Entregable D08 – Lessons learnt:

Item 6: Protocolo HTTPS

Jorge David Cabrera Cruz – José Manuel Navarro Márquez – Aurora Gómez Medina – Jorge Ramos Rivas – Juan Antonio Castañeda Cortázar

07/03/2017

En primer lugar hemos configurado el entorno de Pre-production. Tras ello, para estar seguros que nuestro proyecto funciona correctamente, lo que hemos hecho ha sido introducir en el navegador la siguiente dirección:

https://www.acme.com

Luego vemos que se muestra la página haciendo uso del protocolo que se nos especifica en el ítem, el protocolo HTTPS. Según el navegador que estemos utilizando, se nos va a preguntar por un certificado. Un ejemplo es Google Chrome. No obstante esta petición se puede ignorar.

Con el fin de hacer uso de este protocolo, se deben de configurar varios archivos y seguir en el entorno de Pre-production una serie de pasos que especificamos a continuación.

1º Paso

Creamos el archivo .keystore utilizando Java. Para poder realizar esto debemos de abrir la consola de Windows e introducir los siguientes comandos:

> **cd %JAVA_HOME%/bin**, JAVA_HOME en nuestro caso está ubicado en la siguiente dirección:
>keytool –genkey –alias tomcat –keyalg RSA

2º Paso

Posteriormente, en la consola se nos muestra una serie de preguntas, las cuales debemos de responder y confirmarlas introduciendo un 'y'.

Enter keystore password: changeit
Re-enter new password: changeit
What is your first and last name?
[Unknown]: Jorge D. Cabrera Cruz
What is the name of your organizational unit?
[Unknown]: Universidad de Sevilla
What is the name of your organization?
[Unknown]: US
What is the name of your City or Locality?
[Unknown]: Sevilla
What is the name of your State or Province?
[Unknown]: SE
What is the two-letter country code for this unit?
[Unknown]: ES
Is CN= Jorge D. Cabrera Cruz, OU= Universidad de Sevilla, O= US
, L= Sevilla, ST=SP, C=ES correct?
[no]: y

3º Paso

A continuación, se nos pide una contraseña. Con la finalidad de que NO tengamos confusiones ponemos la misma contraseña en todos los campos que nos la pidan. La contraseña que trae por defecto tomcat es: 'changeit'

Enter key password for
(RETURN if same as keystore password): changeit
Re-enter new password: changeit

4º Paso

Como podemos observar ya se nos ha creado el fichero .keystore. Este fichero por defecto se crea en Windows, en la ruta C:\Documents and Settings\Boss

5º Paso

Posteriormente, lo que hacemos es cambiar la configuración del Tomcat para realizar la configuración SSL, lo cual es indispensable para que podamos hacer uso del protocolo HTTPS. Para ello modificamos el fichero server.xml, eliminamos las líneas:

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

Y añadimos las siguientes líneas:

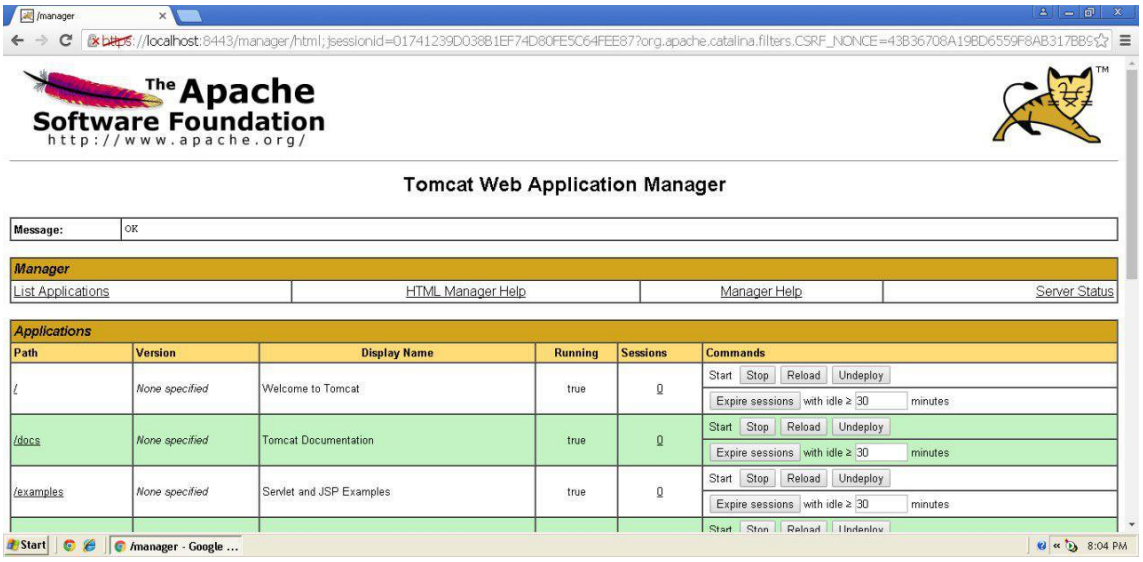
```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
        SSLEnabled="true"
        maxThreads="150" scheme="https" secure="true"
        disableUploadTimeout="true"
        clientAuth="false" sslProtocol="TLS" enableLookups="false"
        acceptCount="100"
        keystoreFile="C:\Documents and Settings\Boss\.keystore"
        keystorePass="changeit"/>
```

6º Paso

Para comprobar que lo que hemos modificado anteriormente funciona, detenemos el Servidor Tomcat y lo volvemos a arrancar.

A continuación abrimos el navegador, y escribimos:

https://localhost:8443/manager



También podemos comprobar que la siguiente URL ha dejado de funcionar:

http://localhost/manager

7º Paso

El penúltimo paso es utilizar el protocolo HTTPS en nuestra aplicación. Para utilizarlo vamos a modificar el archivo web.xml del Servidor Tomcat.

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

HTTPS y CONFIDENTIAL se utilizan para asegurarnos de que nuestra aplicación trabaja en SSL.

8º Paso

Por último, exportamos el war del proyecto, realizamos los scripts de la base de dato y lo subimos a: https://localhost:8443/manager