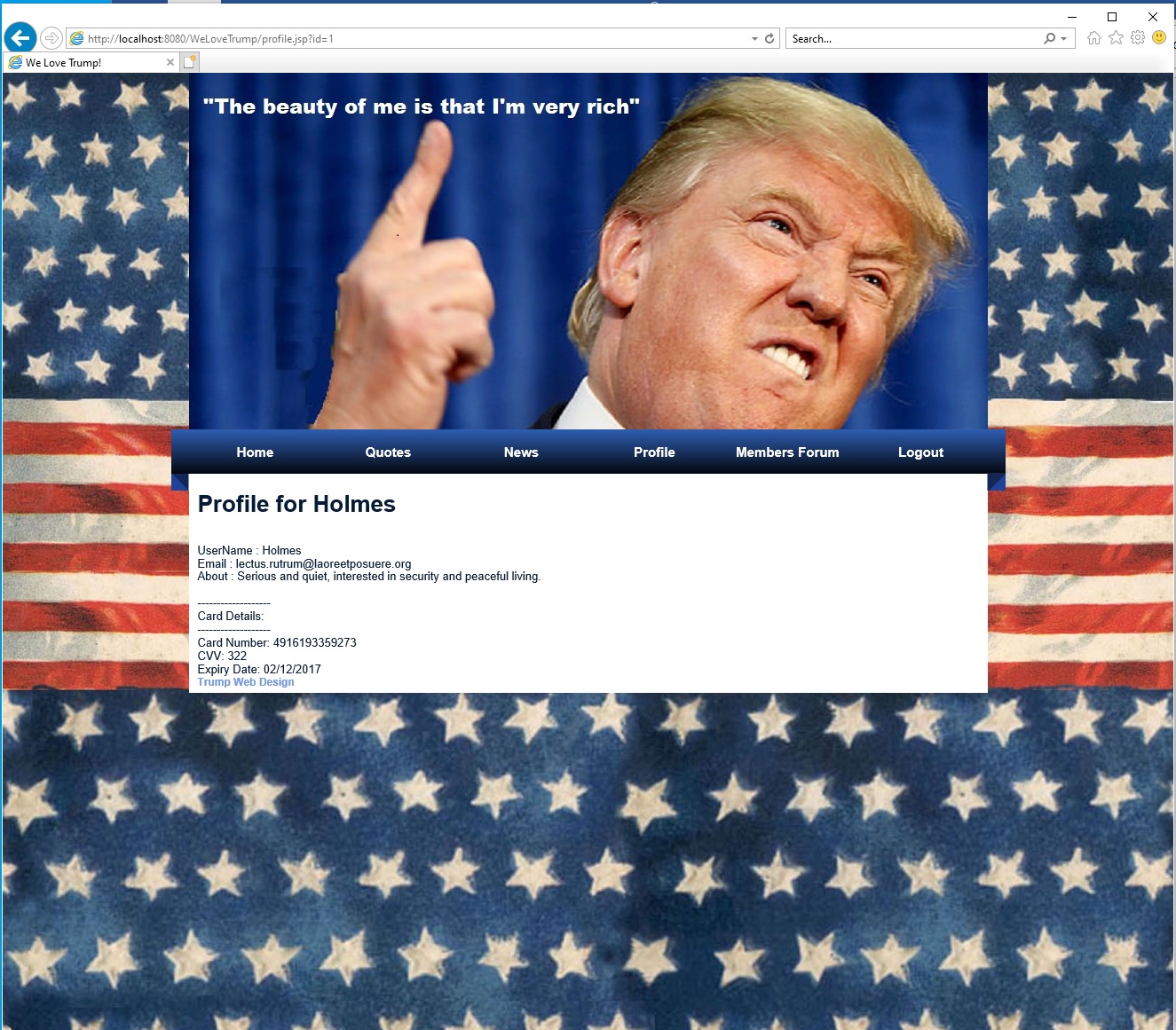
"Holmes","MEC15DBF3XD"

Bypassing login:

Source Packages > validate > ValidateLogin.java uses statement() that means it is executing string-based SQL queries unlike preparedStatement() executes parameterized SQL queries. That means we can exploit it with ‘ or ‘1’=’1’;#. By doing that we creating SQL query which looks like this: select \* from users where username=’’ or ‘1’=’1’;# and password=’’; . It says check username or if 1=1 is true, which is and it will returns from users table 1st column



Which did.

