3. **FORM AUTHENTICATION**

- Rather then spring provided form , here we will build our own form for form-based authentication
- Also now we are going to lock all navigation tabs, only valid users will be able to access the site

<intercept-url pattern="**/***" /> //It will intercept urls only at first level eg. /page.html

<intercept-url pattern="**/****" /> //It will intercept url at all levels eg. /folder/folder1/page.html

- Intercepting urls are executed in the order they are defined in security-config.xml

```
<http>
    <csrf disabled="true"/>

    <intercept-url pattern="/**" access="hasRole('ROLE_USER')"/>
    <intercept-url pattern="/addNewBook.do" access="hasRole('ROLE_ADMIN')"/>

    <form-login />
    <logout logout-success-url="/viewAllBooks.do"/> <!-- /logout; automatically logout -->
</http>
```

So , as per rule #1 , all users can access any of the urls which has 'ROLE_USER' . Therefore our user '**joe**'

Will be able to access the admin page as well

Solution: Resuffle the intercept-url

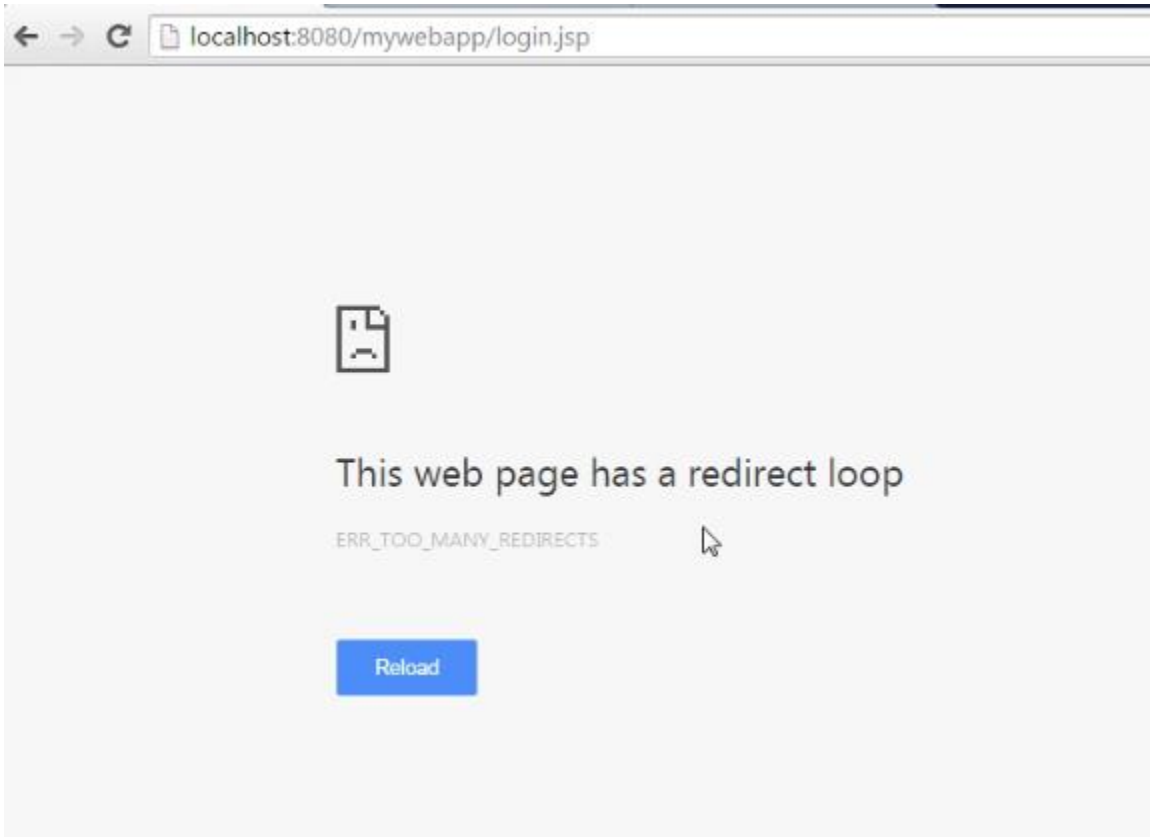
```
<http>
    <csrf disabled="true"/>

    <intercept-url pattern="/addNewBook.do" access="hasRole('ROLE_ADMIN')"/>
    <intercept-url pattern="/**" access="hasRole('ROLE_USER')"/>

    <form-login />
    <logout logout-success-url="/viewAllBooks.do"/> <!-- /logout; automatically logout -->
</http>
```

Also in form-based authentication , on redeploy of allipcation as the session gets invalidated , the user information is lost , whereas in http-basic authentication , the user information was retained.

Creating custom login page :

```
<form-login  login-processing-url="/performLogin" password-parameter="vppPassword"
             username-parameter="vppUsername"
             login-page="/login.jsp"/>
```

Now if I redeploy the application , I get below error .



Problem is there are infinet redirection loops , because we have secured our entire site.

