Boletín de ejercicios Tema 2

1. **Autenticación y autorización**

   SOLUCIÓN

   - En la máquina servidor Xubuntu, crearemos los usuarios y rol en Tomcat, añadiendo al fichero **`/var/lib/tomcat9/conf/tomcat-users.xml`** las siguientes líneas:

```
<role rolename="usuarios-servlet"/>
<user username="usuario1" password="contrasenha" roles="usuarios-servlet"/>
<user username="usuario2" password="contrasenha" roles="usuarios-servlet"/>
```

   - Reiniciamos el servidor Tomcat:

```
sudo service tomcat9 restart
```

   - En la máquina donde hayamos instalado Netbeans, importaremos la carpeta del proyecto Servlet Formulario.
   - Configuramos el Realm, para eso, dentro de este proyecto, creamos el fichero `META-INF/context.xml`, haciendo clic derecho sobre `Web Content/META-INF` y escogiendo New...→ File y escribimos las siguientes líneas:

```
<Context>
  <Realm className="org.apache.catalina.realm.MemoryRealm"/>
</Context>
```

- Protegemos la aplicación con el MemoryRealm, empleando autenticación BASIC, para lo cual editaremos el descriptor de despliegue de la aplicación web (web.xml) añadiendo los siguientes elementos como hijos del elemento raíz `<web-app>`.

```
<security-constraint>
    <web-resource-collection>
        <web-resource-name>Servlet Factorial</web-resource-name>
        <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
        <role-name>usuarios-servlet</role-name>
    </auth-constraint>
</security-constraint>
<login-config>
    <auth-method>BASIC</auth-method>
    <realm-name>Acceso al factorial</realm-name>
</login-config>
```

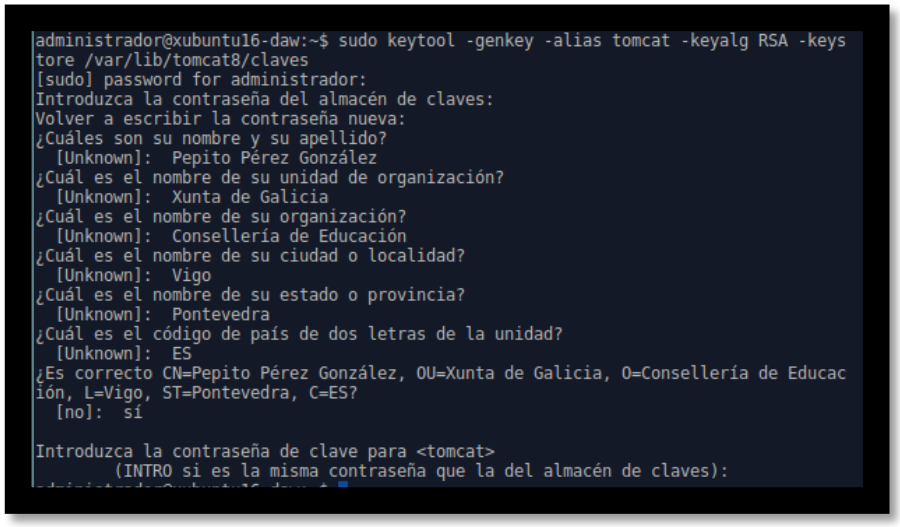
- Eliminamos la aplicación del servidor Tomcat (si ya la habíamos desplegado anteriormente), creamos el fichero WAR y la volvemos a desplegar.
- Comprobamos que la configuración fue la adecuada, accediendo desde el navegador de la máquina cliente a `http://192.168.0.1:8080/Factorial`. Comprobamos que es necesario introducir el usuario y contraseña para acceder a la aplicación.

