICAS Y DE DESARROLLO
Evaluación 2 - PHP

Nombre:_____ **Equipo:**_____

Importante: El resultado de esta prueba consistirá en un proyecto de NetBeans que será comprimido en formato ZIP conteniendo la aplicación. Emplee las credenciales por defecto de XAMPP para la conexión con la base de datos. El nombre del fichero tendrá un formato específico dictado por el nombre de cada alumno. Por ejemplo, para un alumno llamado "José María Núñez Pérez" el fichero se nombrará como NunyezPerezJM.zip. Obsérvese que las tildes son ignoradas y las eñes sustituidas. No se aceptará ningún envío que no cumpla con las anteriores especificaciones de formato y nombrado. **Las rutas de los ficheros empleados serán relativas, a fin de que las resoluciones a los ejercicios y problemas puedan ser examinadas en cualquier equipo. Cualquier entrega que no cumpla las reglas de nombrado, el formato de compresión del archivo o el contenido de los archivos del mismo, será penalizada con 2 puntos sobre 10 por cada incumplimiento. Pasado el límite de entrega se aceptará el envío del trabajo, con una penalización de 2 puntos sobre 10 de la calificación por cada minuto o fracción de retraso a partir de tercer minuto. No es necesario que incluya el script de la base de datos en el envío. Las imágenes sin embargo, sí deberá incluirlas.**

Objetivos

- Demostrar los conocimientos adquiridos en el desarrollo de aplicaciones empleando PHP.

Descripción del ejercicio propuesto

Crear una aplicación web, empleando PHP como lenguaje de programación y MySQL como base datos, que permitirá gestionar un sitio web para una tienda de ropa. Existen dos tipos de usuarios que accederán a la web: clientes y administradores.

Los **clientes** pueden **registrarse** indicando su nombre, contraseña, email y su talla de ropa (S, M, L, XL, XXL). Los clientes pueden hacer **login** y, una vez dentro, pueden escoger qué productos desean comprar en una única **página de listado de productos** que muestra todos los productos de la tienda en una tabla (con una imagen y descripción por cada producto) (no hay carrito de compra, sólo una página única con todos los productos). Mediante checkboxes, el cliente elige los productos que desea comprar y pulsa en un botón. El sistema le muestra como quedaría su pedido en una **página de resumen del pedido**, con detalle del precio de cada producto elegido y el importe total del pedido. Ésta es sólo una página informativa de lo que le costaría el pedido, pues la funcionalidad de compra en sí misma no se incluye. Cada producto puede tener un precio distinto según la talla (las tallas más grandes, XL o XXL, pueden ser más caras que las pequeñas, S o M). Por tanto, el sistema debe calcular el precio de cada producto (en la página de resumen del pedido) en función de la talla del cliente (la cual introdujo éste en su formulario de registro). Algunos productos pueden no estar disponibles en todas las tallas. En el caso de que algún producto elegido por el cliente no está disponible en su talla, se indicará esto en la web (con detalle de qué producto no está disponible) y no se incluirá en el pedido.

Los **administradores**, una vez se loguean como tales, acceden a la **página de listado de productos para administradores**. Éstos pueden **borrar productos** marcando las filas de la tabla que deseen y pulsando en un botón para borrar. Además, pueden **añadir productos** con un botón de añadir que lleva a un **formulario de alta de producto** que permite introducir los datos del nuevo producto. Los datos que almacena el sistema de los productos son los siguientes: nombre, descripción, imagen, tallas y precios. En concreto, estos dos últimos campos son cadenas de caracteres con las diferentes tallas y sus precios asociados separados por ";". Por ejemplo, un producto podría ser: {"Pantalón Gris", "Pantalón gris de tela para hombre", "(nombre fichero de imagen)", "M;L;XL", "29,95;29,95;32,95"} (por ejemplo, este producto no tiene tallas S ni XXL). El formulario de alta de producto incluirá mediante checkboxes las diferentes tallas posibles (S, M, L, XL, XXL) y un cuadro de texto junto a cada una para ingresar un precio. El administrador marcará las tallas que están disponibles para el producto y escribirá el precio de cada una.

Desde el punto de vista técnico, todas las entradas del usuario deben ser saneadas para **evitar inyecciones** tanto de HTML como de SQL, cuando proceda. Las contraseñas deben ser cifradas y descifradas mediante las funciones ***password_hash()*** **y** ***password_verify()***. Se utilizará una **variable se sesión** para controlar el usuario logueado en todas las páginas de la aplicación web. Se permitirá hacer **logout** desde cualquiera de ellas. Se guardará una **cookie** con caducidad que contendrá el nombre del usuario que se ha logueado, para que éste aparezca relleno automáticamente en la página de login en próximas ocasiones.

Encontrará en el material adicional la base de datos exportada (con datos de ejemplo), las imágenes y las vistas que se han de generar desde las que podrá extraer el código HTML a emplear (use dicho código para no perder tiempo en esto).

Actividades a realizar

Para implementar la aplicación realice cada una de las siguientes actividades:

1. **[2.25 puntos]** El sistema dispone de una página inicial con un formulario de login (vista: *login.html*) y un botón de registro que lleva a una página con el formulario de registro (vista: *registro_usuario.html*). Desarrolle ambas funcionalidades, login y registro **(0.5 puntos)**. No se permiten registros de usuarios administradores, sólo de usuarios con tipo cliente. Tenga en cuenta que se guarda el *hash* de las contraseñas en la BD, para ello utilice las funciones *password_hash()* y *password_verify()* para cifrar y comprobar las contraseñas, respectivamente. En el material adicional encontrará un documento, *Manual_password_hash_verify.pdf*, con información sobre como usar dicha función **(0.25 puntos)**. Se asegurará que el sistema no puede verse sometido a ataques de inyección de SQL **(0.1 puntos)**.

