

# TIENDA DE COMERCIO ELECTRÓNICO

## ITERACIÓN 04 – SEGURIDAD CON JAAS (Java Authentication and Authorization Service)

Autor: Mag. Juan Antonio Castro Silva  
Versión: 2.5 Enero 29 de 2020 (20200129T0619)

Java Authentication and Authorization Service, o JAAS, pronunciado como "Jazz", es una Interfaz de Programación de Aplicaciones (API) que permite a las aplicaciones Java acceder a servicios de control de autenticación y acceso [1].

### 1. ENCRIPtar LAS CLAVES

Para activar la librería pgcrypto en el motor de base de datos PostgreSQL, seleccione la base de datos [ecommerce] y ejecute el siguiente comando en la ventana de SQL.

```
001 CREATE EXTENSION pgcrypto;
```

Para encriptar una clave con el algoritmo md5 y mostrar el resultado con el encode base64:

```
001 SELECT encode(digest('clave_a_encriptar', 'md5'), 'base64');
```

Actualizamos las claves de los usuarios:

```
001 UPDATE users set password = encode(digest('pgutierrez2018', 'md5'), 'base64') where
002 username = 'pedro';
003 UPDATE users set password = encode(digest('mquintero2018', 'md5'), 'base64') where
004 username = 'maria';
005 UPDATE users set password = encode(digest('jlopez2018', 'md5'), 'base64') where
006 username = 'jose';
```

Para ver las claves encriptadas, ejecute una sentencia SELECT.

```
001 SELECT * from users;
```

En la columna a la derecha podemos ver el campo password con las claves encriptadas.

2	1	0	jose	jose.lopez@gmail.com	o0i2zmb0n1h/a4ev0Z10fw==
3	2	0	maria	maria.quintero@gmail.com	ICD0TdR2VeZNVGhxiKxaFw==
4	3	0	pedro	pedro.autierrez@gmail.com	ArYun2FnNK48rMrlzd1LX0==

## 2. CREAR LAS TABLAS

Para crear las tablas (profiles y user\_profiles) ejecute las siguientes sentencias en el editor de SQL:

### Tabla profiles:

```
001 CREATE TABLE public.profiles
002 (
003     id serial NOT NULL,
004     name character varying(100),
005     profile character varying(100),
006     CONSTRAINT group_pkey PRIMARY KEY (id)
007 )
008 WITH (
009     OIDS=FALSE
010 );
011 ALTER TABLE public.profiles
012     OWNER TO ecommerce;
013 GRANT ALL ON TABLE public.profiles TO ecommerce;
```

### Tabla user\_profiles:

```
001 CREATE TABLE public.user_profiles
002 (
003     id bigserial NOT NULL,
004     user_id bigint,
005     profile_id bigint,
006     CONSTRAINT user_profiles_pkey PRIMARY KEY (id),
007     CONSTRAINT user_profiles_profile_fkey FOREIGN KEY (profile_id)
008         REFERENCES public.profiles (id) MATCH SIMPLE
009         ON UPDATE NO ACTION ON DELETE NO ACTION,
010     CONSTRAINT user_profiles_user_fkey FOREIGN KEY (user_id)
011         REFERENCES public.users (id) MATCH SIMPLE
012         ON UPDATE NO ACTION ON DELETE NO ACTION
013 )
014 WITH (
015     OIDS=FALSE
016 );
017 ALTER TABLE public.user_profiles
018     OWNER TO ecommerce;
019 GRANT ALL ON TABLE public.user_profiles TO ecommerce;
```

Alimentar la base de datos

### Tabla profiles:

```
001 insert into profiles (name, profile) values ('Administrador', 'ADMINISTRATOR');
002 insert into profiles (name, profile) values ('Cliente', 'CLIENT');
```

### Tabla user\_profiles:

```
001 insert into user_profiles (user_id, profile_id) values
002 (1,1),
003 (2,2),
004 (3,1),
005 (3,2);
```

### 3. ASIGNAR PERMISOS

Para asignar los permisos de acceso a las tablas, ejecute el comando GRANT.

```
001 GRANT SELECT, UPDATE, INSERT, DELETE ON TABLE public.users TO ecommerce_admin;
002 GRANT SELECT, UPDATE, INSERT, DELETE ON TABLE public.profiles TO ecommerce_admin;
003 GRANT SELECT, UPDATE, INSERT, DELETE ON TABLE public.user_profiles TO ecommerce_admin;
004 GRANT USAGE, SELECT ON ALL SEQUENCES IN SCHEMA public TO ecommerce_admin;
```

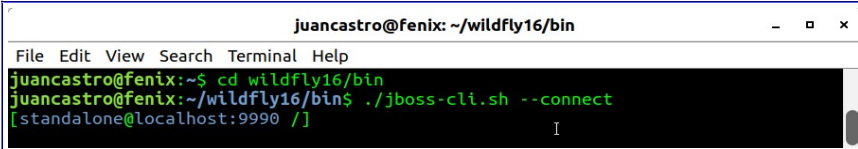
### 4. INSTALAR EL DRIVER JDBC

Abra una ventana de terminal e ingrese al folder donde descargo el driver JDBC. Cree la carpeta /opt/drivers y mueva el driver postgresql-42.2.5.jar al folder /opt/drivers/.

```
001 sudo mkdir /opt/drivers
002 sudo mv postgresql-42.2.5.jar /opt/drivers/
```

Para instalar el driver JDBC descargado, haga correr el servidor de aplicaciones Wildfly, abra una ventana de terminal y vaya a la carpeta wildfly/bin. Para acceder a la interface de la linea de comandos (CLI) digite la siguiente instrucción.

```
001 cd wildfly/bin
002 ./jboss-cli.sh --connect
```



```
juancastro@fenix: ~/wildfly16/bin
File Edit View Search Terminal Help
juancastro@fenix:~$ cd wildfly16/bin
juancastro@fenix:~/wildfly16/bin$ ./jboss-cli.sh --connect
[standalone@localhost:9990 /]
```

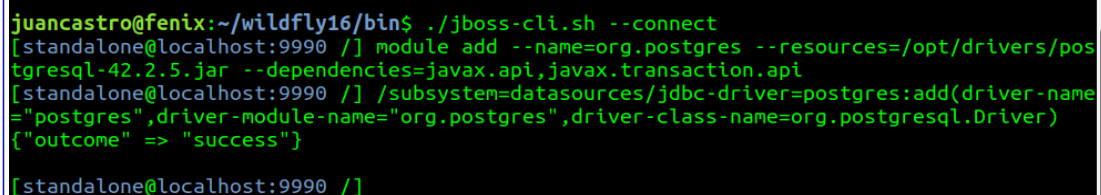
Ahora que esta conectado a la linea de comandos, adicione un modulo a Wildfly el cual apuntará al archivo jar descargado.

```
001 module add --name=org.postgres --resources=/opt/drivers/postgresql-42.2.5.jar --
dependencies=javax.api,javax.transaction.api
```

Para finalizar, instale el driver en Wildfly.

```
001 /subsystem=datasources/jdbc-driver=postgres:add(driver-name="postgres",driver-module-
name="org.postgres",driver-class-name=org.postgresql.Driver)
```

Si todo salio bien debería ver un mensaje de éxito {"outcome"=>"success"}:

