Práctica 7.5 - Seguridad en aplicaciones Java EE

1. Objetivos

El objetivo de esta práctica es aprender a gestionar la seguridad en aplicaciones Java EE, restringiendo el acceso a las páginas JSF y a los métodos de los componentes EJB en base al establecimiento de usuarios y roles.

2. Actividades

Los pasos a seguir en la práctica serán los siguientes:

1. Definir la política de control de accesos de la aplicación:
   - Definir los posibles roles de la aplicación

2. Configurar el servidor Glassfish:
   - Dar de alta un conjunto de usuarios (a elección del alumno) de acuerdo a los roles identificados anteriormente.

3. Configurar la gestión de la seguridad a nivel de la capa de negocio:
   - Anotar los componentes EJB de manera que den soporte al control de accesos definido previamente.
   - Configurar el mapeado de roles a usuarios en el correspondiente descriptor de despliegue `glassfish-ejb-jar.xml`.

4. Configurar la gestión de la seguridad a nivel de la capa de presentación web:
   - Configurar la aplicación web de manera que de soporte a la política de accesos definida. Esta configuración se realiza en el descriptor de despliegue `web.xml`.
   - Configurar el mapeado de roles a usuarios en el correspondiente descriptor de despliegue `glassfish-web.xml`.
   - Crear la vista correspondiente al gerente vacía (o con un simple mensaje) sólo para el propósito de asignar sus propiedades de seguridad.

5. Desplegar la aplicación y comprobar que funciona el control de accesos establecido.

   Nota: Para que funcione el intercambio de credenciales entre el contenedor web y el contenedor de EJBs, es necesario realizar las invocaciones a través de HTTPS, lo cual deberá ser también configurado en el descriptor web.xml.

3. Entrega y evaluación

La práctica se entregará de manera conjunta con el resto al final del cuatrimestre.

Patricia López Martínez