2. Despliegue de aplicaciones web asegurando las comunicaciones entre cliente y servidor

SOLUCIÓN

- Crearemos un almacén de claves con un certificado SSL, utilizando el siguiente comando:

```
sudo keytool -genkey -alias tomcat -keyalg  RSA -keystore /var/lib/tomcat9/claves
```



- Configuramos un conector SSL en Tomcat, editando el fichero /var/lib/tomcat8/conf/server.xml y añadiendo las siguientes líneas dentro del elemento raíz `<Server>`:

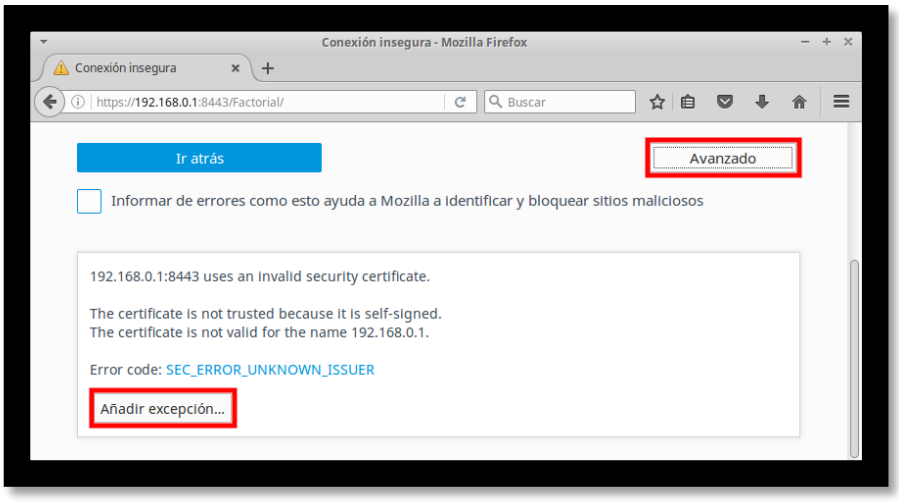
```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="/var/lib/tomcat8/almacen_claves"
keystorePass="tomcat"
keyAlias="tomcat" keyPass="tomcat"/>
```

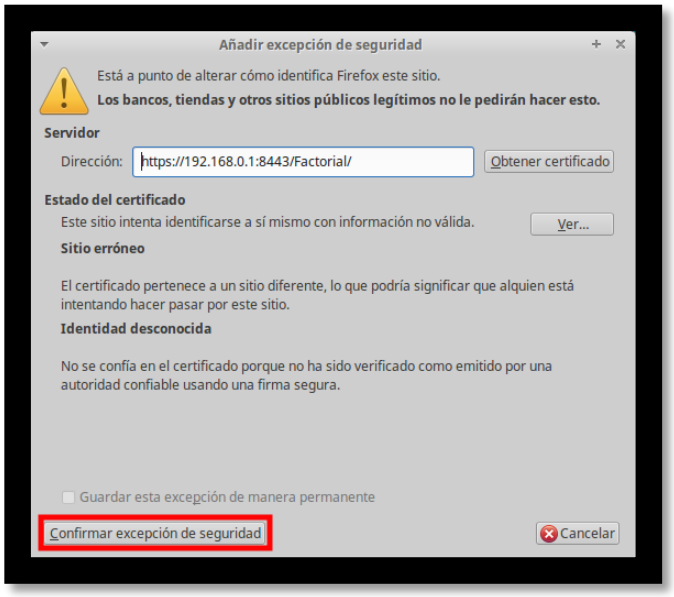
- Reiniciamos el servidor Tomcat:

```
sudo service tomcat9 restart
```

Comprobamos que la configuración fue la adecuada, accediendo desde el navegador de la máquina cliente a `https://192.168.0.1:8443/Factorial`. Donde se nos indicará que la configuración no es la correcta, ya que el certificado está firmado por sí mismo.

- Añadimos una excepción y ya podemos acceder.





- Comprobamos que si tratamos de acceder sin SSL también podemos http://192.168.0.1:8080/Factorial/

- Configuramos la aplicación para que solo acepte conexiones HTTPS, añadiendo en el descriptor de despliegue modificado en la tarea anterior los siguientes elementos, como hijos de `<security-constraint>`:

```
<user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
```

- Y desde el navegador comprobamos ahora que, si tratamos de acceder mediante el protocolo HTTP, obtenemos un error.

