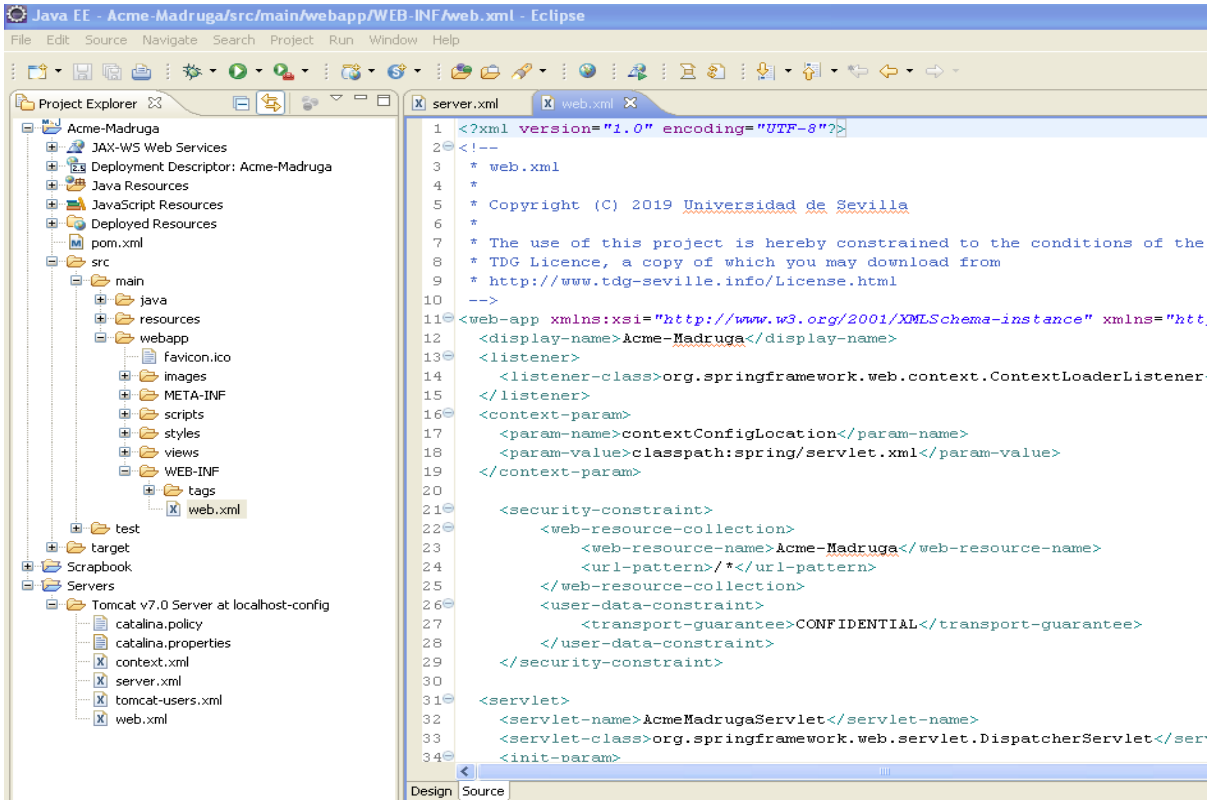
Acme Madrugá – Https Configuration

Configuring our project

To configure our project go to the webapp folder and locate the web.xml file.

We are going to create a new security tag, in this tag we will indicate the name of our project (Acme-Madruga), the url pattern (put "/*" to use https in all our website, not just in the login process), and the transport guarantee constraint "Confidential" to tell the server that the use of SSL is required.

```
<security-constraint>
    <web-resource-collection>
        <web-resource-name>Acme-Madruga</web-resource-name>
        <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <user-data-constraint>
        <transport-guarantee>CONFIDENTIAL</transport-guarantee>
    </user-data-constraint>
</security-constraint>
```