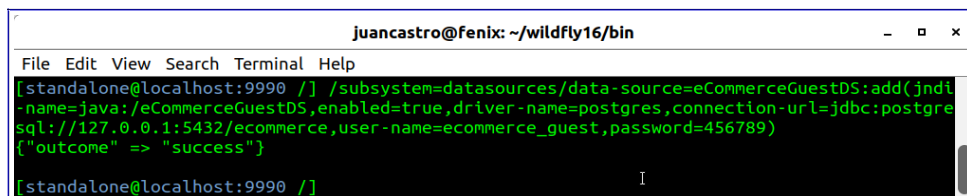


```
juancastro@fenix:~/wildfly16/bin$ ./jboss-cli.sh --connect
[standalone@localhost:9990 /] module add --name=org.postgres --resources=/opt/drivers/postgresql-42.2.5.jar --dependencies=javax.api,javax.transaction.api
[standalone@localhost:9990 /] /subsystem=datasources/jdbc-driver=postgres:add(driver-name="postgres",driver-module-name="org.postgres",driver-class-name=org.postgresql.Driver)
{"outcome" => "success"}
[standalone@localhost:9990 /]
```

## 5. CREAR LOS DATASOURCES (Fuentes de Datos)

### DataSource eCommerceGuestDS:

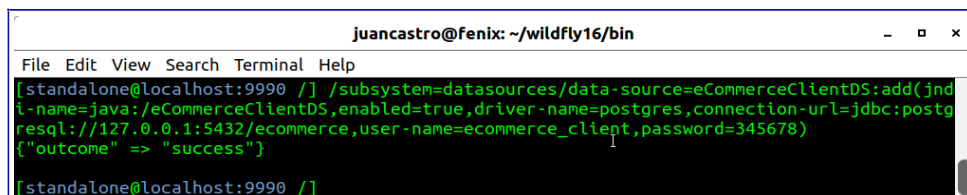
```
001 /subsystem=datasources/data-source=eCommerceGuestDS:add(jndi-name=java:/eCommerceGuestDS,enabled=true,driver-name=postgres,connection-url=jdbc:postgresql://127.0.0.1:5432/ecommerce,user-name=ecommerce_guest,password=456789)
```



```
juancastro@fenix: ~/wildfly16/bin
File Edit View Search Terminal Help
[standalone@localhost:9990 /] /subsystem=datasources/data-source=eCommerceGuestDS:add(jndi-name=java:/eCommerceGuestDS,enabled=true,driver-name=postgres,connection-url=jdbc:postgresql://127.0.0.1:5432/ecommerce,user-name=ecommerce_guest,password=456789)
{"outcome" => "success"}
[standalone@localhost:9990 /]
```

### DataSource eCommerceClientDS:

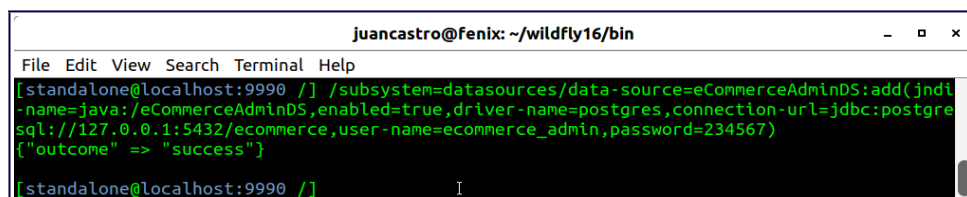
```
001 /subsystem=datasources/data-source=eCommerceClientDS:add(jndi-name=java:/eCommerceClientDS,enabled=true,driver-name=postgres,connection-url=jdbc:postgresql://127.0.0.1:5432/ecommerce,user-name=ecommerce_client,password=345678)
```



```
juancastro@fenix: ~/wildfly16/bin
File Edit View Search Terminal Help
[standalone@localhost:9990 /] /subsystem=datasources/data-source=eCommerceClientDS:add(jndi-name=java:/eCommerceClientDS,enabled=true,driver-name=postgres,connection-url=jdbc:postgresql://127.0.0.1:5432/ecommerce,user-name=ecommerce_client,password=345678)
{"outcome" => "success"}
[standalone@localhost:9990 /]
```

### DataSource eCommerceAdminDS:

```
001 /subsystem=datasources/data-source=eCommerceAdminDS:add(jndi-name=java:/eCommerceAdminDS,enabled=true,driver-name=postgres,connection-url=jdbc:postgresql://127.0.0.1:5432/ecommerce,user-name=ecommerce_admin,password=234567)
```



```
juancastro@fenix: ~/wildfly16/bin
File Edit View Search Terminal Help
[standalone@localhost:9990 /] /subsystem=datasources/data-source=eCommerceAdminDS:add(jndi-name=java:/eCommerceAdminDS,enabled=true,driver-name=postgres,connection-url=jdbc:postgresql://127.0.0.1:5432/ecommerce,user-name=ecommerce_admin,password=234567)
{"outcome" => "success"}
[standalone@localhost:9990 /]
```

En el archivo de configuración del servidor de aplicaciones wildfly (wildfly\_path/standalone/configuration/standalone.xml) quedan registrados los cambios realizados en la línea de comandos (CLI):

```
--- ESTO SE MUESTRA SOLO PARA COMPARAR EN CASO DE ERROR ---

<subsystem xmlns="urn:jboss:domain:datasources:5.0">
  <datasources>
    <datasource jndi-name="java:jboss/datasources/ExampleDS" pool-name="ExampleDS"
enabled="true" use-java-context="true" statistics-enabled="{wildfly.datasources.statistics-enabled:$
{wildfly.statistics-enabled:false}}">
      <connection-url>jdbc:h2:mem:test;DB_CLOSE_DELAY=-1;DB_CLOSE_ON_EXIT=FALSE</connection-url>
      <driver>h2</driver>
      <security>
        <user-name>sa</user-name>
        <password>sa</password>
      </security>
    </datasource>

    <datasource jndi-name="java:/eCommerceGuestDS" pool-name="eCommerceGuestDS" enabled="true">
      <connection-url>jdbc:postgresql://127.0.0.1:5432/ecommerce</connection-url>
      <driver>postgres</driver>
      <security>
        <user-name>ecommerce_guest</user-name>
        <password>456789</password>
      </security>
    </datasource>

    <datasource jndi-name="java:/eCommerceClientDS" pool-name="eCommerceClientDS" enabled="true">
      <connection-url>jdbc:postgresql://127.0.0.1:5432/ecommerce</connection-url>
      <driver>postgres</driver>
      <security>
        <user-name>ecommerce_client</user-name>
        <password>345678</password>
      </security>
    </datasource>

    <datasource jndi-name="java:/eCommerceAdminDS" pool-name="eCommerceAdminDS" enabled="true">
      <connection-url>jdbc:postgresql://127.0.0.1:5432/ecommerce</connection-url>
      <driver>postgres</driver>
      <security>
        <user-name>ecommerce_admin</user-name>
        <password>234567</password>
      </security>
    </datasource>

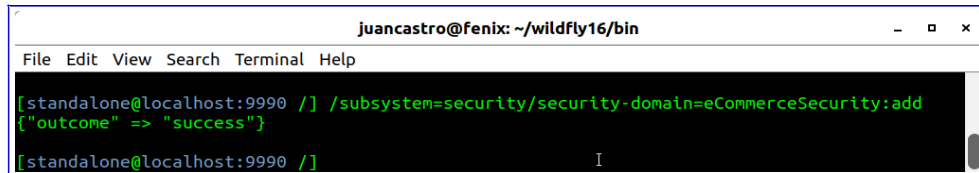
    <drivers>
      <driver name="h2" module="com.h2database.h2">
        <xa-datasource-class>org.h2.jdbcx.JdbcDataSource</xa-datasource-class>
      </driver>
      <driver name="postgres" module="org.postgres">
        <driver-class>org.postgresql.Driver</driver-class>
      </driver>
    </drivers>
  </datasources>
</subsystem>

...
```

