HTTPS CONFIGURATION

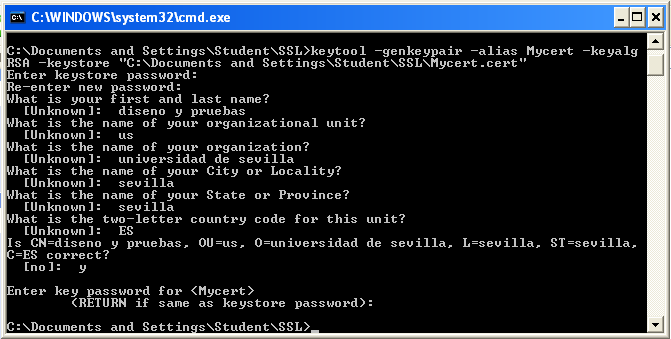
Step by step guide to configure https in Tomcat and our projects.

It is important to follow this steps to configure HTTPS correctly in our application:

STEP 1: We must create the security certificate. To create it, we just need to open a CMD and write the command:

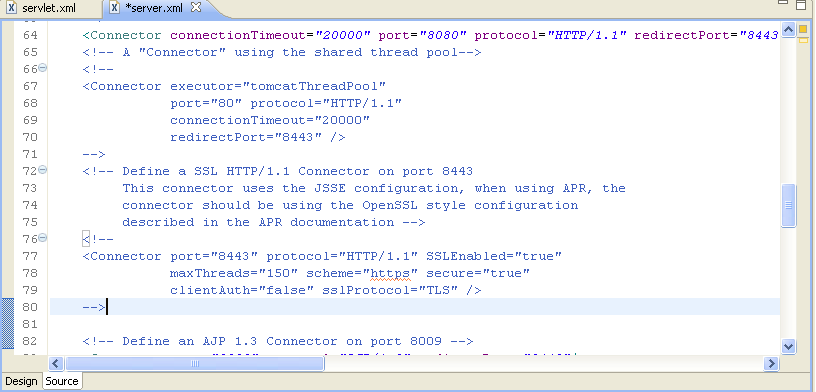
Keytool -genkeypair -alias Mycert -keyalg RSA -keystore “ruta en la que se va a guardar el certificado”.

Then we will need to ask some questions about our organisations, a password and some personal data. We just need to answer the quiestions and the certificate Mycert.cert will be in the path especified.



(PS: in this case, keystore password and key password we are using is “pass123”).

STEP 2: We must configure Tomcat so it accepts the HTTPS protocol. To do it, we have to edit the file “server.xml” in Tomcat:

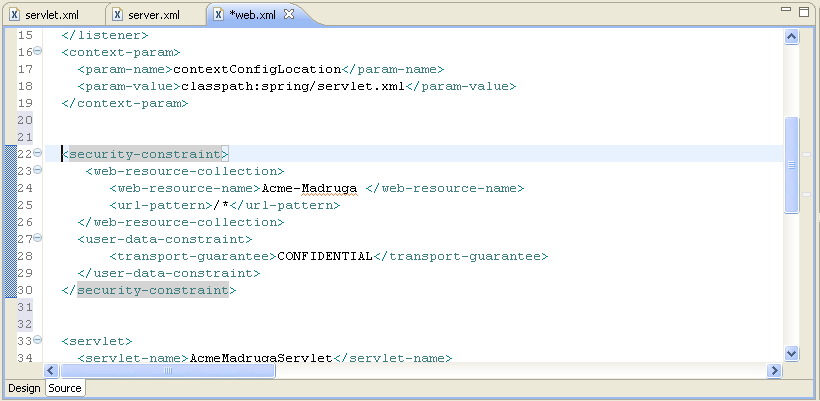


To configure HTTPS in the server we only have to delete the comment of the lines below and add the following atributes:

* KeystoreFile: the installation path in step 1.
* KeystorePass: the pass in the step 1 (in this case, we are using the same password as step 1).

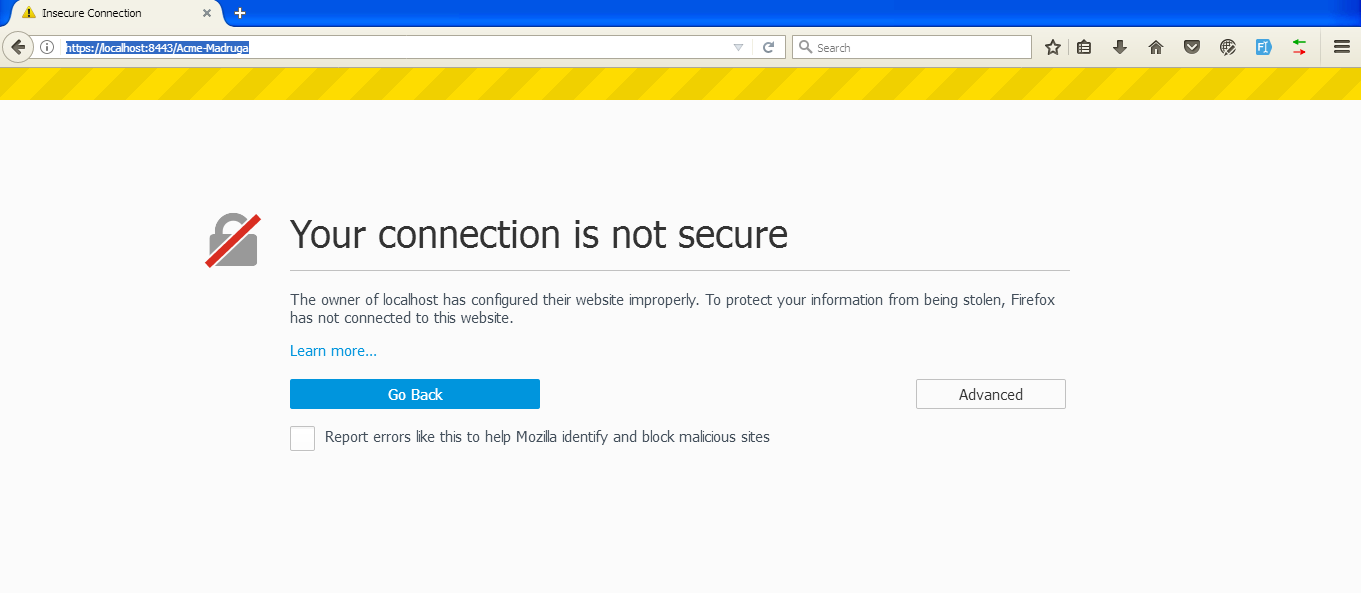
After this step, the file server.xml should look like this:

STEP 3: We must configure our Project so it admits HTTPS. Its pretty simple, we just need to add the following code to the file “web.xml” of the Project:



(PS: Attribute web-resource-name may change depending on the project).

Once completed, just start the server and try to enter <https://localhost:8443/Acme-Madruga>:



Then we must click on “Advanced” and on “Add exception” to add our Project as an exception, and this will allow us to enter the specified webpage.

Once added, we will be redirectioned to the welcome page, and the HTTPS configuration will be finished.