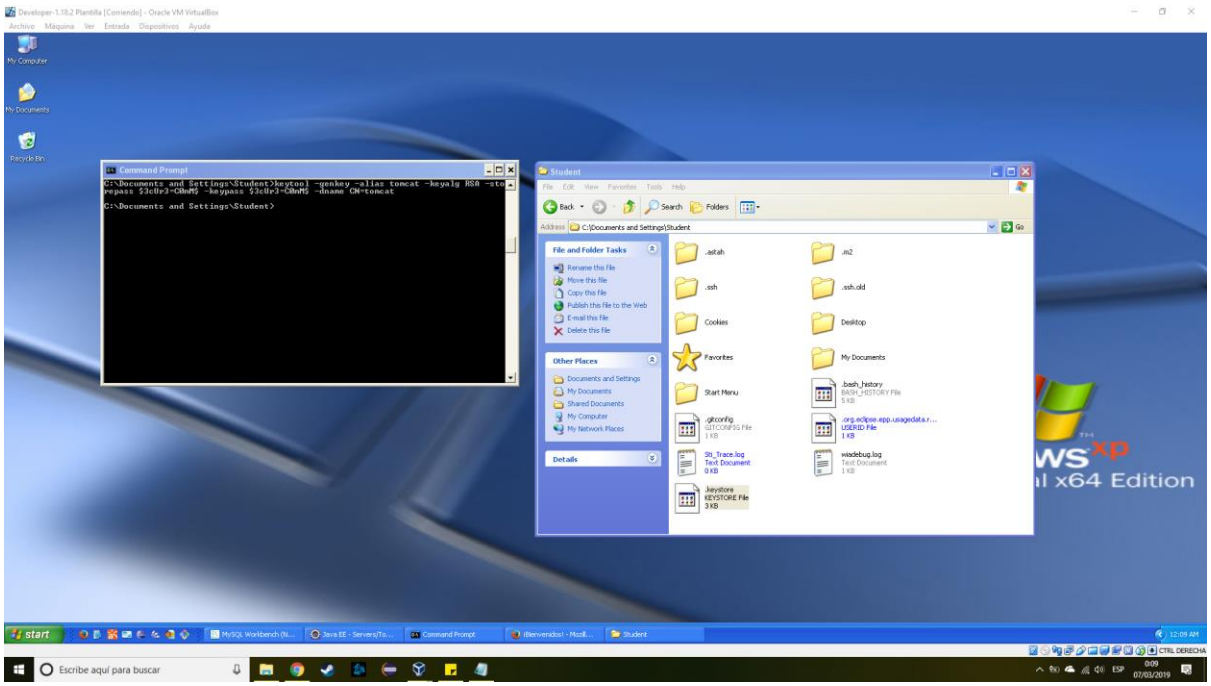


Creating the SSL certificate

To create our certificate we are going to open a command prompt in the location where we are going to stablish the certificate and execute the next command:

```
keytool -genkey -alias tomcat -keyalg RSA -storepass $3cUr3=C0mM$ -keypass $3cUr3=C0mM$ -dname
```

Where keypass is the password of our certificate, in our case we decided to use “$3cUr3=C0mM$”. It will generate the certificate in the user folder.

