Ejercicios de seguridad en Tomcat

Índice

¡Cuidado!

Antes de realizar los ejercicios debes estar seguro de que el JAR con el driver de MySQL está en el directorio `lib` de Tomcat. En caso contrario Tomcat no podrá usar la base de datos para autentificar a los usuarios.

1. Creación de un Realm de base de datos (1 pto)

Vamos a crear la configuración y la estructura necesarias para un realm de Tomcat con BD, que usaremos en el segundo ejercicio para asegurar la aplicación de comentarios.

1. En las plantillas de la sesión hay un script SQL que crea las tablas necesarias para almacenar logins, passwords y roles. Ejecútalo y comprueba que se han creado correctamente y que contienen usuarios creados.
2. Las plantillas también incluyen un proyecto de Eclipse llamado `testJDBCRealm` que ya está configurado para usar la BD para autentificación. **Tendrás que crear el META-INF/context.xml con la información del JDBCRealm**. Mira el ejemplo de las transparencias. Una vez creado el realm, prueba a identificarte como "espe", "espe" (debes tener permiso de acceso) y luego como "pepe","pepe" (no lo tendrás). Ten en cuenta que como la aplicación usa autentificación BASIC debes cerrar el navegador si quieres entrar con otro usuario (en Eclipse esto no es posible, así que tendrás que hacerlo desde un navegador externo).

2. Seguridad basada en formularios (1 pto)

Vamos a asegurar la aplicación de comentarios con seguridad basada en formularios, de modo que solamente los usuarios con rol "registrado" puedan insertar comentarios. Para ello, tendrás que:

1. Crear la configuración del realm en el `context.xml` de la aplicación. Puedes tomar como ejemplo la de la aplicación `testJDBCRealm` del ejercicio anterior
2. Crear una página `login.html` con un formulario de autentificación como se indica en los apuntes.
3. Configurar la seguridad protegiendo la URL "/addComentario" para que solo puedan acceder a ella los usuarios con rol "registrado". Usa las etiquetas vistas en los apuntes para configurar seguridad basada en formularios.
4. Comprobar que al intentar añadir un comentario se salta a la página de login y tras introducir usuario y password válido se permite el acceso

3. Seguridad del servidor (1 punto)

En las plantillas de la sesión tienes una aplicación llamada visitas.war muy similar a la de comentarios, pero que guarda los comentarios enviados por los usuarios en un fichero. En

este ejercicio no es necesario que uses Eclipse

1. Despliega el war copiándolo manualmente al directorio webapps.
2. Arranca manualmente Tomcat entrando en su directorio bin y ejecutando "./startup.sh -security" para activar las políticas de seguridad. Comprueba que la aplicación a un error al intentar guardar el comentario, ya que por defecto las aplicaciones web no pueden crear ficheros con las restricciones de seguridad activas.
3. Modifica el fichero de Tomcat "conf/catalina.policy" añadiendo al final un permiso para guardar archivos.
   - Toma como modelo el ejemplo de las transparencias para darle el permiso en este caso a la aplicación "visitas"
   - El "permission" para guardar ficheros es java.io.FilePermission "directorio_donde_hay_permiso", "read,write"
4. Para Tomcat ("./shutdown.sh") y vuelve a arrancarlo de nuevo con la seguridad activada ("./startup.sh -security") y comprueba que ahora sí se guarda el archivo "prueba.txt"