## 6. CREAR EL DOMINIO DE SEGURIDAD (SECURITY DOMAIN)

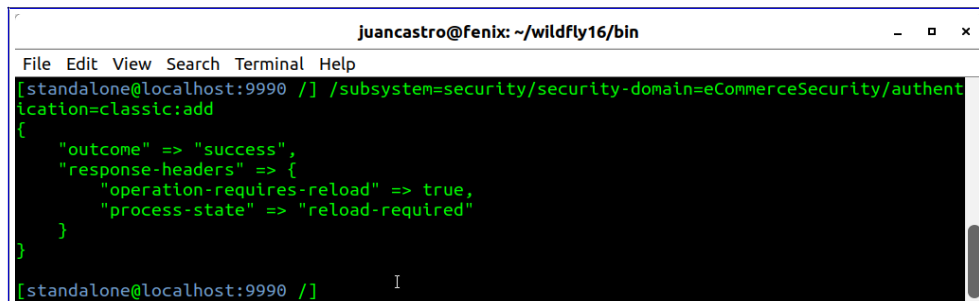
Para crear el dominio de seguridad (Security Domain) ejecute las siguientes instrucciones en la Interfaz de la Línea de Comandos (CLI).

```
001 /subsystem=security/security-domain=eCommerceSecurity:add
```



```
juancastro@fenix: ~/wildfly16/bin
File Edit View Search Terminal Help
[standalone@localhost:9990 /] /subsystem=security/security-domain=eCommerceSecurity:add
{"outcome" => "success"}
[standalone@localhost:9990 /]
```

```
001 /subsystem=security/security-domain=eCommerceSecurity/authentication=classic:add
```



```
juancastro@fenix: ~/wildfly16/bin
File Edit View Search Terminal Help
[standalone@localhost:9990 /] /subsystem=security/security-domain=eCommerceSecurity/authentication=classic:add
{
  "outcome" => "success",
  "response-headers" => {
    "operation-requires-reload" => true,
    "process-state" => "reload-required"
  }
}
[standalone@localhost:9990 /]
```

Crear el mecanismo de seguridad.

```
001 /subsystem=security/security-domain=eCommerceSecurity/authentication=classic/login-
module=Database:add(code=Database,flag=required,module-options=[("dsJndiName"=>"java:/
eCommerceAdminDS"),("principalsQuery"=>"SELECT password FROM users WHERE username=?"),
("rolesQuery"=>"SELECT profiles.profile, 'Roles' FROM users, user_profiles, profiles
WHERE users.id = user_profiles.user_id AND profiles.id = user_profiles.profile_id AND
username=?"),("hashAlgorithm"=>"MD5"),("hashEncoding"=>"base64")])
```

```
juancastro@fenix: ~/wildfly16/bin
File Edit View Search Terminal Help
[standalone@localhost:9990 /] /subsystem=security/security-domain=eCommerceSecurity/authent
ication=classic/login-module=Database:add( \
>   code=Database, \
>   flag=required, \
>   module-options=[ \
>     ("principalsQuery"=>"SELECT password FROM users WHERE username=?"), \
>     ("rolesQuery"=>"SELECT profiles.profile, 'Roles' FROM users,
> user_profiles, profiles
> WHERE users.id = user_profiles.user_id
> AND profiles.id = user_profiles.profile_id
> AND username=?"), \
>     ("hashAlgorithm"=>"MD5"), \
>     ("hashEncoding"=>"base64") \
>   ])
{
  "outcome" => "success",
  "response-headers" => {
    "operation-requires-reload" => true,
    "process-state" => "reload-required"
  }
}
[standalone@localhost:9990 /]
```

Para finalizar debe recargar (reload) la Interfaz de la Linea a de Comandos (CLI).

001	reload
-----	--------

```
juancastro@fenix: ~/wildfly16/bin
File Edit View Search Terminal Help
[standalone@localhost:9990 /] reload
[standalone@localhost:9990 /]
```

Los cambios realizados se registran en el subsistema de seguridad del archivo de configuración de servidor de aplicaciones wildfly.

```
--- ESTO SE MUESTRA SOLO PARA COMPARAR EN CASO DE ERROR ---

<subsystem xmlns="urn:jboss:domain:security:2.0">
  <security-domains>
    <security-domain name="other" cache-type="default">
      <authentication>
        <login-module code="Remoting" flag="optional">
          <module-option name="password-stacking" value="useFirstPass"/>
        </login-module>
        <login-module code="RealmDirect" flag="required">
          <module-option name="password-stacking" value="useFirstPass"/>
        </login-module>
      </authentication>
    </security-domain>

    <security-domain name="jboss-web-policy" cache-type="default">
      <authorization>
        <policy-module code="Delegating" flag="required"/>
      </authorization>
    </security-domain>

    <security-domain name="jaspitest" cache-type="default">
      <authentication-jaspi>
        <login-module-stack name="dummy">
          <login-module code="Dummy" flag="optional"/>
        </login-module-stack>
        <auth-module code="Dummy"/>
      </authentication-jaspi>
    </security-domain>

    <security-domain name="jboss-ejb-policy" cache-type="default">
      <authorization>
        <policy-module code="Delegating" flag="required"/>
      </authorization>
    </security-domain>

    <security-domain name="eCommerceSecurity">
      <authentication>
        <login-module code="Database" flag="required">
          <module-option name="dsJndiName" value="java:/eCommerceAdminDS"/>
          <module-option name="principalsQuery" value="SELECT password FROM users
WHERE username=?"/>
          <module-option name="rolesQuery" value="SELECT profiles.profile,
'Roles' FROM users, user_profiles, profiles WHERE users.id = user_profiles.user_id AND
profiles.id = user_profiles.profile_id AND username=?"/>
          <module-option name="hashAlgorithm" value="MD5"/>
          <module-option name="hashEncoding" value="base64"/>
        </login-module>
      </authentication>
    </security-domain>

  </security-domains>
</subsystem>
...
```



## 7. APLICACIÓN WEB

Cambios en el código fuente.

### Archivo org.software.util.Database.java

```
001 package org.software.util;
002
003 import java.sql.Connection;
004 import java.sql.DriverManager;
005 import java.sql.PreparedStatement;
006 import java.sql.ResultSet;
007 import java.sql.SQLException;
008 import java.sql.Statement;
009
010 import javax.naming.InitialContext;
011 import javax.sql.DataSource;
012
013 public class DataBase {
014     public Connection getConnection(String profile) {
015         Connection connection = null;
016
017         /*
018         String driver = "org.postgresql.Driver";
019         String url = "jdbc:postgresql://localhost:5432/ecommerce";
020         String user = "";
021         String password = "";
022         */
023
024         String JndiDataSourceName = "";
025
026         if (profile.equals("admin")) {
027             JndiDataSourceName = "eCommerceAdminDS";
028             //user = "ecommerce_admin";
029             //password = "234567";
030         }
031         if (profile.equals("client")) {
032             JndiDataSourceName = "eCommerceClientDS";
033             //user = "ecommerce_client";
034             //password = "345678";
035         }
036         if (profile.equals("guest")) {
037             JndiDataSourceName = "eCommerceGuestDS";
038             //user = "ecommerce_guest";
039             //password = "456789";
040         }
041
042         try {
043             InitialContext ctx = new InitialContext();
044             DataSource ds = (DataSource)ctx.lookup(JndiDataSourceName);
045             connection = ds.getConnection();
046
047             //Class.forName(driver);
048             //connection = DriverManager.getConnection(url, user, password);
049         } catch (Exception e) {
050             System.out.println("Error: " + e.toString());
051         }
052
053         return connection;
054     }
055 }
```

```

054
055     public void closeObject(Connection connection) {
056         try {
057             connection.close();
058         } catch (SQLException e) {
059             e.printStackTrace();
060         }
061     }
062
063     public void closeObject(PreparedStatement preparedStatement) {
064         try {
065             preparedStatement.close();
066         } catch (SQLException e) {
067             e.printStackTrace();
068         }
069     }
070
071     public void closeObject(Statement statement) {
072         try {
073             statement.close();
074         } catch (SQLException e) {
075             e.printStackTrace();
076         }
077     }
078
079     public void closeObject(ResultSet resultSet) {
080         try {
081             resultSet.close();
082         } catch (SQLException e) {
083             e.printStackTrace();
084         }
085     }
086 }