Solution : Open up the security for this Login page

```
<http>
    <csrf disabled="true"/>

    <intercept-url pattern="/login.jsp" access="permitAll"/>
    <intercept-url pattern="/addNewBook.do" access="hasRole('ROLE_ADMIN')"/>
    <intercept-url pattern="/**" access="hasRole('ROLE_USER')"/>

    <form-login  login-processing-url="/performLogin" password-parameter="vppPassword"
                 username-parameter="vppUsername"
                 login-page="/login.jsp"/>

    <logout logout-success-url="/viewAllBooks.do"/> <!-- /logout; automatically logout -->
</http>
```

Now there will be some styling issues :

So we also need to remove the security from styling , this we are doing via , another http block

```
<http pattern="/styles.css" security="none"/>
```

There is a little difference , when we bypass security as above,

Earlier using `<intercept-url pattern="/login.jsp" access="permitAll"/>` , the **spring secuirty is applied** on that url-pattern , but spring security is going to decide , yes its fineto access this url .

Wheras with `<http pattern="/styles.css" security="none"/>` this version , we are not doing any security atall.

Now if we redploy the application and run :

- If the credentials did not match or invalid credentials , then application is doing nothing ie. We get no response from the server that , the credentials are invalid.

Solution : Attribute authentication-failure-url

- This is the url which we are going to get if there is login failure.
- And If we don't supply this url then spring is going to generate one for me
- Default login-failure url : /login?error
    - **?error** is my request parameter

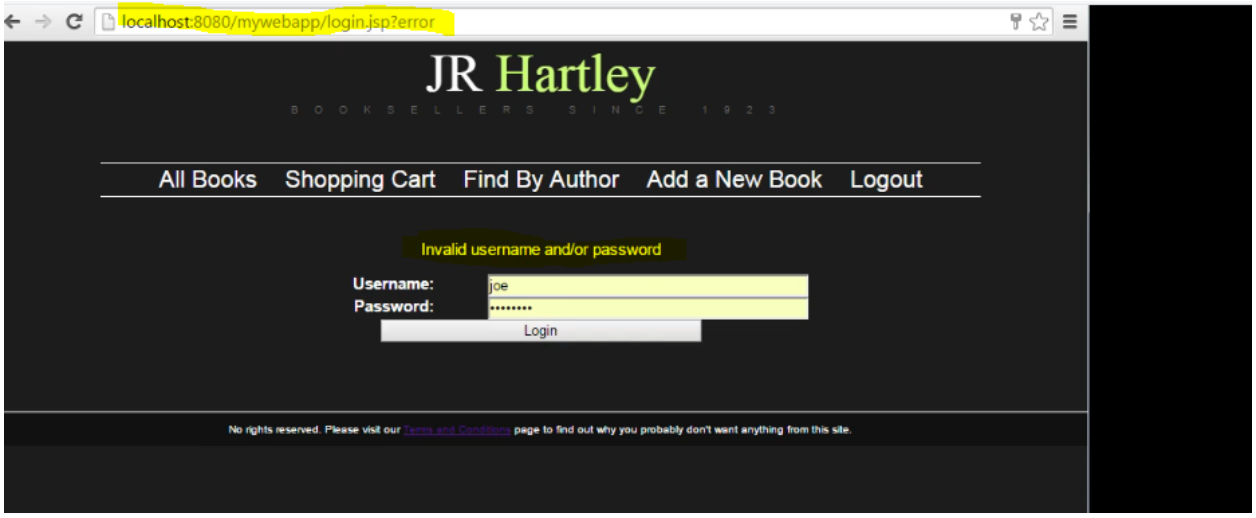
- If we send this failure-login to same page where we have login url , then we can query this login parameter ie. **error** , and show the failure response for login

```
<http>
    <csrf disabled="true"/>

    <intercept-url pattern="/login.jsp" access="permitAll"/>
    <intercept-url pattern="/addNewBook.do" access="hasRole('ROLE_ADMIN')"/>
    <intercept-url pattern="/**" access="hasRole('ROLE_USER')"/>

    <form-login  login-processing-url="/performLogin" password-parameter="vppPassword"
                 username-parameter="vppUsername"
                 login-page="/login.jsp"
                 authentication-failure-url="/login.jsp?error"/>

    <logout logout-success-url="/viewAllBooks.do"/> <!-- /logout; automatically logout -->
</http>
```

- In login.jsp page we can test for this parameter

```
<%@ taglib uri="http://java.sun.com/jsp/jstl/core" prefix="c" %>

<html>
   <head>
    <title>Login</title>
    <link href="<c:url value="/styles.css"/>" rel="Stylesheet" type="text/css"/>
   </head>

   <body>
      <jsp:include page="/header.jsp"/>

      <div id="addBook">

          <c:url value="/performLogin" var="loginUrl"/>

          <form action="${loginUrl}" method="post">

            <c:if test="${param.error != null}">
                <p>Invalid username and/or password</p>
            </c:if>

            <label>Username:</label> <input type="text" name="vppUsername" value="${username}"/>
            <label>Password:</label> <input type="password" name="vppPassword"/>

            <input type="submit" value="Login"/>
          </form>
      </div>

      <jsp:include page="/footer.jsp"/>
```

Redeploy and run the application :


localhost:8080/mywebapp/login.jsp?error
JR Hartley
BOOKSELLERS SINCE 1923
All Books
Shopping Cart
Find By Author
Add a New Book
Logout
Invalid username and/or password
Username:
joe
Password:
Login
No rights reserved. Please visit our Terms and Conditions page to find out why you probably don't want anything from this site.