Ejercicios de seguridad en aplicaciones web

Índice

1. Políticas de seguridad

Probar la aplicación `visitas.war` de la plantilla (instaladla subiendo el WAR desde el manager de Tomcat). Ejecutar ahora Tomcat de manera que haga uso del fichero de políticas de seguridad. Para ello, en Linux se ejecuta el script `startup.sh -security`. En Windows, debemos abrir la configuración de Tomcat (botón de *Inicio*, y luego ir a *Todos los programas - Apache Tomcat 5.5 - Configure Tomcat*). Después, en el cuadro que nos sale, ir a la pestaña de *Java*, y en el cuadro *Java Options* añadir las siguientes líneas:

```
-Djava.security.manager
-Djava.security.policy==
    C:\Archivos de programa\Apache Software Foundation\Tomcat
5.5\conf\catalina.policy
```

En la segunda línea, aseguraos de que la ruta hasta el fichero `catalina.policy` es la correcta.

Tras esto, ya podemos rearrancar Tomcat. Con la política de seguridad por defecto las aplicaciones web no pueden escribir en disco. Probar qué ocurre con la aplicación **visitas**. Dar permisos a la aplicación para que pueda escribir datos en el disco.

NOTA: Deberéis editar el fichero `conf/catalina.policy` y crear un grupo de permisos para la aplicación `visitas` (fijaos en los grupos que ya hay), poniéndole un permiso de tipo `java.io.FilePermission`:

```
grant codebase "..." {
        permission java.io.FilePermission "ruta_absoluta_del_fichero",
"permiso";
};
```

donde la ruta será la ruta hasta el fichero que se quiere escribir, y el permiso será de escritura (`write`)

2. Trabajando con seguridad declarativa

Incluir seguridad declarativa en la aplicación **conversorSeguro** (descomprimid el fichero ZIP de la plantilla dentro del `webapps` de Tomcat), para que solo puedan tener acceso al formulario y al servlet aquellos usuarios que tengan rol `conversor`.

- Modificar el fichero `tomcat-users.xml` para crear algún usuario con este rol
- Configurar la seguridad declarativa utilizando autentificación por formulario (FORM)
- Re-comprimid la aplicación con los cambios introducidos, y volvedla a guardar en el proyecto de Eclipse

3. (*)Seguridad declarativa con base de datos

En las plantillas de la sesión hay una base de datos MySQL llamada `authority` con dos tablas: `users` almacena logins y passwords de los usuarios, y `user_roles` relaciona logins y roles.

- Crear dicha base de datos ejecutando el script de la plantilla en MySQL. Para ello, puedes utilizar el fichero de Ant que se proporciona para instalar la base de datos.
- Crear un *realm* de Tomcat enlazado con dicha base de datos y asociado a la aplicación **conversorSeguro** (deberéis crear un `Context` de la aplicación e incluirle un `Realm`). Como base para dicho *realm* se puede utilizar el que viene comentado en el server.xml original de Tomcat. Los nombres de las tablas coinciden, deberéis modificar el de algunos campos y el login y password de la base de datos. Comprobar que efectivamente se pueden añadir usuarios de manera dinámica a la base de datos y Tomcat los toma sin necesidad de rearrancar.