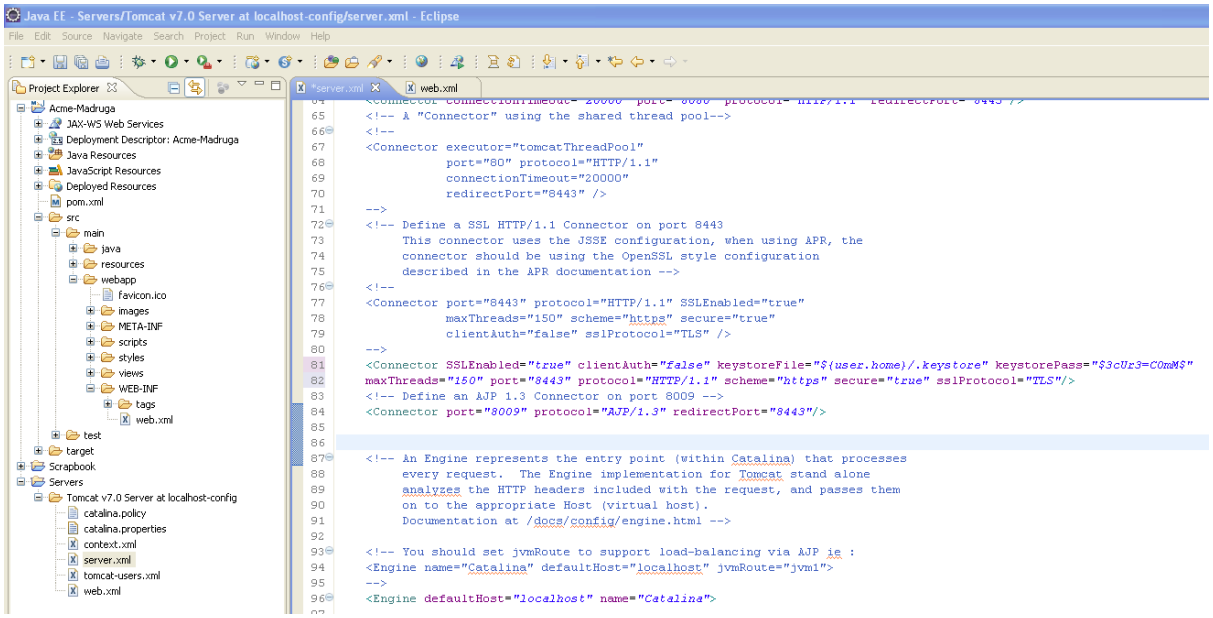


Configuring Tomcat

Configuring Tomcat is really easy, go to your server folder an open server.xml, we are going to define a new Connector tag.

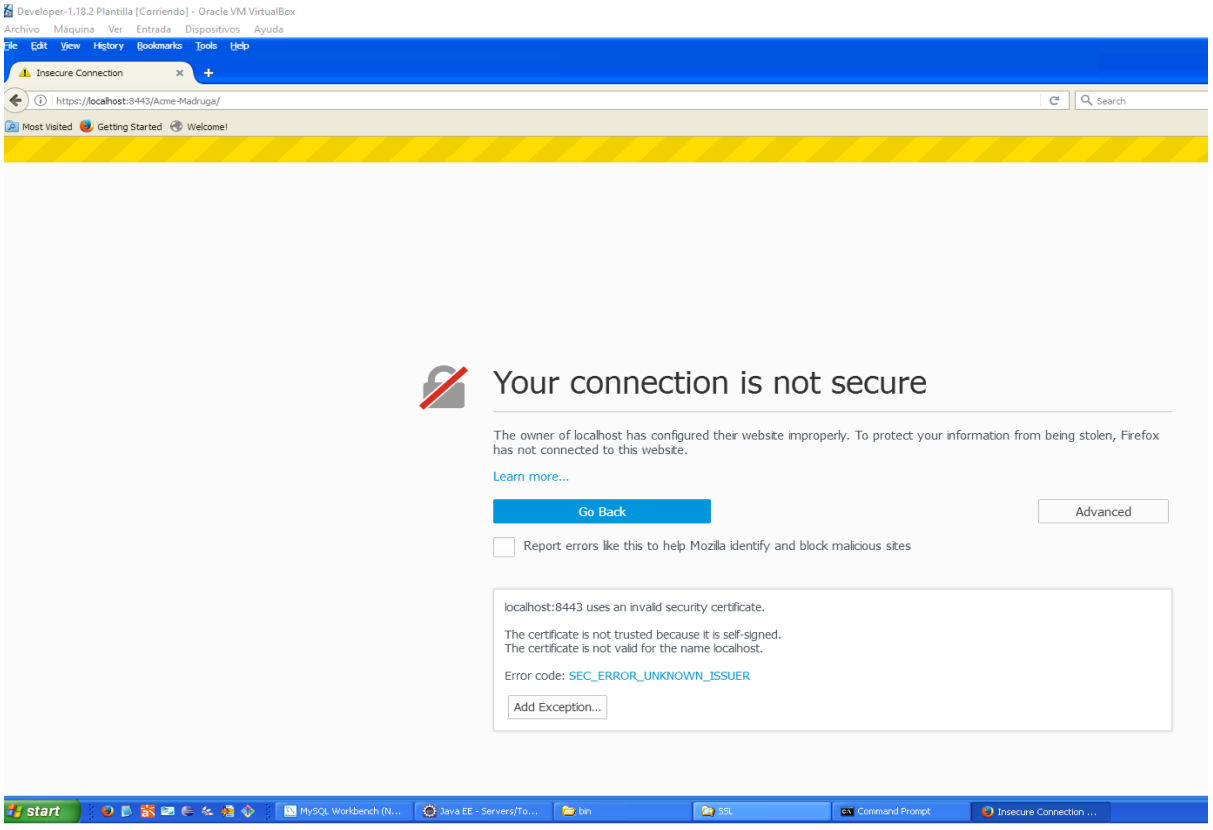
This tag already exist in the file but is commented, you just need to add two new params to indicate the location and password of the certificate:

```
<Connector SSLEnabled="true" clientAuth="false" keystoreFile="${user.home}/.keystore"
keystorePass="$3cUr3=C0mM$"
maxThreads="150" port="8443" protocol="HTTP/1.1" scheme="https" secure="true"
sslProtocol="TLS"/>
```



