SPRING BOOT + SECURITY + BOOTSTRAP

# SEGURIDAD CON SPRING BOOT + THYMELEAF Y MYSQL. CAPÍTULO 6. VISTAS PRINCIPALES

Es hora de comenzar a escribir html, lo primero que vamos a hacer es crear las vistas principales.

En la carpeta templates crearemos 6 documentos html:

* error
* forbidden
* fragments
* index
* login
* registro

**fragments.html:**

Comenzaremos con fragments,html, que es el que lleva la cabecera y el footer que se mostrarán en todos los documentos:

|  |  |
| --- | --- |
|  | <!DOCTYPE HTML> |
|  | <html xmlns:th="http://www.thymeleaf.org" |
|  | xmlns:sec="http://www.thymeleaf.org/extras/spring-security"> |
|  |  |
|  | <head th:fragment="headerfiles"> |
|  | <title>Productos</title> |
|  | <meta http-equiv="Content-Type" content="text/html" charset="UTF-8"/> |
|  | <link th:href="@{/bootstrap/bootstrap.min.css}" rel="stylesheet" type="text/css"> |
|  | <link th:href="@{/fontawesome/css/all.css}" rel="stylesheet" type="text/css"> |
|  | </head> |
|  | <body> |
|  |  |
|  | <div th:fragment="nav"> |
|  | <nav class="navbar navbar-expand-lg navbar-dark bg-dark mb-3"> |
|  | <a class="navbar-brand" href="#">Productos</a> |
|  |  |
|  | <div class="collapse navbar-collapse" id="navbarSupportedContent"> |
|  | <ul class="navbar-nav mr-auto"> |
|  | <li class="nav-item"> |
|  | <a class="nav-link" href="#" th:href="@{/index}"><i class="fa fa-home"></i>&nbsp;Inicio</a> |
|  | </li> |
|  | <li class="nav-item"> |
|  | <a sec:authorize="isAuthenticated()" class="nav-link" href="#" th:href="@{/producto}">Productos</a> |
|  | </li> |
|  | </ul> |
|  | <form sec:authorize="isAuthenticated()" class="form-inline" form-method="post" th:action="@{/logout}"> |
|  | <button class="btn btn-outline-danger" type="submit"><i class="fas fa-sign-out-alt"></i> Cerrar Sesión</button> |
|  | </form> |
|  |  |
|  | <a sec:authorize="!isAuthenticated()" th:href="@{/login}"><button class="btn btn-outline-success"><i class="fa fa-user"></i> Iniciar Sesión</button></a> |
|  |  |
|  | </div> |
|  | </nav> |
|  | </div> |
|  | <div class="container"></div> |
|  | <footer th:fragment="footer" class="dark bg-dark fixed-bottom text-center p-3"> |
|  | <div class="container"> |
|  | <span class="text-muted">Footer de la página &copy; yo mismo</span> |
|  | </div> |
|  | </footer> |
|  | <script src="https://code.jquery.com/jquery-3.3.1.slim.min.js" integrity="sha384-q8i/X+965DzO0rT7abK41JStQIAqVgRVzpbzo5smXKp4YfRvH+8abtTE1Pi6jizo" crossorigin="anonymous"></script> |
|  | <script>window.jQuery || document.write('<script src="../../assets/js/vendor/jquery-slim.min.js"><\/script>')</script> |
|  | <script src="../../assets/js/vendor/popper.min.js"></script> |
|  | <script src="../../dist/js/bootstrap.min.js"></script> |
|  | </body> |
|  | </html> |

[**view raw**](https://gist.github.com/cavanosa/d3da98eccffbb26da4f878b4e41b3aa6/raw/b1b1e8ca5756efb9af5c3c8717db738e141cdefd/fragments.html)[**fragments.html**](https://gist.github.com/cavanosa/d3da98eccffbb26da4f878b4e41b3aa6#file-fragments-html) hosted with  by [**GitHub**](https://github.com/)

Tenemos un navbar en la cabecera que muestra los menús de navegación así como el pie de página (footer).

