Grupo 12

PROTOCOLO HTTPS

HTTP es el acrónimo de Hypertext Transfer Protocol (en español protocolo de transferencia de hiper texto). **HTTPS** es igual pero añadiéndole "**Seguro**". Estos dos protocolos se usan para lo mismo, la transferencia de datos.

La diferencia básica entre ambos es la forma en la que viajan los datos. Si los datos son transferidos mediante HTTP, estos viajan en claro y son accesibles para cualquiera que intercepte la comunicación. En cambio, el protocolo HTTPS usa una **conexión segura** mediante un cifrado SSL y por tanto los datos viajan de un modo seguro de un lugar a otro.

Configuración Apache Tomcat

Para configurar este servidor se deben realizar los siguientes pasos descritos:

-**Primer paso**: debemos empezar creando una Keystore. Las claves que Tomcat utilizará para las conexiones SSL, serán almacenadas en un archivo protegido por contraseña llamado “Keystore”. Existen dos formas de crear este archivo, una importando la clave existente al keystore o creando una clave desde cero.

Por simplicidad crearemos nuestro propio certificado autofirmado. Para ello ejecutaremos los siguientes comandos:

cd %JAVA_HOME%\bin

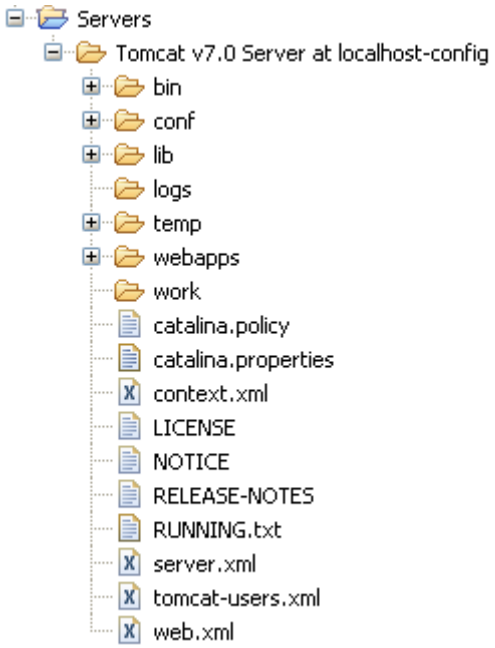
Este comando nos llevará a la carpeta java donde se encuentra nuestro JDK instalado y dentro de la misma a la carpeta bin. Luego introducimos este comando:

keytool -genkey -alias tomcat -keyalg RSA

Al ejecutarlo nos pedirá una serie de datos como contraseña, nombre, organización, ciudad entre otros para completar nuestro certificado autofirmado.

-**Segundo paso**: al rellenar la información solicitada se generará un archivo “.keystore” en la siguiente ruta “C:\Documents and Settings\Student”.

-**Tercer paso**: configurar Tomcat para que use HTTPS y el archivo ".keystore". Para ello vamos a la carpeta servers asociada a nuestro proyecto y clickamos sobre el archivo **server.xml** (Estos mismos archivos se encuentran en la carpeta de configuración de Apache Tomcat v7).



Añadimos las siguientes líneas de código:

<Connector SSLEnabled="true" clientAuth="false"

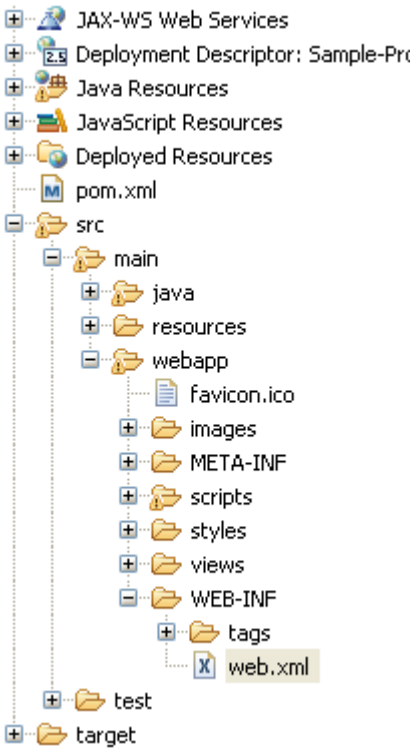
keystoreFile="C:\Documents and Settings\Student\.keystore"

keystorePass="password" maxThreads="150" port="8443" scheme="https" secure="true" sslProtocol="TLS"/>

-keystoreFile: es la ruta donde colocaremos nuestro certificado(incluido en la entrega).

-password: ahí pondremos la contraseña puesta a la keystore en nuestro caso es "DPgrupo12".

-**Paso cuarto:** Para configurar la aplicación web con HTTPS, hemos modificado el **web.xml** de nuestra aplicación añadiendo las siguientes líneas de código:



<security-constraint>

<web-resource-collection>

<web-resource-name>NombreProyecto</web-resource-name>

<url-pattern>/*</url-pattern>

</web-resource-collection>

<user-data-constraint>

<transport-guarantee> CONFIDENTIAL </transport-guarantee>

</user-data-constraint>

</security-constraint>

CONFIDENTIAL: se utiliza para que nuestra aplicación trabaje con SSL.

<url-pattern>/*</url-pattern>: con esta línea conseguimos que cualquier uri de nuestra aplicación tenga un transporte confidencial

**Después de este paso se debe reiniciar Tomcat.

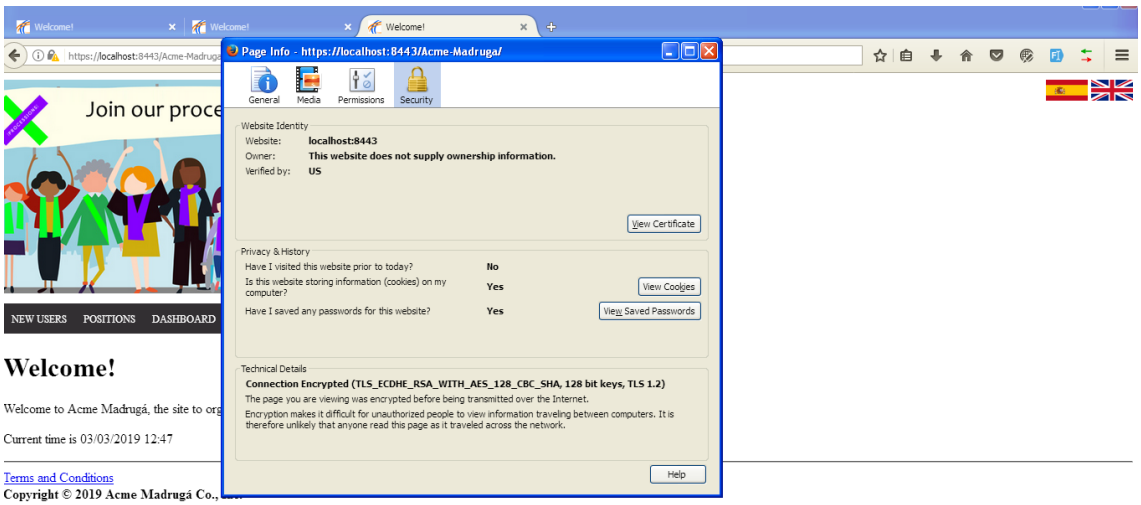


Ilustración 1: certificado autofirmado

Ilustración 2:uso correcto del protocolo https