

PRÁCTICA 5B. AUTENTICACIÓN II

El propósito de la presente práctica es integrar un servicio de autenticación de usuarios en una aplicación desarrollada por el propio alumno.

Se propone emplear el paquete *PEAR* de autenticación *AUTH* para constatar y verificar la identidad de los usuarios, utilizando como mecanismo interno de acceso a datos el paquete *MDB2* de *PEAR*.

Al contrario que en la práctica 5a, para completar la práctica deberán emplearse las instrucciones propias del paquete *AUTH* de *PEAR*, y en ningún caso deberán lanzarse consultas directamente a la base de datos mediante el paquete *MDB2*.

5.1 Materiales.

El material suministrado para la práctica es:

- Código fuente del sitio web con indicaciones y huecos a rellenar.
- Base de datos con datos iniciales.

5.2 Objetivos.

Los objetivos de la práctica son:

- Aprender a utilizar el paquete *AUTH* de *PEAR*.
- Conocer el funcionamiento de los sistemas de autenticación de usuarios.

- Conocer los mecanismos habituales de control de acceso.

5.3 Actividades a realizar.

Las actividades a realizar son:

- Modificar el fichero "*auth_concrete.php*" para contrastar la información de usuario con la tabla apropiada de la base de datos, y para comprobar si el usuario ha sido validado previamente. Utilizar la librería AUTH sobre *MDB2*. En ningún caso deben lanzarse consultas directamente mediante *MDB2* para realizar las comprobaciones.
- Modificar el método *clean* de *AuthClass* para que no elimine la información de seguridad del paquete *AUTH* de *PEAR*, que se almacena en la sesión.
- Añadir el código necesario al fichero "*iniciar_sesion_admin.php*" para que valide las credenciales introducidas por el usuario utilizando el objeto definido en el punto anterior.
- Impedir el acceso a aquellas páginas que consideres que deben estar protegidas hasta que el usuario se haya registrado en el sistema. Redirigir a la página de logado en el caso de que no se haya logado en el sistema. Utilizar los métodos del objeto creado en el primer punto.
- Limitar la duración total de la sesión a 5 minutos, y el tiempo de espera entre acciones a 60 segundos. Para ello, utilizar las constantes definidas en el fichero "*auth_concrete.php*".
- Hacer los cambios necesarios en el objeto *AuthClass* para que si se han superado los tiempos establecidos al invocar al método *checkLog* se redirija automáticamente a la página de logado,

informando sobre el problema. Se aconseja reducir los tiempos de caducidad para efectuar las pruebas.