Need to replace:

Statement stmt = con.createStatement();

rs=stmt.executeQuery("select \* from users where username='"+user+"' and password='"+pass+"'");

with:

PreparedStatement pst = con.prepareStatement("select \* from users where username=? and password=?");

pst.setString(1,user);

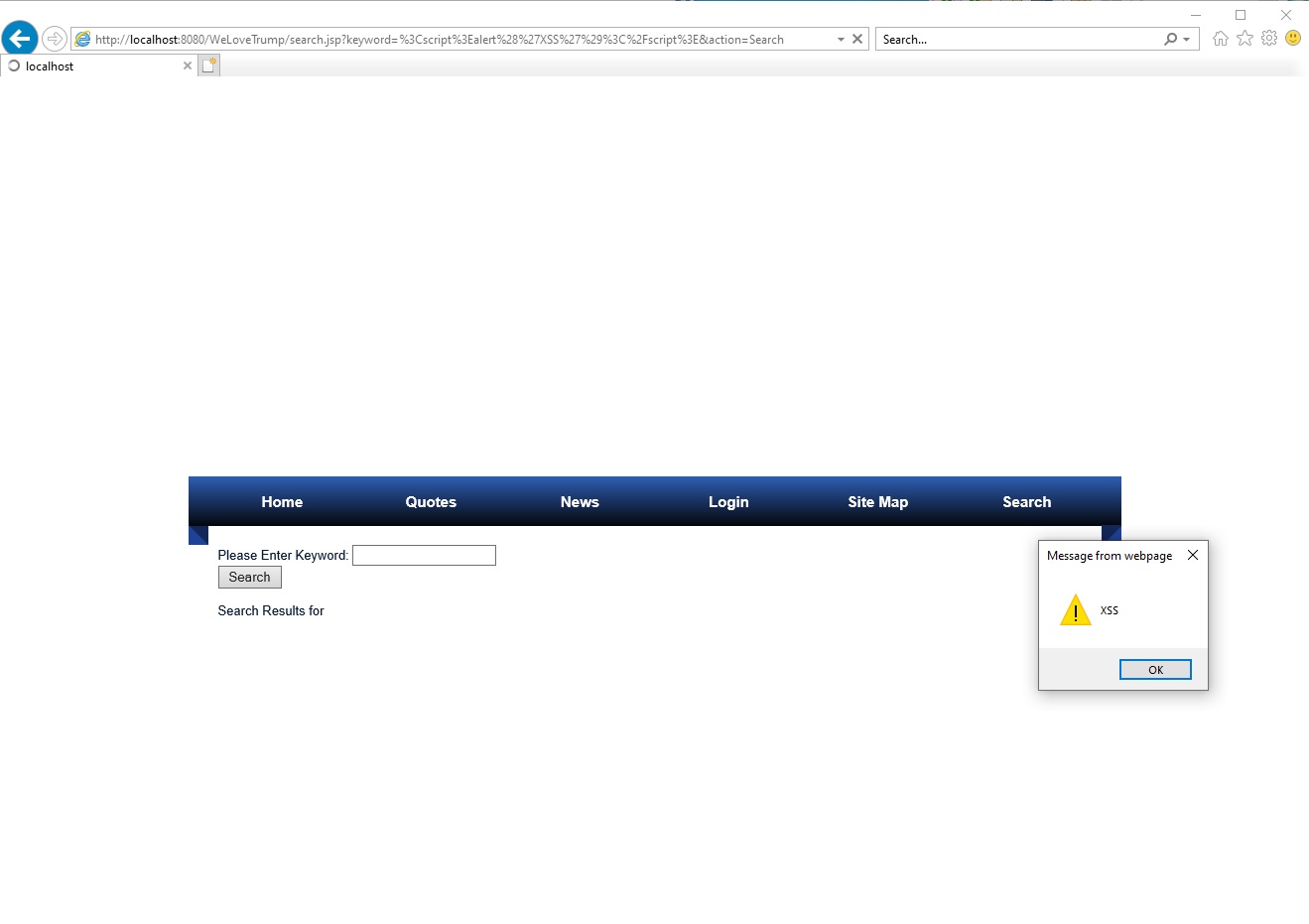
pst.setString(1,pass);