```

### Archivo org.software.util/Logout.java:

```

001 package org.software.util;
002
003 import java.io.IOException;
004 import javax.servlet.ServletException;
005 import javax.servlet.annotation.WebServlet;
006 import javax.servlet.http.HttpServlet;
007 import javax.servlet.http.HttpServletRequest;
008 import javax.servlet.http.HttpServletResponse;
009 import javax.servlet.http.HttpSession;
010
011 /**
012  * Servlet implementation class Logout
013  */
014 @WebServlet("/Logout")
015 public class Logout extends HttpServlet {
016     private static final long serialVersionUID = 1L;
017
018     public Logout() {
019         super();
020         // TODO Auto-generated constructor stub
021     }
022
023     /**
024      * @see HttpServlet#doGet(HttpServletRequest request, HttpServletResponse

```

```

025 response)
026     */
027     protected void doGet(HttpServletRequest request, HttpServletResponse response)
028     throws ServletException, IOException {
029         HttpSession session = request.getSession();
030         session.invalidate();
031         response.sendRedirect("");
032     }
033 }

```

### Archivo portal/products.jsp:

```

001 <div class="row">
002     <div class="col-lg-4 col-md-6 mb-4">
003         <div class="card h-100">
004             <a href="#"></a>
006             <div class="card-body">
007                 <h4 class="card-title">
008                     <a href="#">Item One</a>
009                 </h4>
010                 <h5>$24.99</h5>
011                 <p class="card-text">Lorem ipsum dolor sit amet, consectetur
012                     adipisicing elit. Amet numquam aspernatur!</p>
013             </div>
014             <div class="card-footer">
015                 <small class="text-muted">&#9733; &#9733; &#9733; &#9733;
016                     &#9734;</small>
017             </div>
018         </div>
019     </div>
020 </div>
021 <!-- /.row -->

```

### Archivo portal/menu.jsp:

```

001 <%
002     response.sendRedirect("home/");
003 %>
004 <%
005     String username = "";
006     try{
007         username = request.getUserPrincipal().getName();
008     }catch(Exception e){
009         username = "";
010     }
011 %>
012 <nav class="navbar navbar-expand-lg navbar-dark bg-dark fixed-top">
013     <div class="container">
014         <a class="navbar-brand" href="#">Start Bootstrap</a>
015         <button class="navbar-toggler" type="button" data-toggle="collapse"
016             data-target="#navbarResponsive" aria-controls="navbarResponsive"
017             aria-expanded="false" aria-label="Toggle navigation">
018             <span class="navbar-toggler-icon"></span>
019         </button>
020         <div class="collapse navbar-collapse" id="navbarResponsive">
021             <ul class="navbar-nav ml-auto">
022                 <li class="nav-item active">
023                     <a class="nav-link" href="..">
024                         Home<span class="sr-only">(current)</span>
025                     </a>

```

```

026         </li>
027         <li class="nav-item"><a class="nav-link" href="#">About</a></li>
028         <li class="nav-item">
029             <a class="nav-link" href=" ../order">Orders</a></li>
030         <li class="nav-item">
031             <a class="nav-link" href=" ../category">Category</a></li>
032         <li class="nav-item"><a class="nav-link" href="#">Contact</a></li>
033         <%
034             if (username.length() == 0) {
035             %>
036             <li class="nav-item">
037                 <a class="nav-link" href=" ../user">
038                     <button type="button" class="btn btn-success">Login</button>
039                 </a>
040             <%
041                 }
042             %>
043             <%
044                 if (username.length() > 0) {
045                 %>
046                 <li class="nav-item">
047                     <div class="btn-group nav-link" role="group">
048                         <button id="btnGroupDrop1" type="button"
049                             class="btn btn-primary
050                             dropdown-toggle" data-toggle="dropdown"
051                             aria-haspopup="true" aria-expanded="false">
052                             <%=username%>
053                         </button>
054                         <div class="dropdown-menu" aria-labelledby="btnGroupDrop1">
055                             <a class="dropdown-item" href=" ../user">Control Panel</a>
056                             <a class="dropdown-item" href=" ../Logout">Logout</a>
057                         </div>
058                     </div>
059                 </li>
060             <%
061                 }
062             %>
063             </ul>
064         </div>
065     </div>
066 </nav>

```

## Archivo home/index.jsp:

```
001 <%@ page language="java" contentType="text/html; charset=UTF-8"
002     pageEncoding="UTF-8"%>
003
004 <!DOCTYPE html>
005 <html lang="en">
006 <head>
007 <meta charset="utf-8">
008 <meta name="viewport"
009     content="width=device-width, initial-scale=1, shrink-to-fit=no">
010 <meta name="description" content="">
011 <meta name="author" content="">
012
013 <title>Shop Homepage - Start Bootstrap Template</title>
014
015 <!-- Bootstrap core CSS -->
016 <link rel="stylesheet"
017 href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css">
018
019 <!-- Custom styles for this template -->
020 <link href="../../css/shop-homepage.css" rel="stylesheet">
021 </head>
022
023 <body>
024     <!-- Navigation -->
025     <jsp:include page="../../portal/menu.jsp" />
026
027     <!-- Page Content -->
028     <div class="container">
029         <div class="row">
030             <div class="col-lg-3">
031                 <jsp:include page="../../portal/category.jsp" />
032             </div>
033             <!-- /.col-lg-3 -->
034
035             <div class="col-lg-9">
036                 <jsp:include page="../../portal/carousel.jsp" />
037                 <jsp:include page="../../portal/products.jsp" />
038             </div>
039             <!-- /.col-lg-9 -->
040         </div>
041         <!-- /.row -->
042
043     </div>
044     <!-- /.container -->
045
046     <!-- Footer -->
047     <jsp:include page="../../portal/footer.jsp" />
048     <!-- Bootstrap core JavaScript -->
049     <script src="https://code.jquery.com/jquery-3.3.1.js"></script>
050     <script
051 src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js"></script>
052 </body>
053 </html>
```