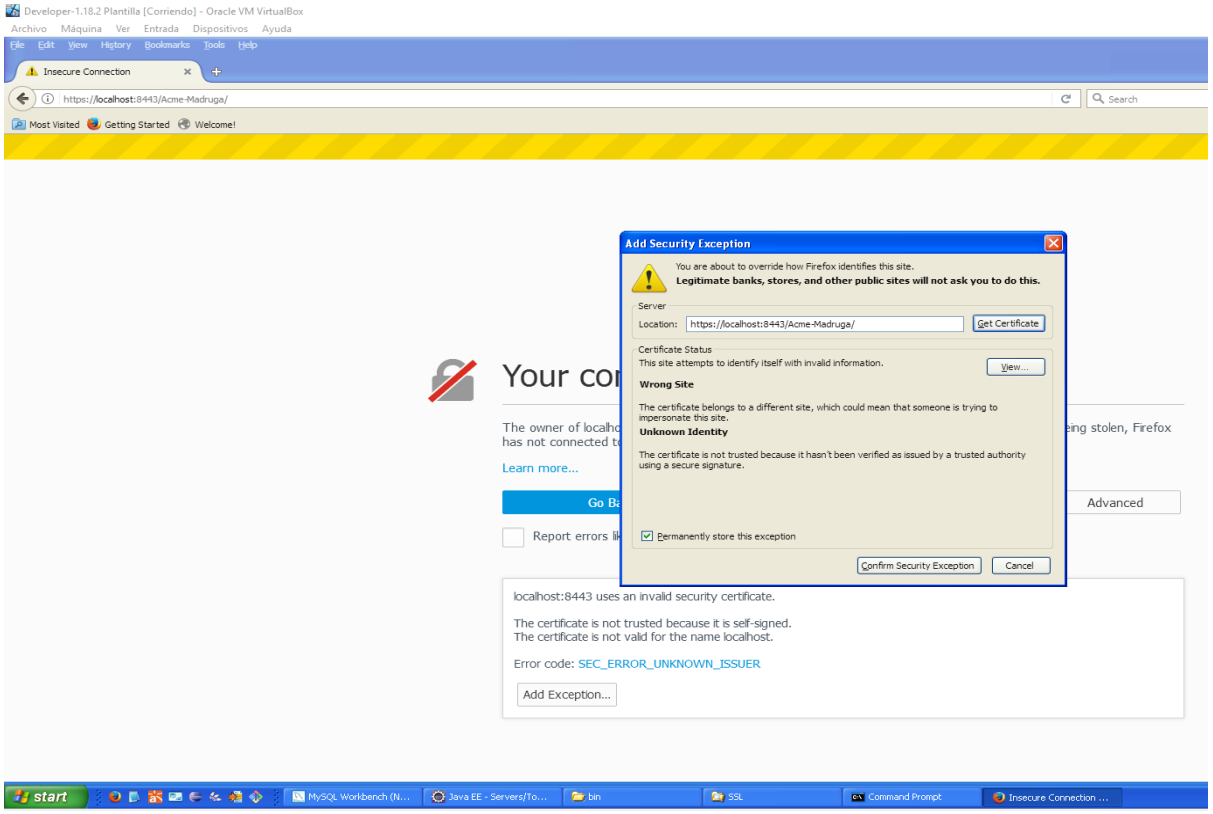
Checking the results

Now that our project is ready, go to http://localhost:8080/Acme-Madruga/



If we see this page, we succeeded configuring https for our application, but since we created our own certificate, the browser will warn us that is probably an insecure page.

Add the exception to the browser and confirm the security exception.

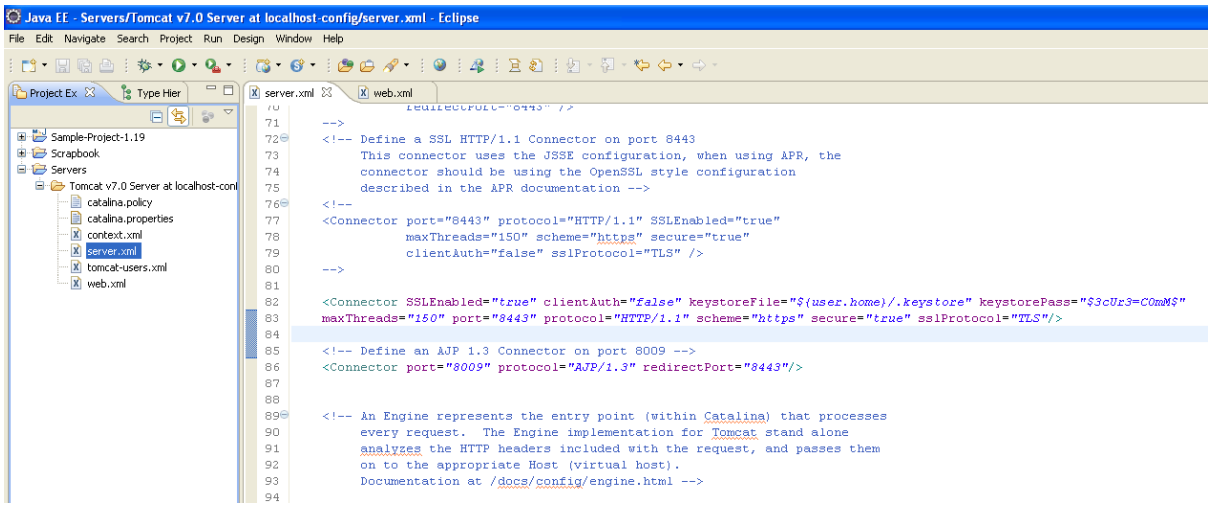

Developer-1.18.2 Plantilla [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
File Edit View History Bookmarks Tools Help
Insecure Connection
https://localhost:8443/Acme-Madruga/
Most Visited Getting Started Welcome!
Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location: https://localhost:8443/Acme-Madruga/
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Wrong Site
The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.
Unknown Identity
The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.
Permanently store this exception
Confirm Security Exception
Cancel
Your co
The owner of localho has not connected t
Learn more...
Go Ba
Advanced
Report errors lik
localhost:8443 uses an invalid security certificate.
The certificate is not trusted because it is self-signed.
The certificate is not valid for the name localhost.
Error code: SEC_ERROR_UNKNOWN_ISSUER
Add Exception...
start
MySQL Workbench (N...
Java EE - Servers/To...
bin
SSL
Command Prompt
Insecure Connection ...


Developer-1.18.2 Plantilla [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
File Edit View History Bookmarks Tools Help
Welcome!
https://localhost:8443/Acme-Madruga/
Most Visited Getting Started Welcome!
ACME MADRUGÁ
LOGIN REGISTER BROTHERHOOD LIST
en | es
Welcome!
Join our processions!
Welcome to Acme Madrugá, the site to organise your processions.
Greetings!
Current time is 02/03/2019 00:03
Copyright © 2019 Acme-Madruga Co., Inc.
start
MySQL Workbench (N...
Java EE - Acme-Madr...
Command Prompt
Welcome! - Mozilla Fir...