3. Valves

SOLUCIÓN

- En la máquina donde hayamos instalado Netbeans, importaremos la carpeta del proyecto Servlet Formulario.

- Configuramos la Valve. Para eso, dentro de este proyecto, creamos el fichero `META-INF/context.xml`, haciendo clic derecho sobre `Web Content/META- INF` y escogiendo New...→ File y escribimos las siguientes líneas:

```
<Context>
    <Valve className="org.apache.catalina.valves.RemoteAddrValve"
    allow="192.168.0.3"/>
</Context>
```

- Eliminamos la aplicación del servidor Tomcat (si ya la habíamos desplegado anteriormente), creamos el fichero WAR y la volvemos a desplegar empleando el método que nos resulte más cómodo (Tomcat Manager, Ant o despliegue manual).
- Comprobamos que la configuración fue la adecuada, accediendo desde el navegador de la máquina cliente a `http://192.168.0.1:8080/Factorial` y comprobamos que podemos acceder. Accedemos desde otra máquina, por ejemplo, desde la máquina Windows 7 y comprobamos que no se permite el acceso (error 403).

4. **Crea una Valve para todo el servidor Tomcat de Ubuntu que sólo permita acceder al ordenador cliente.**

- Modificamos el fichero "/etc/tomcat7/server.xml"
- Dentro de la etiqueta <Engine> añadimos:

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve" allow="192.168.0.3"/>
```

- Reiniciamos el Tomcat
- Accedemos a la siguiente dirección y vemos que nos permite acceder.

```
http://192.168.0.3:8080
```

- Accedemos desde cualquier otro equipo y comprobamos que no podemos acceder.

5. **Crea una Valve para todo el servidor Tomcat de Ubuntu que NO permita acceder al ordenador cliente.**

- Modificamos el fichero "/etc/tomcat7/server.xml"
- Dentro de la etiqueta <Engine> añadimos:

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve" deny="192.168.0.3"/>
```

- Reiniciamos el Tomcat
- Accedemos a la siguiente dirección y vemos que NO nos permite acceder.

```
http://192.168.0.3:8080
```

- Accedemos desde cualquier otro equipo y comprobamos que SÍ podemos acceder.

6. **Para el ejercicio 1 configura:**
   a. **Un Valve que permita acceder solamente al ordenador cliente**

- Editamos o creamos el archivo context.xml en el directorio web/META-INF y añadimos:

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve" allow="192.168.0.3"/>
```

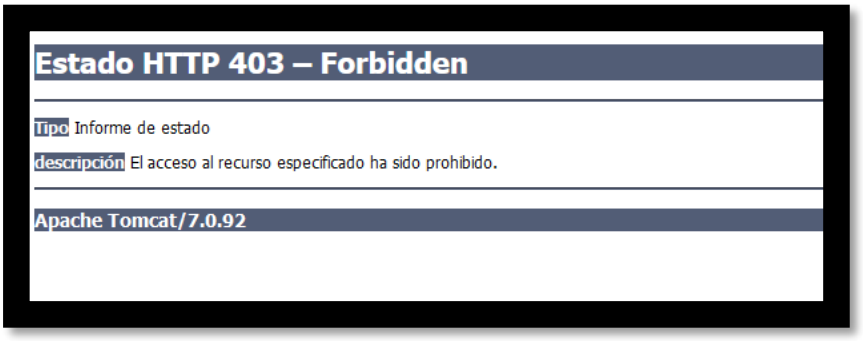
- Desplegamos la aplicación http://192.168.0.3:8080/Ejercicio6

b. Un Valve que impida el acceso al ordenador cliente

- Editamos o creamos el archivo context.xml en el directorio web/META-INF y añadimos:

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve" deny="192.168.0.3"/>
```

- Desplegamos la aplicación http://192.168.0.3:8080/Ejercicio6


Estado HTTP 403 – Forbidden
Tipo Informe de estado
descripción El acceso al recurso especificado ha sido prohibido.
Apache Tomcat/7.0.92