rs=pst.executeQuery();

and import java.sql.PreparedStatement;

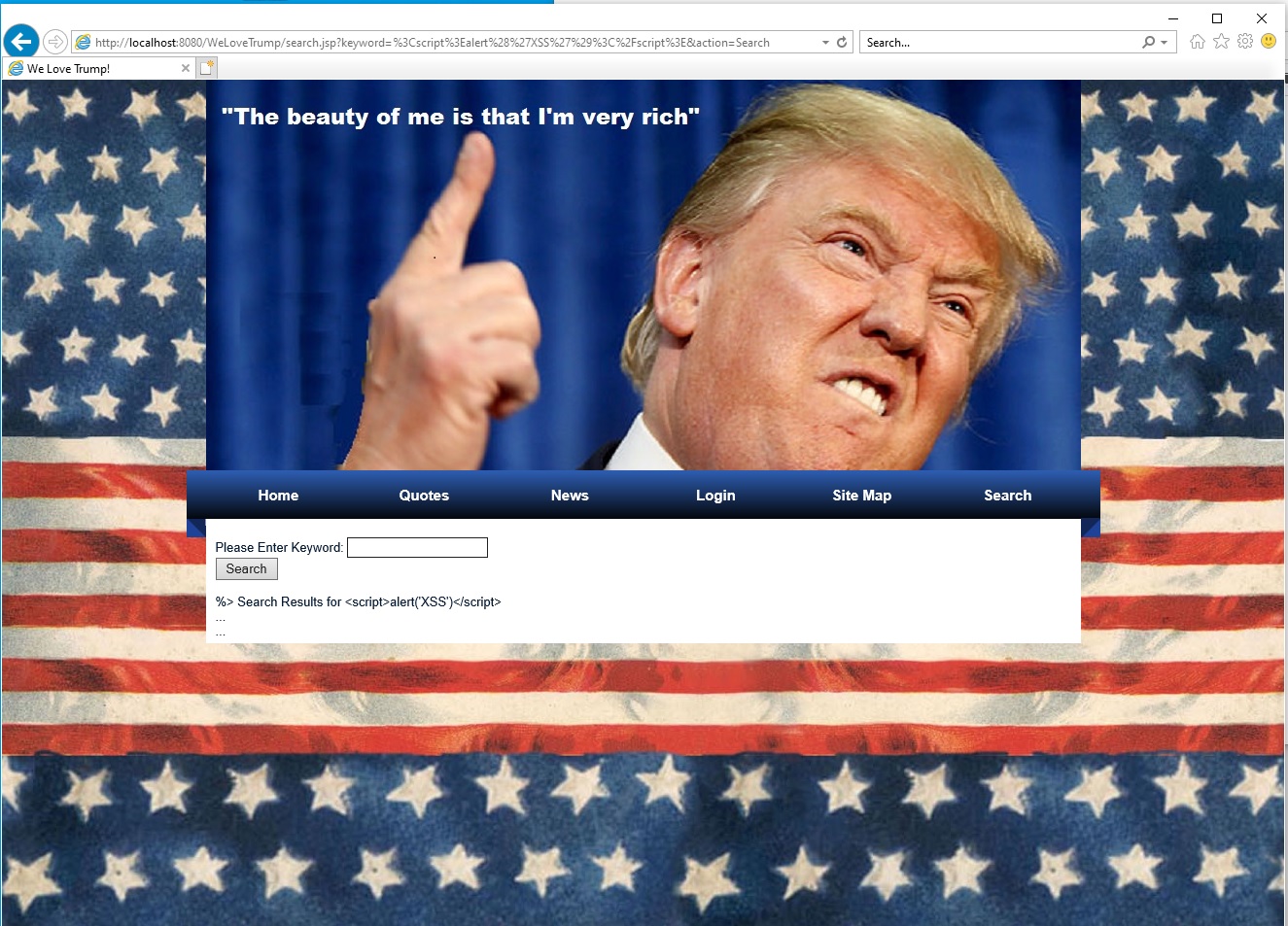
Cross-Site-Scripting(XSS)