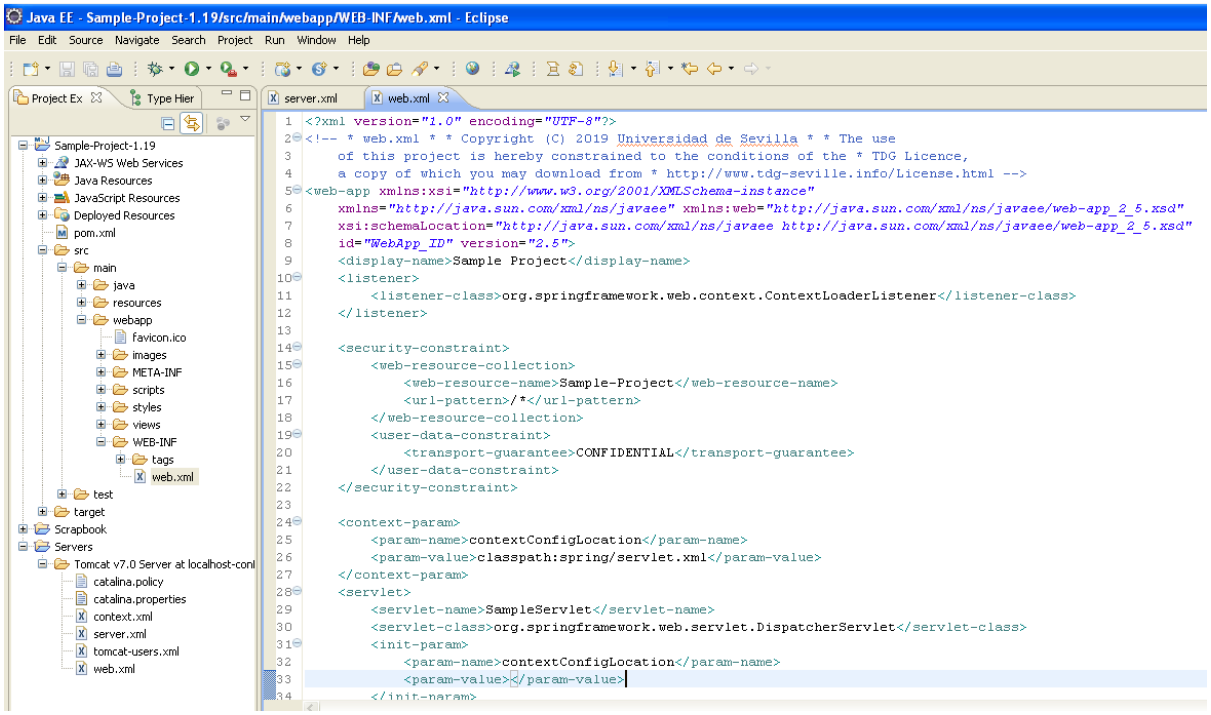
Sample-project

Following this same steps will configure https to the sample-project:

Tomcat server.xml:



Sample project web.xml:



The certificate is the same that we used before in Acme-Madruga.