## Archivo order/index.jsp:

```
001 <%@ page language="java" contentType="text/html; charset=UTF-8"
002     pageEncoding="UTF-8"%>
003
004 <!DOCTYPE html>
005 <html lang="en">
006 <head>
007 <meta charset="utf-8">
008 <meta name="viewport"
009     content="width=device-width, initial-scale=1, shrink-to-fit=no">
010 <meta name="description" content="">
011 <meta name="author" content="">
012 <title>Shop Homepage - Start Bootstrap Template</title>
013 <!-- Bootstrap core CSS -->
014 <link rel="stylesheet"
015 href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css">
016
017 <!-- Custom styles for this template -->
018 <link href="../css/shop-homepage.css" rel="stylesheet">
019 </head>
020 <body>
021     <!-- Navigation -->
022     <jsp:include page="../portal/menu.jsp" />
023
024     <!-- Page Content -->
025     <div class="container">
026         <div class="row">
027             <div class="col-lg-3">
028                 <jsp:include page="../portal/category.jsp" />
029             </div>
030             <!-- /.col-lg-3 -->
031
032             <div class="col-lg-9">
033                 <br/>
034                 <br/>
035                 <div class="alert alert-primary" role="alert">
036                     Componente pedidos!
037                 </div>
038             </div>
039             <!-- /.col-lg-9 -->
040         </div>
041         <!-- /.row -->
042         <br/>
043         <br/>
044     </div>
045     <!-- /.container -->
046
047     <!-- Footer -->
048     <jsp:include page="../portal/footer.jsp" />
049     <!-- Bootstrap core JavaScript -->
050     <script src="https://code.jquery.com/jquery-3.3.1.js"></script>
051     <script
052 src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js"></script>
053 </body>
054 </html>
```

## Archivo login/login.jsp:

```
001 <%@ page language="java" contentType="text/html; charset=UTF-8"
002     pageEncoding="UTF-8"%>
003 <!doctype html>
004 <html lang="en">
005 <head>
006 <!-- Required meta tags -->
007 <meta charset="utf-8">
008 <meta name="viewport"
009     content="width=device-width, initial-scale=1, shrink-to-fit=no">
010
011 <!-- Bootstrap CSS -->
012 <link rel="stylesheet"
013 href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css">
014 <link href=" ../css/login.css" rel="stylesheet">
015 <title>eCommerce</title>
016 </head>
017 <body>
018     <!-- Navigation -->
019     <jsp:include page=" ../portal/menu.jsp"/>
020
021     <!-- Page Content -->
022     <div class="container login-container">
023         <br/>
024         <br/>
025         <div class="row">
026             <div class="col-md-3"></div>
027             <div class="col-md-6 login-form-1">
028                 <h3>Ingresar al Sistema</h3>
029                 <form action=" ../j_security_check" method="post">
030                     <div class="form-group">
031                         <input type="text" class="form-control" name="j_username"
032                             placeholder="Your Email *" value="" />
033                     </div>
034                     <div class="form-group">
035                         <input type="password" class="form-control" name="j_password"
036                             placeholder="Your Password *" value="" />
037                     </div>
038                     <div class="form-group">
039                         <input type="submit" class="btnSubmit" value="Login" />
040                     </div>
041                     <div class="form-group">
042                         <a href="#" class="ForgetPwd">Forget Password?</a>
043                     </div>
044                 </form>
045             </div>
046             <div class="col-md-3"></div>
047         </div>
048     </div>
049     <!-- /.container -->
050
051     <!-- Footer -->
052     <jsp:include page=" ../portal/footer.jsp"/>
053
054     <!-- jQuery first, then Popper.js, then Bootstrap JS -->
055     <script src="https://code.jquery.com/jquery-3.3.1.js"></script>
056     <script
057 src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js"></script>
058 </body>
059 </html>
060
```

## Archivo login/error.jsp:

```
001 <%@ page language="java" contentType="text/html; charset=UTF-8"
002     pageEncoding="UTF-8"%>
003 <!doctype html>
004 <html lang="en">
005 <head>
006 <!-- Required meta tags -->
007 <meta charset="utf-8">
008 <meta name="viewport"
009     content="width=device-width, initial-scale=1, shrink-to-fit=no">
010
011 <!-- Bootstrap CSS -->
012 <link rel="stylesheet"
013     href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css">
014 <link href="../css/login.css" rel="stylesheet">
015 <title>eCommerce</title>
016 </head>
017 <body>
018     <!-- Navigation -->
019     <jsp:include page="../portal/menu.jsp"/>
020
021     <!-- Page Content -->
022     <div class="container">
023         <br/>
024         <br/>
025         <br/>
026         <div class="row">
027             <div class="col-md-12">
028                 <h2>Error al digitar el usuario o la clave.</h2>
029                 <a class="nav-link" href="user">
030                     <button type="button" class="btn btn-danger">
031                         Volver a intentar.</button>
032                     </a>
033                 </div>
034             </div>
035         </div>
036         <br/>
037         <br/>
038         <br/>
039     </div>
040     <!-- /.container -->
041
042     <!-- Footer -->
043     <jsp:include page="../portal/footer.jsp"/>
044
045     <!-- jQuery first, then Popper.js, then Bootstrap JS -->
046     <script src="https://code.jquery.com/jquery-3.3.1.js"></script>
047     <script
048     src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js"></script>
049 </body>
050 </html>
```



## Archivo portal/forbidden.jsp:

```
001 <%@ page language="java" contentType="text/html; charset=UTF-8"
002     pageEncoding="UTF-8"%>
003 <!doctype html>
004 <html lang="en">
005 <head>
006 <!-- Required meta tags -->
007 <meta charset="utf-8">
008 <meta name="viewport"
009     content="width=device-width, initial-scale=1, shrink-to-fit=no">
010
011 <!-- Bootstrap CSS -->
012 <link rel="stylesheet"
013 href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css">
014 <link href="../css/login.css" rel="stylesheet">
015 <title>eCommerce</title>
016 </head>
017 <body>
018     <!-- Navigation -->
019     <jsp:include page="../portal/menu.jsp"/>
020
021     <!-- Page Content -->
022     <div class="container">
023         <br/>
024         <br/>
025         <br/>
026         <div class="row">
027             <div class="col-md-12">
028                 <h2>Acceso no permitido, perfil no valido.</h2>
029                 <a class="nav-link" href="..">
030                     <button type="button" class="btn btn-danger">Home</button>
031                 </a>
032             </div>
033         </div>
034         <br/>
035         <br/>
036         <br/>
037     </div>
038     <!-- /.container -->
039
040     <!-- Footer -->
041     <jsp:include page="../portal/footer.jsp"/>
042
043     <!-- jQuery first, then Popper.js, then Bootstrap JS -->
044     <script src="https://code.jquery.com/jquery-3.3.1.js"></script>
045     <script
046 src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js"></script>
047 </body>
048 </html>
```

## Archivo user/index.jsp:

```
001 <%@ page language="java" contentType="text/html; charset=UTF-8"
002     pageEncoding="UTF-8"%>
003 <!doctype html>
004 <html lang="en">
005 <head>
006 <!-- Required meta tags -->
007 <meta charset="utf-8">
008 <meta name="viewport"
009     content="width=device-width, initial-scale=1, shrink-to-fit=no">
010
011 <!-- Bootstrap CSS -->
012 <link rel="stylesheet"
013     href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css">
014
015 <title>eCommerce</title>
016 </head>
017 <body>
018     <!-- Navigation -->
019     <jsp:include page="../portal/menu.jsp"/>
020
021     <!-- Page Content -->
022     <div class="container">
023         <br/>
024         <br/>
025         <br/>
026         <div class="list-group">
027             <%
028                 String usuario = request.getUserPrincipal().getName();
029                 out.println("<h3>Bienvenido: " + usuario + "</h3>");
030                 if (request.isUserInRole("CLIENT")) {
031                     <a href="../order" class="list-group-item list-group-item-action">
032                         Pedidos</a>
033                     <%
034                         }
035                     if (request.isUserInRole("ADMINISTRATOR")) {
036                         <a href="../category" class="list-group-item list-group-item-action">
037                             Gestión de Categorías</a>
038                     <%
039                         }
040                     <%
041                     }
042                 <%
043             </div>
044             <br/>
045             <br/>
046         </div>
047     <!-- /.container -->
048
049     <!-- Footer -->
050     <jsp:include page="../portal/footer.jsp"/>
051
052     <!-- jQuery first, then Popper.js, then Bootstrap JS -->
053     <script src="https://code.jquery.com/jquery-3.3.1.js"></script>
054     <script
055     src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js"></script>
056 </body>
057 </html>
```