Images >search.jsp is vulnerable for xss attack. Tried to put in search bar javascript code <script>alert('XSS')</script> after I got displayed alert box with “XXS”.



Fixed it by adding JSTL library add before <html> tag <%@ taglib uri="http://java.sun.com/jsp/jstl/core"prefix="c"%>

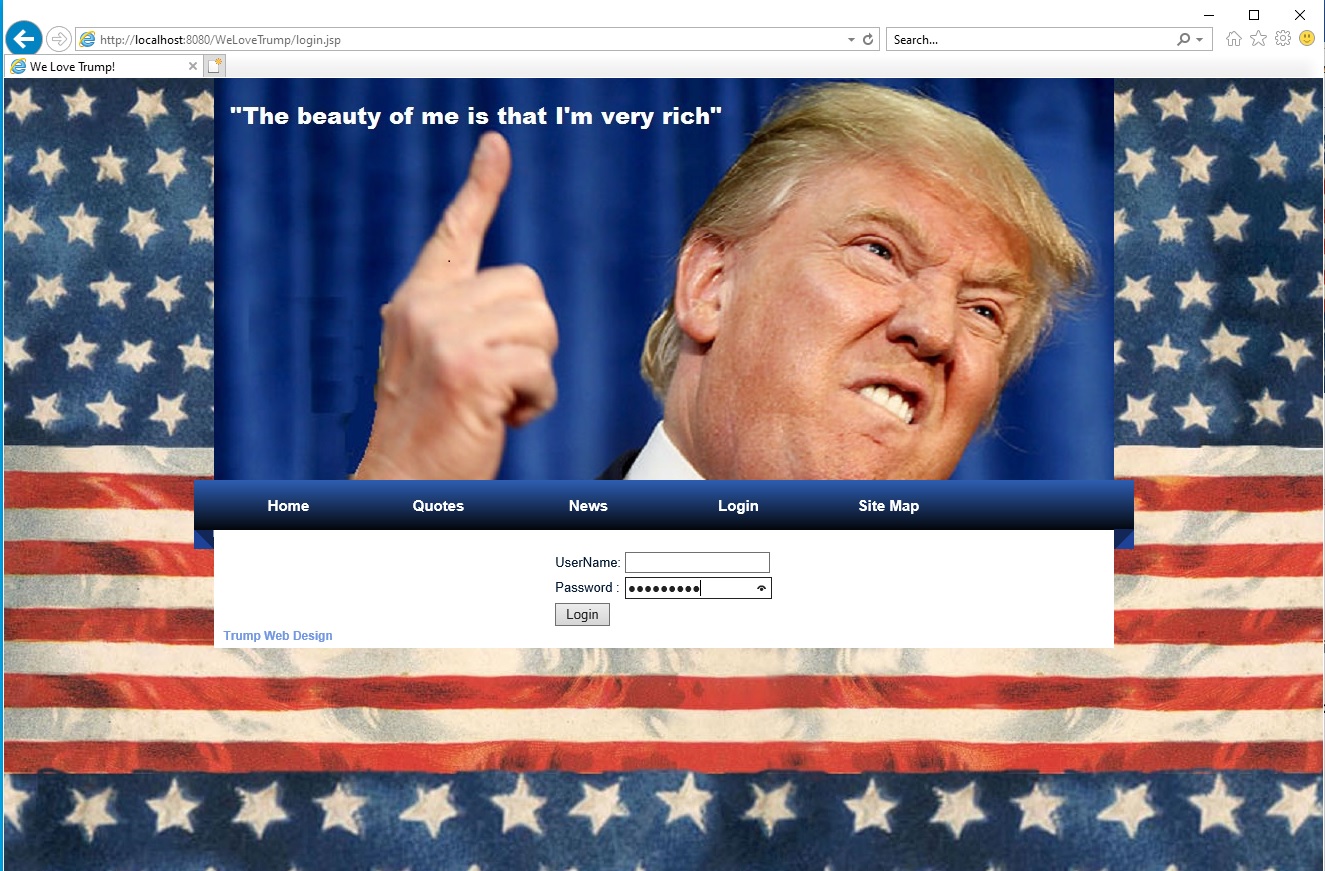
and moderating Search Results for <%=searchedName%> to > Search Results for <c:out value="<%=searchedName%>" /> in search.jsp