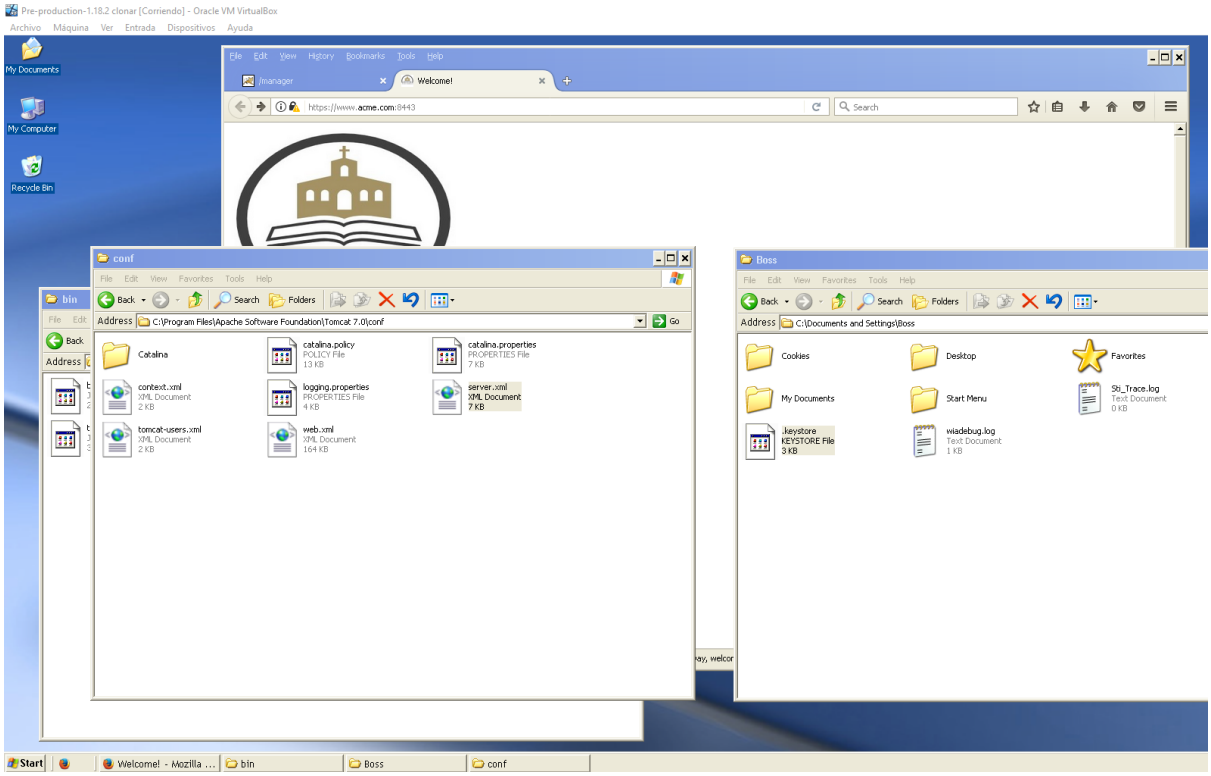
Results:

If you want to check this results please use the sample project and sample workspace that we attached to item 2 and move the certificate (inside sample workspace folder) to the users folder, in our case is C:\Documents and Settings\Student.

Pre-Production

To deploy with https configuration in the pre-production machine we need to do some additional steps.

First, copy the key generated previously (.keystore) and put it in C:\Documents and Settings\Boss. Once you do this, go to C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf\server.xml and open it with notepad.



