



Informática Documental
2003/2004

Práctica Final

Biblioteca Leonardo Da Vinci

Jaime Pérez Crespo

japecre@lsub.org

Laboratorio de Sistemas, Grupo de Sistemas y Comunicaciones

Teléfono: 91-2265644

Objetivos

El objetivo de esta práctica es familiarizarse con las distintas tecnologías y posibilidades que hoy día ofrece la web para la creación y distribución de contenidos.

Dentro de las inmensas posibilidades que se nos ofrecen, nos centraremos en las aplicaciones de gestión documental, realizando para ello un estudio de tecnologías adecuadas a nuestro propósito, como pueden ser lenguajes de *scripting* o gestores de base de datos.

Tecnologías

Para la realización de este proyecto se han utilizado las siguientes tecnologías disponibles en el mercado actual:

- **MS Access:** se ha optado por utilizar un programa sencillo para facilitar la tarea del diseño e implementación de la base de datos.
- **MS ADODB:** el gestor de microsoft para bases de datos, que permite utilizar aquellas diseñadas con el programa anteriormente mencionado de forma fácil y rápida.
- **ASP:** Active Server Pages, usualmente conocido como ASP, es un lenguaje de scripting basado en *basic*, que ejecuta del lado del servidor. Permite generar páginas web en tiempo real, así como muchas otras funcionalidades entre las que se encuentran la interconectividad con ADODB para el acceso a bases de datos y manipulación de las mismas a través de su propia API. Se ha tomado la decisión de mantener todo el código dinámico en la parte del servidor mediante ASP por una sencilla razón. Pese a que esto puede ser costoso, y el cliente puede realizar de su lado ciertas tareas mediante lenguajes como *JavaScript*, un buen diseño de la aplicación implica la verificación y comprobación constante de los datos introducidos por el usuario. Así, pese a que cierto precálculo podría realizarse en el propio navegador, interpretando código *JavaScript*, el servidor tendrá exactamente la misma carga. Puesto que no tiene sentido duplicar las comprobaciones en cliente y servidor, se ha decidido omitirlas en el lado del cliente. Esta aproximación al problema es más costosa pero también más fiable. Un usuario con ciertos conocimientos que se salte las comprobaciones realizadas en el navegador no podrá insertar datos inválidos en la base de datos, pues éstos son comprobados permanentemente.

- **XHTML:** se ha decidido seguir el estándar del *World Wide Web Consortium* (W3C) para la composición de las páginas que son enviadas a los clientes. La razón fundamental es permitir la accesibilidad y usabilidad óptimas para los usuarios, sea cual sea su plataforma. Utilizando el mencionado estándar nos aseguramos que se cumpla dicho objetivo, al deber todos los navegadores interpretarlo en igualdad de condiciones. Así, se ha comprobado que las páginas servidas por el sistema de biblioteca cumplen estrictamente el estándar, y son visualizadas correctamente desde los siguientes navegadores:
 - Microsoft Internet Explorer.
 - Mozilla.
 - Mozilla FireFox.
 - Opera.
 - Netscape.
 - Konqueror.

Cuestiones de diseño

Aparte de las decisiones de diseño que han llevado a usar unas u otras tecnologías, y que ya han sido comentadas, se han tomado ciertas decisiones relativas al desarrollo inherente de la práctica:

- La biblioteca no es puramente virtual. Esto es, tiene una sede física a la que hay que acudir para realizar ciertas operaciones, como efectuar un préstamo, devolverlo, o acreditarse para darse de alta. A día de hoy es difícil acreditar la identidad de una persona a través de la red. Existen aproximaciones bastante fiables pero no infalibles.

Una solución tan buena como la adoptada hubiese sido requerir a los usuarios una tarjeta de crédito válida para registrarse. Con dicho sistema, y siempre y cuando los servicios concretos que requieran transacciones con la tarjeta de crédito se lleven a cabo por canales seguros, como SSL, se podría verificar la identidad de los usuarios a través de entidades de cobro. No sería necesario efectuar ningún tipo de pago por parte de los mismos, sino sencillamente proporcionar su tarjeta de crédito. Esto permitiría a la biblioteca consultar con alguna entidad asociada la validez de dicha tarjeta, y por tanto la autenticidad de su poseedor.

Otra forma de solucionar este problema podría ser la utilización de un sistema de certificados electrónicos. Se requeriría al usuario la inclusión de un certificado en su registro, firmado por una entidad conocida y fiable, como la Real Fábrica de Moneda y Timbre, de forma que con dicho certificado y la clave pública firmada del cliente se podría verificar la identidad del mismo, estableciendo un margen de confianza en el expendedor del certificado. El problema de esta aproximación radica en que se requiere al cliente más recursos que los habituales. Cualquiera tiene una tarjeta de crédito hoy día,

pero muy poca gente, por contra, posee un certificado expedido por una entidad reconocida. Afortunadamente, con la implantación del DNI electrónico a finales del presente año, este proceso será viable, ya que el propio DNI contendrá el certificado de identidad requerido.

- No se ha separado la web de la biblioteca en distintos módulos bien delimitados. Existen diversas razones para apoyar esta decisión. En primer lugar, no está claro el hecho de que un usuario no pueda ser administrador de la base de datos, y a la inversa. Cualquier administrador puede querer disponer de los recursos facilitados a los usuarios.

Por otro lado, evita problemas de seguridad. La ocultación nunca es una buena política de seguridad, pero en este caso es una medida complementaria muy útil. Ningún atacante tiene porque conocer la existencia de páginas exclusivas de administradores. De hecho, en ninguna parte se hace una referencia a dicha posibilidad, por lo que desde el punto de vista de un usuario normal, esas funcionalidades pueden no existir. Esto facilita (que no evita) que a un atacante le sea más difícil tratar de conseguir acceso a la base de datos, ya que primero deberá averiguar cómo puede conseguir ese acceso con derechos de administrador.

Así pues, la decisión es sencillamente agregar o eliminar opciones en los menús de navegación de la página dependiendo de la identidad del usuario registrado. Si dicho usuario no tiene más privilegios de los normales, sus opciones serán exclusivas de un usuario corriente, y no sabrá de la existencia de opciones de administración. Si por contra el usuario está marcado en la base de datos como administrador de la misma, en su menú de opciones personales se incluirán enlaces a las distintas páginas desde las que podrá manejar el sistema.

- Se ha optado por no incluir contenidos multimedia que se puedan consultar en línea. Este tipo de contenidos tiene un claro inconveniente, y es que no se puede limitar el acceso a los mismos. Si bien en el caso de la biblioteca no se trata de una entidad comercial que pretenda hacer negocio con sus servicios, los contenidos que ofrece están sujetos a leyes y restricciones de *copyright* que la biblioteca debe proteger por su propio interés. Por muchos sistemas que se ideen para restringir y limitar el acceso a los recursos, no se puede evitar que los usuarios hagan el uso que quieran con ellos. Para que un usuario vea un vídeo, por ejemplo, se puede utilizar una solución de *streaming*, que difunde el vídeo a través de la red en tiempo real, visualizándolo en algún reproductor empotrado en el cliente. Si bien aparentemente no es fácil obtener el vídeo original a través de la reproducción realizada del mismo, la información que lo compone ha viajado por la red y ha sido enviada a la máquina del cliente. Nada impide que esa información sea almacenada allí y reproducida cuantas veces se quiera. Por ello, es mejor no ofrecer servicios de contenidos en línea, antes que intentar limitar algo que no se puede evitar de ninguna forma.