En este documento utilizamos varias etiquetas de thymeleaf; por ejemplo

th:href="@{/index}"

es un link con thymeleaf. También hay etiquetas de thymeleaf security como

sec:authorize="isAuthenticated()"

con la que comprobamos si se ha iniciado sesión o no para mostrar el link de productos.

Tenemos un formulario para el logout

form-method="post" th:action="@{/logout}"

que mostrará el botón de cerrar sesión si estamos autenticados y, en el caso contrario, el de iniciar de sesión.

**index.html:**

Esta es la página principal a la que todo el mundo puede acceder y muestra un saludo genérico. En caso de estar logueado, además, el saludo se personaliza mostrando el nombre de usuario:

|  |  |
| --- | --- |
|  | <!DOCTYPE html> |
|  | <html xmlns:th="http://www.thymeleaf.org" |
|  | xmlns:sec="http://www.thymeleaf.org/extras/spring-security"> |
|  | <head th:insert="fragments.html :: headerfiles"></head> |
|  | <body> |
|  | <header th:insert="fragments.html :: nav"></header> |
|  | <div class="container"> |
|  | <div class="jumbotron"> |
|  | <h1 sec:authorize="!isAuthenticated()" class="display-4">Muy buenas, visitante</h1> |
|  | <h1 sec:authorize="isAuthenticated()" class="display-4">Muy buenas, <span sec:authentication="name"></span></h1> |
|  | <p class="lead">Bienvenido a nuestra tienda de productos</p> |
|  | <hr class="my-4"> |
|  | <p>Si quieres más tutoriales, visita nuestro blog</p> |
|  | <p class="lead"> |
|  | <a class="btn btn-primary btn-lg" href="https://inezpre5.wordpress.com" role="button" target="\_blank">Visitar el blog</a> |
|  | </p> |
|  | </div> |
|  | </div> |
|  | <footer th:insert="fragments.html::footer"></footer> |
|  | </body> |
|  | </html> |

[**view raw**](https://gist.github.com/cavanosa/e96efba69febe2d1549e38480e1c70ad/raw/c965a0b9de581df67f9fc1dfe8fffc5c878dd79c/index.html)[**index.html**](https://gist.github.com/cavanosa/e96efba69febe2d1549e38480e1c70ad#file-index-html) hosted with  by [**GitHub**](https://github.com/)

En cuanto a los fragmentos (cabecera y footer) vemos que se insertan con las anotacione

th:insert="fragments.html :: nav"

th:insert="fragments.html :: footer"

**Página de error:**

Si creamos un documento con el nombre error.html, se mostrará esa página en vez del clásico whitelabel error page de Spring Boot. Este es el código:

|  |  |
| --- | --- |
|  | <!DOCTYPE html> |
|  | <html xmlns:th="http://www.thymeleaf.org" |
|  | xmlns:sec="http://www.thymeleaf.org/extras/spring-security"> |
|  | <head th:insert="fragments.html :: headerfiles"> |
|  | <title>Fail</title> |
|  | </head> |
|  | <body> |
|  | <header th:insert="fragments.html :: nav"></header> |
|  | <div class="container mt-5"> |
|  | <div> |
|  | <div class="card mt-4"> |
|  | <div class="card-header"> |
|  | <i class="fa fa-bomb"></i>&nbsp;Página no Encontrada 404 |
|  | </div> |
|  | <div class="card-block p-4"> |
|  |  |
|  |  |
|  | <img th:src="@{/img/chuck.jpg}" class="img-fluid"> |
|  |  |
|  | </div> |
|  | <a th:href="@{/index}"><button class="btn btn-primary btn-lg"><i class="far fa-hand-point-left"></i>&nbsp;Inicio</button></a> |
|  | </div> |
|  | </div> |
|  | </div> |
|  | <footer th:insert="fragments.html::footer"></footer> |
|  | </body> |
|  | </html> |

[**view raw**](https://gist.github.com/cavanosa/3cde1c957b318ac1982af9369b4a6631/raw/35e415aeecd11deafc72a148e1cd8cc3612ce317/error.html)[**error.html**](https://gist.github.com/cavanosa/3cde1c957b318ac1982af9369b4a6631#file-error-html) hosted with  by [**GitHub**](https://github.com/)