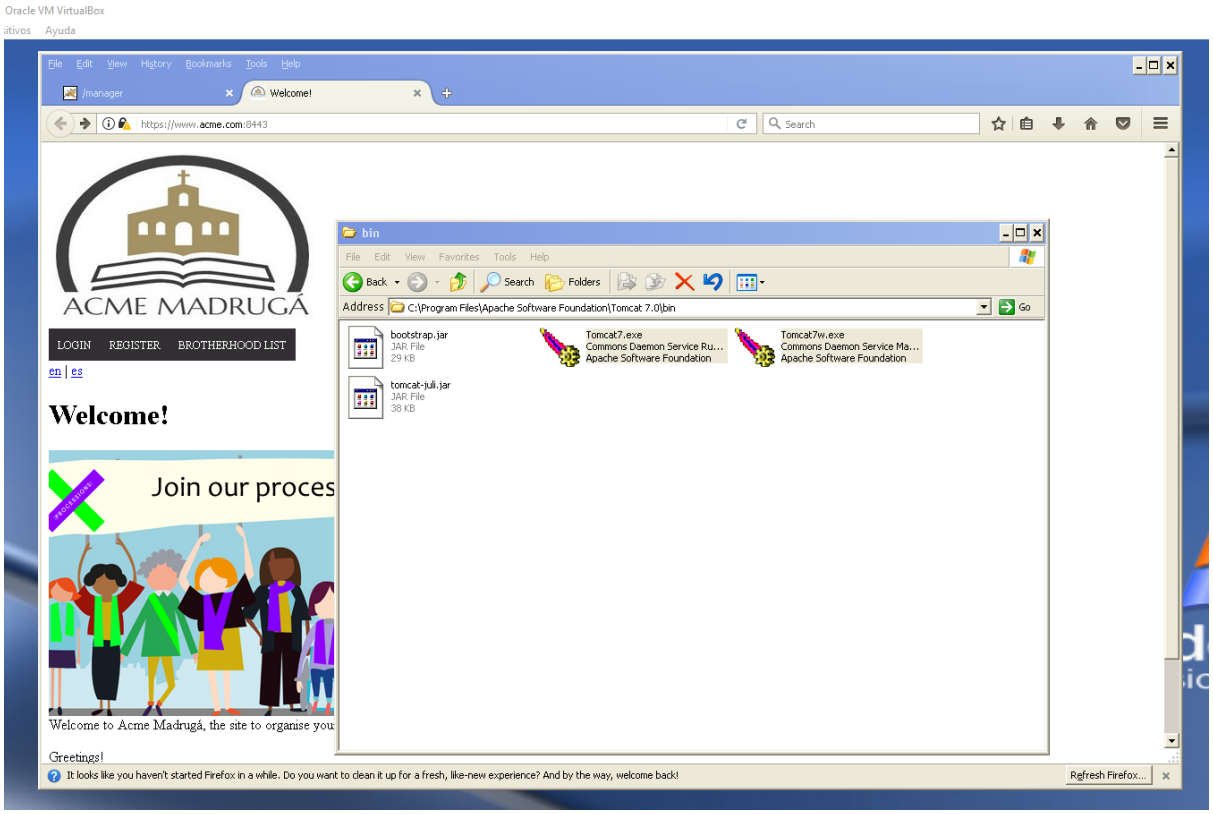
This file is practically the same file we modified in the developer machine but now we need to uncomment and additional line. Make sure you add the parameters keystore and keypass to the connector port like this:

server.xml - Notepad

```
File  Edit  Format  View  Help
      Documentation at /docs/config/service.html
  -->
  <Service name="Catalina">

    <!--The connectors can use a shared executor, you can define one or more named thread pools-->
    <!--
    <Executor name="tomcatThreadPool" namePrefix="catalina-exec-"
        maxThreads="150" minSpareThreads="4"/>
    -->


    <!-- A "Connector" represents an endpoint by which requests are received
         and responses are returned. Documentation at :
         Java HTTP Connector: /docs/config/http.html (blocking & non-blocking)
         Java AJP  Connector: /docs/config/ajp.html
         APR (HTTP/AJP) Connector: /docs/apr.html
         Define a non-SSL HTTP/1.1 Connector on port 80
    -->
    <Connector port="80" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443" />

    <Connector executor="tomcatThreadPool"
               port="80" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443" />

    <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
               maxThreads="150" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS"
                keystoreFile="C:\Documents and Settings\Boss\.keystore" keystorePass="$3cUr3=COmM$" />


    <!-- Define an AJP 1.3 Connector on port 8009 -->
    <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

```
<Connector executor="tomcatThreadPool"
        port="80" protocol="HTTP/1.1"
        connectionTimeout="20000"
        redirectPort="8443" />

<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
        maxThreads="150" scheme="https" secure="true"
        clientAuth="false" sslProtocol="TLS"
        keystoreFile="C:\Documents and Settings\Boss\.keystore"
    keystorePass="$3cUr3=C0mM$" />
```

Now we need to restart Tomcat. Go to C:\Program Files\Apache Software Foundation\Tomcat 7.0\bin and execute TomCat7w.exe and Tomcat7.exe , in this order, to restart the server.



Create the database and deploy the war like always and open www.acme.com in the browser, it will change automatically to https://www.acme.com:8443/ allowing us to use https.