## Archivo css/login.css

```
001 .login-container{
002     margin-top: 5%;
003     margin-bottom: 5%;
004 }
005 .login-form-1{
006     padding: 5%;
007     box-shadow: 0 5px 8px 0 rgba(0, 0, 0, 0.2), 0 9px 26px 0 rgba(0, 0, 0, 0.19);
008 }
009 .login-form-1 h3{
010     text-align: center;
011     color: #333;
012 }
013 .login-form-2{
014     padding: 5%;
015     background: #0062cc;
016     box-shadow: 0 5px 8px 0 rgba(0, 0, 0, 0.2), 0 9px 26px 0 rgba(0, 0, 0, 0.19);
017 }
018 .login-form-2 h3{
019     text-align: center;
020     color: #fff;
021 }
022 .login-container form{
023     padding: 10%;
024 }
025 .btnSubmit
026 {
027     width: 50%;
028     border-radius: 1rem;
029     padding: 1.5%;
030     border: none;
031     cursor: pointer;
032 }
033 .login-form-1 .btnSubmit{
034     font-weight: 600;
035     color: #fff;
036     background-color: #0062cc;
037 }
038 .login-form-2 .btnSubmit{
039     font-weight: 600;
040     color: #0062cc;
041     background-color: #fff;
042 }
043 .login-form-2 .ForgetPwd{
044     color: #fff;
045     font-weight: 600;
046     text-decoration: none;
047 }
048 .login-form-1 .ForgetPwd{
049     color: #0062cc;
050     font-weight: 600;
051     text-decoration: none;
052 }
```

## Archivo css/shop-homepage.css

```
001 </*!
002  * Start Bootstrap - Shop Homepage
003  (https://startbootstrap.com/template-overviews/shop-homepage)
004  * Copyright 2013-2019 Start Bootstrap
005  * Licensed under MIT (https://github.com/BlackrockDigital/startbootstrap-shop-
006  homepage/blob/master/LICENSE)
007  */
008 body {
009     padding-top: 56px;
010 }
```

## 7. CONFIGURACIÓN DEL MECANISMO DE SEGURIDAD

### Archivo WebContent/WEB-INF/jboss-web.xml

```
001 <?xml version="1.0" encoding="UTF-8"?>
002 <jboss-web>
003     <security-domain>java:/jaas/eCommerceSecurity</security-domain>
004 </jboss-web>
```

### Archivo WebContent/WEB-INF/web.xml

```
001 <?xml version="1.0" encoding="UTF-8"?>
002 <web-app xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
003     xmlns="http://xmlns.jcp.org/xml/ns/javaee"
004     xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
005     http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd" id="WebApp_ID" version="4.0">
006     <display-name>ecommerce</display-name>
007
008     <welcome-file-list>
009         <welcome-file>index.html</welcome-file>
010         <welcome-file>index.htm</welcome-file>
011         <welcome-file>index.jsp</welcome-file>
012         <welcome-file>default.html</welcome-file>
013         <welcome-file>default.htm</welcome-file>
014         <welcome-file>default.jsp</welcome-file>
015     </welcome-file-list>
016
017     <security-constraint>
018         <display-name>Restricción de Seguridad - Usuarios</display-name>
019         <web-resource-collection>
020             <web-resource-name>Area de User</web-resource-name>
021             <url-pattern>/user/*</url-pattern>
022             <http-method>GET</http-method>
023         </web-resource-collection>
024         <auth-constraint>
025             <role-name>ADMINISTRATOR</role-name>
026             <role-name>CLIENT</role-name>
027         </auth-constraint>
028         <user-data-constraint>
029             <transport-guarantee>NONE</transport-guarantee>
030         </user-data-constraint>
031     </security-constraint>
032
033     <security-constraint>
034         <display-name>Security Constraint - Category</display-name>
033         <web-resource-collection>
034             <web-resource-name>Category Management</web-resource-name>
```

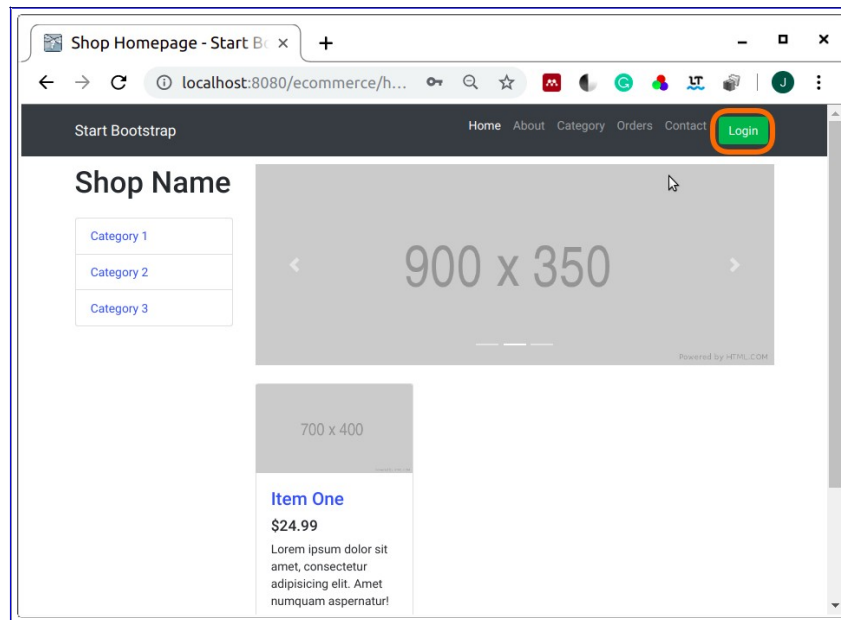
```

035         <url-pattern>/ws/category/*</url-pattern>
036         <url-pattern>/category/*</url-pattern>
037         <http-method>POST</http-method>
038         <http-method>GET</http-method>
039         <http-method>PUT</http-method>
040         <http-method>DELETE</http-method>
041     </web-resource-collection>
042     <auth-constraint>
043         <role-name>ADMINISTRATOR</role-name>
044     </auth-constraint>
045     <user-data-constraint>
046         <transport-guarantee>NONE</transport-guarantee>
047     </user-data-constraint>
048 </security-constraint>
049 <security-constraint>
050     <display-name>Security Constraint - Order</display-name>
051     <web-resource-collection>
052         <web-resource-name>Client Orders</web-resource-name>
053         <url-pattern>/order/*</url-pattern>
054         <http-method>POST</http-method>
055         <http-method>GET</http-method>
056         <http-method>PUT</http-method>
057         <http-method>DELETE</http-method>
058     </web-resource-collection>
059     <auth-constraint>
060         <role-name>CLIENT</role-name>
061         <role-name>ADMINISTRATOR</role-name>
062     </auth-constraint>
063     <user-data-constraint>
063         <transport-guarantee>NONE</transport-guarantee>
064     </user-data-constraint>
065 </security-constraint>
066
067 <login-config>
068     <auth-method>FORM</auth-method>
069     <realm-name>eCommerceSecurity</realm-name>
070     <form-login-config>
071         <form-login-page>/login/login.jsp</form-login-page>
072         <form-error-page>/login/error.jsp</form-error-page>
073     </form-login-config>
074 </login-config>
075
076 <!-- roles-(perfiles o grupos) válidos para la aplicación web -->
077 <security-role>
078     <role-name>ADMINISTRATOR</role-name>
079 </security-role>
080 <security-role>
081     <role-name>CLIENT</role-name>
082 </security-role>
083
084 <error-page>
085     <error-code>403</error-code>
086     <location>/portal/forbidden.jsp</location>
087 </error-page>
088 </web-app>

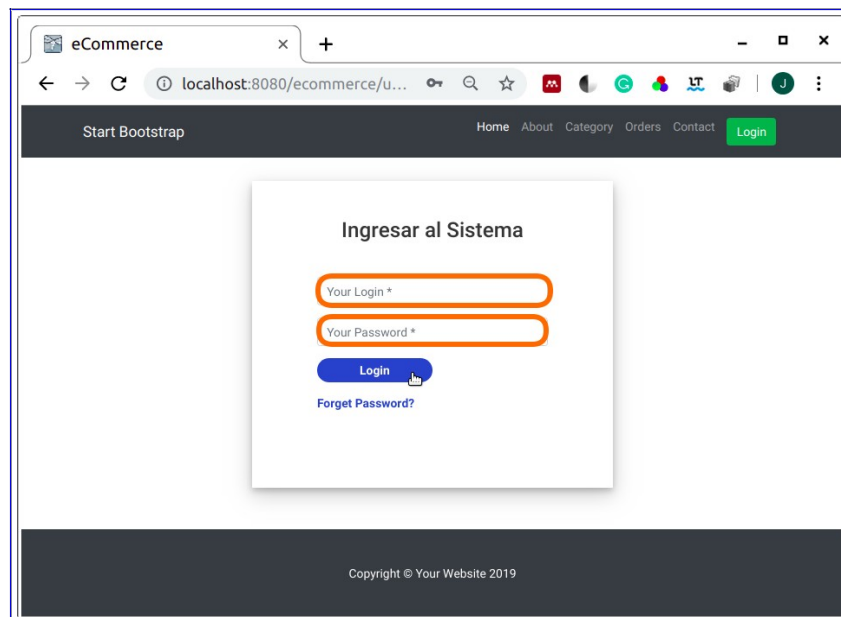
```