   Una vez realizada con éxito la identificación, se definirá una variable de sesión para conocer en el resto de páginas que el usuario se ha identificado con éxito y cuál es su nombre de usuario (campo *nombre* de la tabla usuarios) **(0.4 puntos)**, mostrándose el contenido de la misma en el saludo al usuario en las diferentes páginas **(0.2 puntos)**.

   Tenga en cuenta que, al estar el usuario identificado, cada página de la aplicación tendrá un botón que permitirá cerrar la sesión (logout), tras lo cual se volverá a mostrar la página de login **(0.4 puntos)**. Se establecerá una *cookie* con duración de 30 días que recordará el usuario con el que se logueó y lo mostrará prerelleno en el formulario de *login* **(0.4 puntos)**.

2. **[1.5 puntos]** Una vez realizado el login, la aplicación redirigirá al usuario a la página de listado de productos **(0.25 puntos)**. En esta página se mostrará un listado en forma de tabla con todos los productos de la tabla *productos* de la BD (respetando el formato definido en la vista: *listado_productos.html*) **(1 punto)**. Tenga en cuenta que cada producto tiene asociada una imagen que deberá mostrarse en cada fila del listado de productos **(0.15 puntos)**. Recuerde que si el usuario accediera a esta página directamente (por ejemplo, escribiendo la URL) y no estuviera identificado, redirigirá al usuario a la página de login **(0.1 puntos)**.

3. **[3.5 puntos]** Amplíe el punto anterior, teniendo en cuenta que la página mostrará una información diferente dependiendo del tipo de usuario que haya accedido a la página, teniendo en cuenta las siguientes consideraciones por tipo de usuario:
   1. Usuarios ***administrador*** (el campo *tipo* de la tabla *usuarios* de la BD es *"administrador"*), se mostrará:
      - Un checkbox en cada fila de la tabla de productos para marcar un producto y un botón al final de la página para borrar los productos marcados. Implementar el borrado de productos como acción del botón. Tras borrar productos, se mostrará de nuevo el listado actualizado con los productos existentes. **(1.5 puntos)**
      - Un botón al final de la página para añadir un producto nuevo. Al pulsar sobre él nos mostrará un formulario con los siguientes campos y sus respectivas restricciones (vista: *alta_producto.html*) **(0.7 puntos)**:
        - Nombre del producto: no podrá dejarse en blanco y debe ser de tipo cadena (utilice para ello la siguiente expresión regular: *'/^[[:alpha:]]+$/').*
        - Descripción: no podrá dejarse en blanco y debe ser de tipo cadena.
        - Tallas: checkboxes con las etiquetas S, M, L, XL y XXL.
        - Precios: debe ser numérico (utilice para ello la siguiente expresión regular: *'/^[0-9]+([,][0-9]+)?$/').* Son obligatorios sólo aquellos precios cuyo checkbox de talla esté marcado.
        - Imagen: debe ser un archivo de tipo imagen (compruebe el tipo MIME de la misma) y su tamaño máximo será de 200 KB. No es obligatorio adjuntar una imagen (Tenga en cuenta que si no se especifica el archivo, el valor del parámetro *error* del archivo será 4).

      Si se cumplen todos los criterios, se insertará el producto en la base de datos **(0.6 puntos)** y se mostrará de nuevo el listado de todos los productos **(0.2 puntos)**.
   2. Usuarios ***cliente*** (el campo *tipo* de la tabla *usuarios* es *"cliente"*)*:* se mostrará en el listado de productos un checkbox en cada fila para marcar productos y un botón al final de la página para realizar un pedido con esos productos. Al pulsar sobre él nos redirigirá a la página de resumen del pedido (en la siguiente Actividad 4) **(0.5 puntos)**.

4. **[2.75 puntos]** Crear una página de resumen del pedido que se genere dinámicamente cuando el usuario pulse en el botón de realizar pedido (Actividad 3, apartado 2). Esta página de resumen del pedido mostrará una tabla con los productos previamente elegidos por el usuario y el importe de cada uno de ellos según la talla del usuario que está logueado **(2 puntos)**. Al final de la página debe aparecer el importe total del pedido **(0.75 puntos)**.

Material suministrado

Como material adicional dispondrá del fichero material.zip que contendrá:

- Carpeta **BBDD**, fichero *tiendaRopa.sql*: Script de creación de la base de datos. Existe ya creado un usuario "admin" con clave "admin" de tipo administrador y un usuario de tipo cliente "Pepe" con clave "pepe".
- Carpeta **Vistas**, ficheros *login.html*, *registro_usuario.html*, *listado_productos.html* y *alta_producto.html*, con el código HTML de cada vista.
- Carpeta **img**: donde encontrará imágenes de prueba para los productos de la tienda registrados en la base de datos, así como algunas más para que pueda realizar pruebas (por ejemplo, no debería permitir subir *imagen_grande.jpg*).
- Carpeta **Documentación**, fichero *Manual_password_hash_verify.pdf:* con información sobre las funciones *password_hash* y *password_verify*.

Datos de la Práctica

Autor del documento: Gualberto Asencio Cortés (Diciembre 2017). Basado en el examen de 2016.

Revisiones del documento

1. Carlos D. Barranco (Diciembre 2017): Arreglo de errata menores.