Images > login.jpg

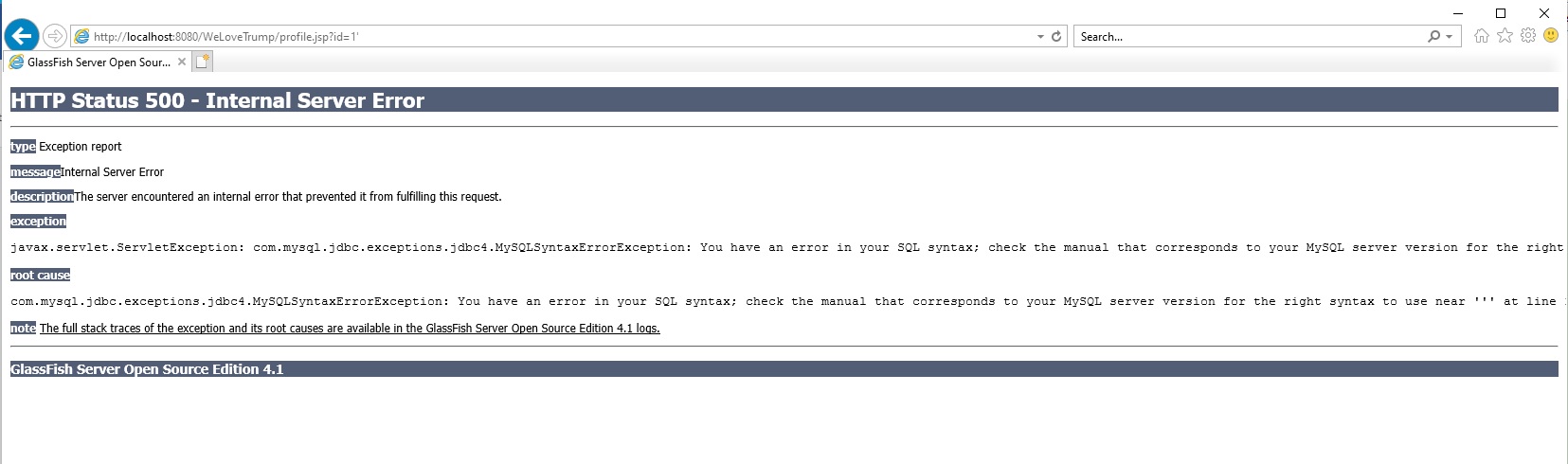
Line 46 password input changed type from “text” to “password” it’s always good idea to hide your password in case someone is looking over the shoulder.