**Forbidden:**

Es igual a la de error (podéis ponerlas como queráis) salvo un par de frases:

|  |  |
| --- | --- |
|  | <!DOCTYPE html> |
|  | <html xmlns:th="http://www.thymeleaf.org" |
|  | xmlns:sec="http://www.thymeleaf.org/extras/spring-security"> |
|  | <head th:insert="fragments.html :: headerfiles"> |
|  | <title>Fail</title> |
|  | </head> |
|  | <body> |
|  | <header th:insert="fragments.html :: nav"></header> |
|  | <div class="container mt-5"> |
|  | <div> |
|  | <div class="card mt-4"> |
|  | <div class="card-header"> |
|  | <i class="fa fa-bomb"></i>&nbsp;Sólo Chuck Norris puede ver esta página 403 |
|  | </div> |
|  | <div class="card-block p-4"> |
|  |  |
|  |  |
|  | <img th:src="@{/img/chuck.jpg}" class="img-fluid"> |
|  |  |
|  | </div> |
|  | <a th:href="@{/index}"><button class="btn btn-primary btn-lg"><i class="far fa-hand-point-left"></i>&nbsp;Inicio</button></a> |
|  | </div> |
|  | </div> |
|  | </div> |
|  | <footer th:insert="fragments.html::footer"></footer> |
|  | </body> |
|  | </html> |

[**view raw**](https://gist.github.com/cavanosa/4059e0e60964115bb8ad2e3f7efd2a5f/raw/16da426cbe7c9e4790d33b255c48046a67b0a61c/forbidden.html)[**forbidden.html**](https://gist.github.com/cavanosa/4059e0e60964115bb8ad2e3f7efd2a5f#file-forbidden-html) hosted with  by [**GitHub**](https://github.com/)

**Login:**

|  |  |
| --- | --- |
|  | <!DOCTYPE html> |
|  | <html xmlns:th="http://www.thymeleaf.org" |
|  | xmlns:sec="http://www.thymeleaf.org/extras/spring-security"> |
|  | <head th:insert="fragments.html :: headerfiles"> |
|  | <title>Log In</title> |
|  | </head> |
|  | <body> |
|  | <header th:insert="fragments.html :: nav"></header> |
|  | <div class="container mt-5"> |
|  | <div> |
|  | <div class="card mt-4"> |
|  | <div class="card-header"> |
|  | <i class="fa fa-user"></i> Iniciar sesión |
|  | </div> |
|  | <div class="card-block p-4"> |
|  | <form sec:authorize="!isAuthenticated()" name="f" th:action="@{/signin}" method="post"> |
|  | <fieldset> |
|  | <div th:if="${param.error}" class="alert alert-danger"> |
|  | Credenciales erróneas |
|  | </div> |
|  | <div th:if="${registroOK}" class="alert alert-success" th:text="${registroOK}">> |
|  | </div> |
|  | <div th:if="${param.logout}" class="alert alert-success"> |
|  | Hasta pronto!! |
|  | </div> |
|  | <div class="form-group"> |
|  | <label for="textUsername">Nombre</label> |
|  | <input type="text" name="textUsername" id="textUsername" class="form-control" placeholder="nombre..."> |
|  | </div> |
|  | <div class="form-group"> |
|  | <label for="textPassword">Contraseña</label> |
|  | <input type="password" name="textPassword" id="textPassword" class="form-control"> |
|  | </div> |
|  | <div class="form-check"> |
|  | <input type="checkbox" class="form-check-input" id="checkRememberMe" name="checkRememberMe"> |
|  | <label for="checkRememberMe" class="form-check-label">Recordarme</label> |
|  | </div> |
|  | <div class="form-actions mt-4"> |
|  | <button type="submit" class="btn btn-success">Iniciar Sesión</button> |
|  | </div> |
|  | </fieldset> |
|  | </form> |
|  | <div class="mt-3" sec:authorize="!isAuthenticated()"> |
|  | <a th:href="@{/usuario/registro}"><button class="btn btn-primary" >Registrarse</button></a> |
|  | </div> |
|  |  |
|  | <p sec:authorize="isAuthenticated()">Ya estás logueado</p> |
|  | </div> |
|  | </div> |
|  | </div> |
|  | </div> |
|  | <footer th:insert="fragments.html::footer"></footer> |
|  | </body> |
|  | </html> |