## 8. PRUEBAS DE SEGURIDAD

Corra la aplicación web en el servidor, abra una ventana de navegador y haga click arriba a la derecha en el botón [Login].



El sistema mostrará el formulario de login.

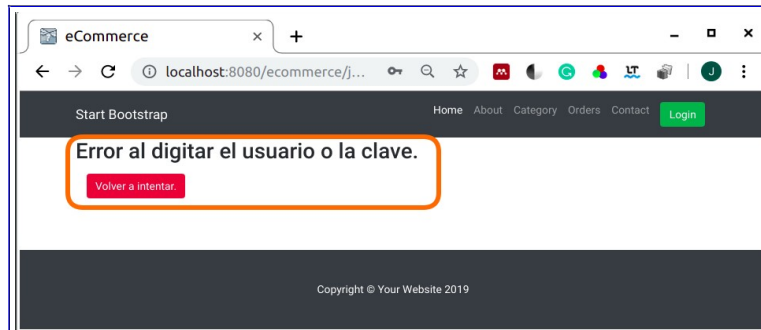


## Prueba de login

Digite los siguientes usuarios y claves:

- usuario y una clave errada,
- usuario correcto y clave errada,
- usuario incorrecto y clave correcta,
- usuario y clave correcta.

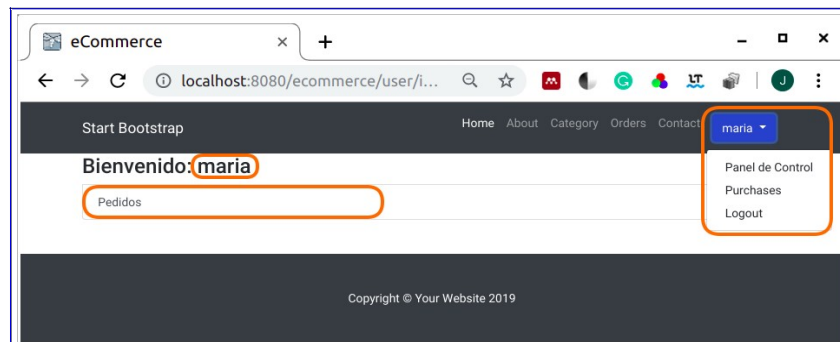
En caso de error al digitar las credenciales, el sistema debe mostrar la pagina login/error.jsp .



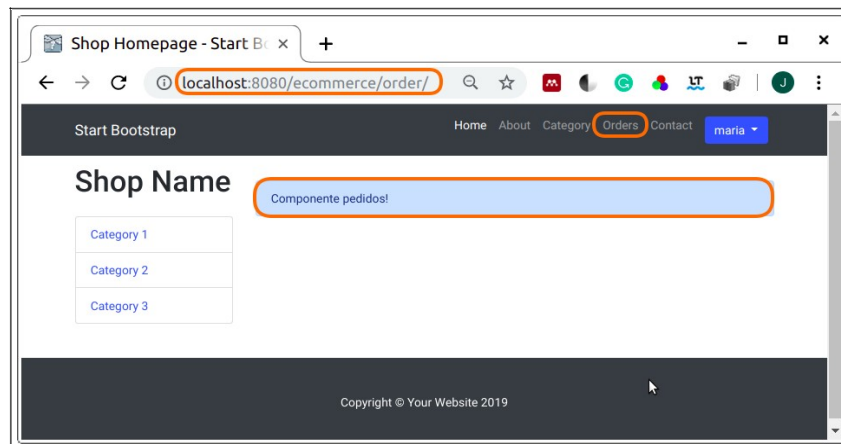
## Prueba del perfil Cliente

Haga click arriba a la derecha en el botón de [Login] y digite las credenciales de un usuario con el perfil Cliente. (user=maria, password=mquintero2018).

El sistema determina el usuario logueado (maria) y presenta el panel de control con las opciones (funcionalidad) a la que tiene permisos. A la derecha se presenta un menú con los ítems [Panel de Control] y [Logout].

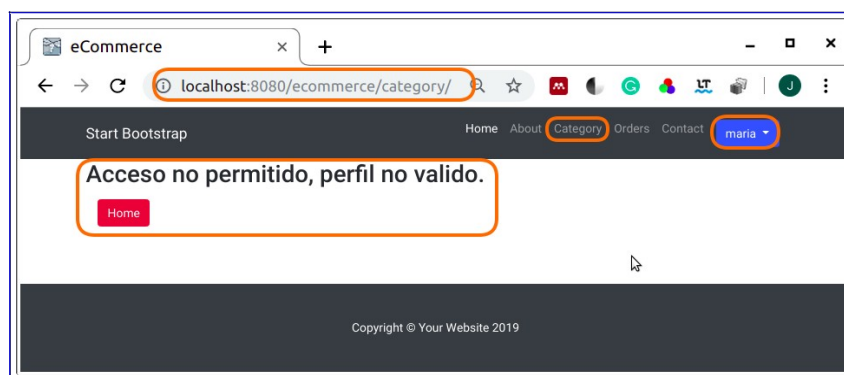


Al seleccionar la opción de pedidos (orders), se mostrará la página [order/index.jsp]. Esta funcionalidad se implementará en una iteración posterior.



## Prueba acceso no autorizado

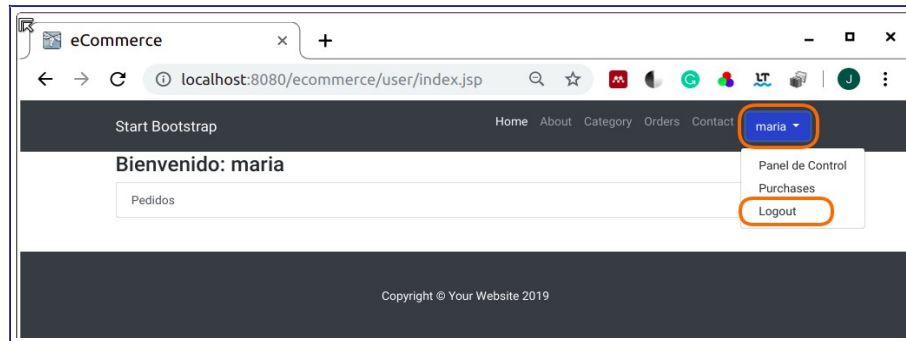
Si el usuario con perfil Cliente (maria) intenta acceder a un recurso al cual no tiene permiso (category), se producirá un error [403 Forbidden] y el sistema mostrará una pagina con el mensaje apropiado, de acuerdo a lo que se parametrizó en el archivo de configuración de la aplicación web [web.xml].



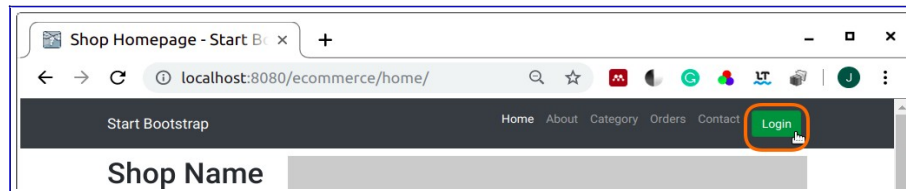


## Prueba Logout

Haga click arriba a la derecha en el menú del usuario y seleccione la opción [Logout].

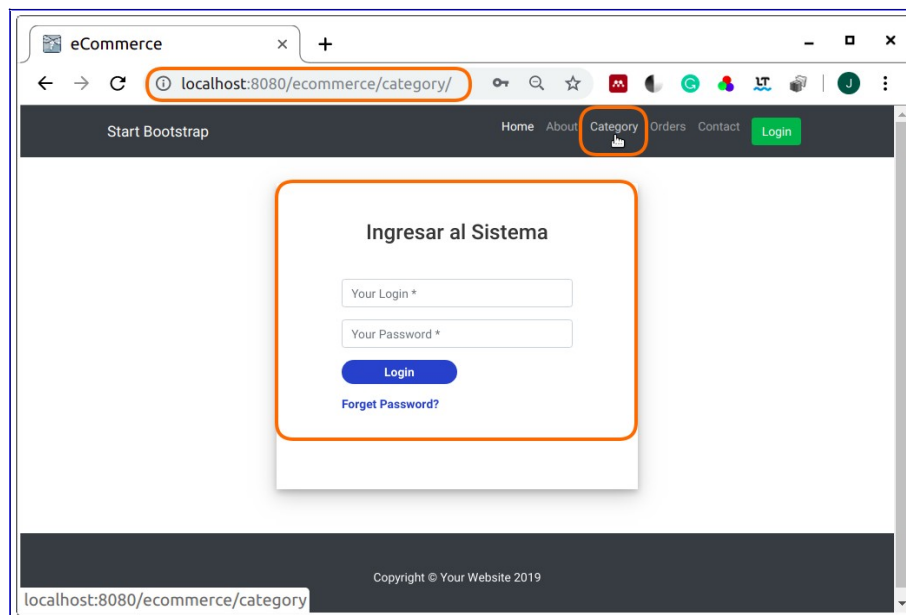


El sistema debe cerrar la sesión de usuario y presentar nuevamente el menú [Login], lo cual indica que no hay ningún usuario logueado.



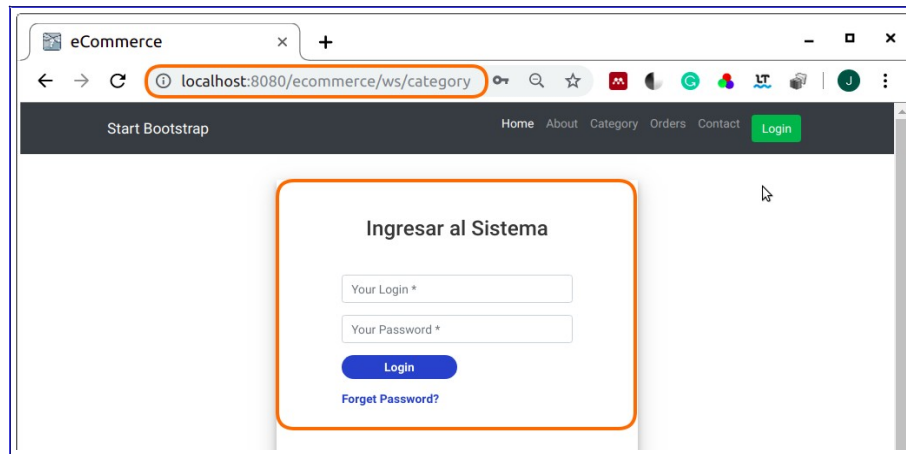
## Prueba de recurso protegido – asegurado

Si un usuario que no está logueado intenta acceder a un recurso protegido, el sistema lanzará la ventana de login. Sin estar logueado, haga click en la opción de menú [Category] o digite la url [<http://localhost:8080/eCommerce/category/>].

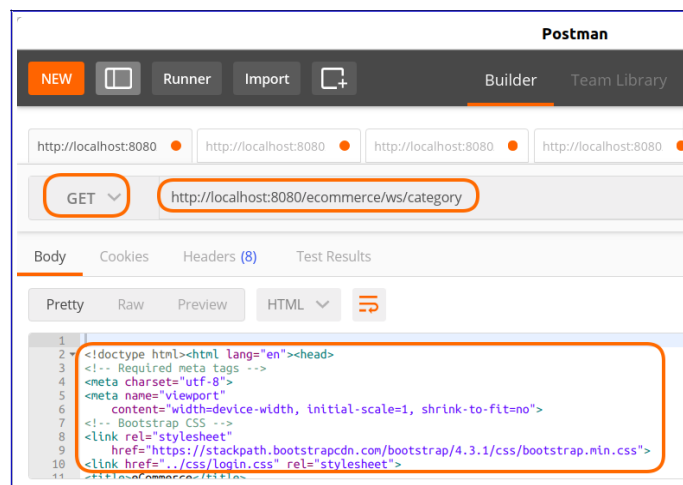


## Prueba de los Servicios Web

Si el usuario no está logueado e intenta acceder al servicio web category [<http://localhost:8080/ecommerce/ws/category>], el sistema protege el recurso y lanza la ventana de login.



Las pruebas de los servicios web en Postman, también obligan al usuario a loguearse, protegiendo – asegurando los recursos.



## REFERENCIAS

[1] <https://es.wikipedia.org/wiki/JAAS>