[**view raw**](https://gist.github.com/cavanosa/a7038ed67c910402980d824aea08ad2c/raw/38be305991ecba86b83165044da9b692d40dfd24/login.html)[**login.html**](https://gist.github.com/cavanosa/a7038ed67c910402980d824aea08ad2c#file-login-html) hosted with  by [**GitHub**](https://github.com/)

El formulario se muestra si no se ha iniciado sesión, en caso contrario aparece un texto donde se informa al usuario de que ya está loguedao.

El form action es signin, tal como se había especificado en la clase SecurityConfig.

También hay varios textos condicionales (th:if) que aparecerán si se han introducido mal las credenciales, si se ha creado una cuenta con éxito o si se ha cerrado sesión.

Los campos del formulario de nombre de usuario, password y rememberMe deberán llamarse textUsername, textPassword y checkRememberMe, tal como se indicó en SecurityConfig.

**Registro:**

Y ya para finalizar este post, creamos el formulario de registro (registro.html):

|  |  |
| --- | --- |
|  | <!DOCTYPE html> |
|  | <html xmlns:th="http://www.thymeleaf.org" |
|  | xmlns:sec="http://www.thymeleaf.org/extras/spring-security"> |
|  | <head th:insert="fragments.html :: headerfiles"> |
|  | <title>Nuevo Usuario</title> |
|  | </head> |
|  | <body> |
|  | <header th:insert="fragments.html :: nav"></header> |
|  | <div class="container mt-5"> |
|  | <div> |
|  | <div class="card mt-4"> |
|  | <div class="card-header"> |
|  | <i class="fa fa-user"></i> Nuevo Usuario |
|  | </div> |
|  | <div th:if="${error}" class="alert alert-danger"> |
|  | <p class="text text-danger" th:text="${error}"></p> |
|  | </div> |
|  | <div class="card-block p-4"> |
|  | <form action="/usuario/registrar" method="post" sec:authorize="!isAuthenticated()"> |
|  | <!-- protección csrf --> |
|  | <input type="hidden" th:name="${\_csrf.parameterName}" th:value="${\_csrf.token}" /> |
|  | <!-- fin csrf --> |
|  | <fieldset> |
|  | <div class="form-group"> |
|  | <label for="nombre">Nombre</label> |
|  | <input type="text" name="nombre" id="nombre" class="form-control" placeholder="nombre..."> |
|  | </div> |
|  | <div class="form-group"> |
|  | <label for="password">Contraseña</label> |
|  | <input type="password" name="password" id="password" class="form-control"> |
|  | </div> |
|  | <div class="form-actions mt-4"> |
|  | <button type="submit" class="btn btn-success">Crear Cuenta</button> |
|  | </div> |
|  | </fieldset> |
|  | </form> |
|  | <p sec:authorize="isAuthenticated()">Ya tienes cuenta</p> |
|  | </div> |
|  | </div> |
|  | </div> |
|  | </div> |
|  | <footer th:insert="fragments.html::footer"></footer> |
|  | </body> |
|  | </html> |

[**view raw**](https://gist.github.com/cavanosa/baa71805534f877712627bd8dc9b78bc/raw/a4aea1f3fbff50950aa4f292b197dad74e9f217e/registro.html)[**registro.html**](https://gist.github.com/cavanosa/baa71805534f877712627bd8dc9b78bc#file-registro-html) hosted with  by [**GitHub**](https://github.com/)

Aquí hay un campo oculto con los tokens csrf (cross site request forgery). Es un tipo de ataque malicioso y Spring Boot activa por defecto la protección contra este malware. Una opción es deshabilitarlo en SecurityConfig con csrf().disable(), aunque no es una buena idea. Lo recomendable es utilizar los tokens csrf en los métodos POST

input type="hidden" th:name="${\_csrf.parameterName}" th:value="${\_csrf.token}"

Aquí concluye esta entrada, en la siguiente finalizaremos el proyecto con las vistas de los productos.