<tr><td>Password :</td><td><input type="password" name="password" value="<%=password%>"/></td></tr>



Getting server information Web pages > profile.jsp

Adding ‘ in the end of url <http://localhost:8080/WeLoveTrump/profile.jsp?id=1'> will crash site and will give information about web server and what db site is using



Solution: surround statement with try catch block

}catch(Exception e)

{

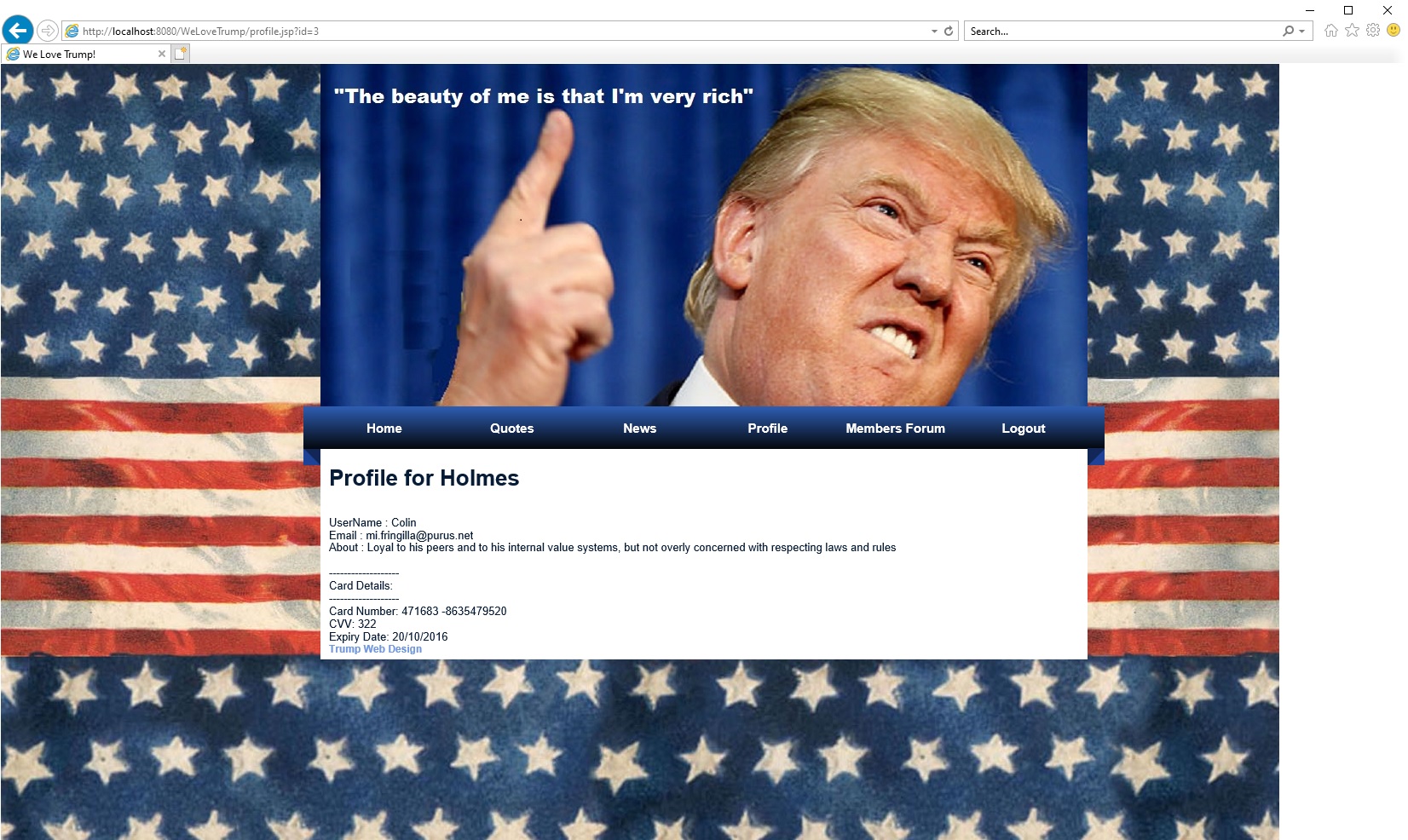
response.sendRedirect("profile.jsp"); }

testing after inserting try catch

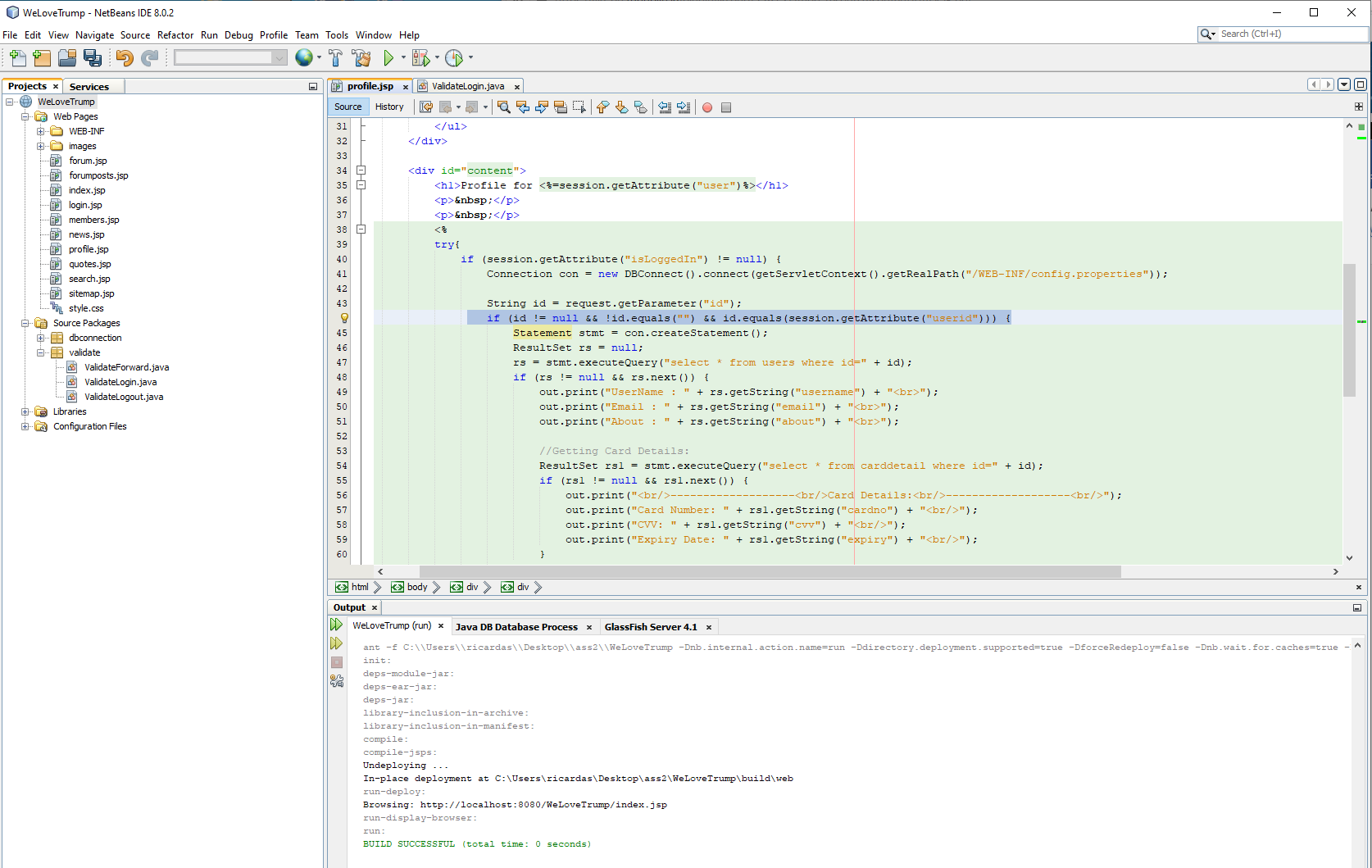


**Profile.jsp**

Changing users id from url and accessing different users profile details. Login with Holmes whos user id is 1, and changed in url to 3 and it gave me details of user id = 3

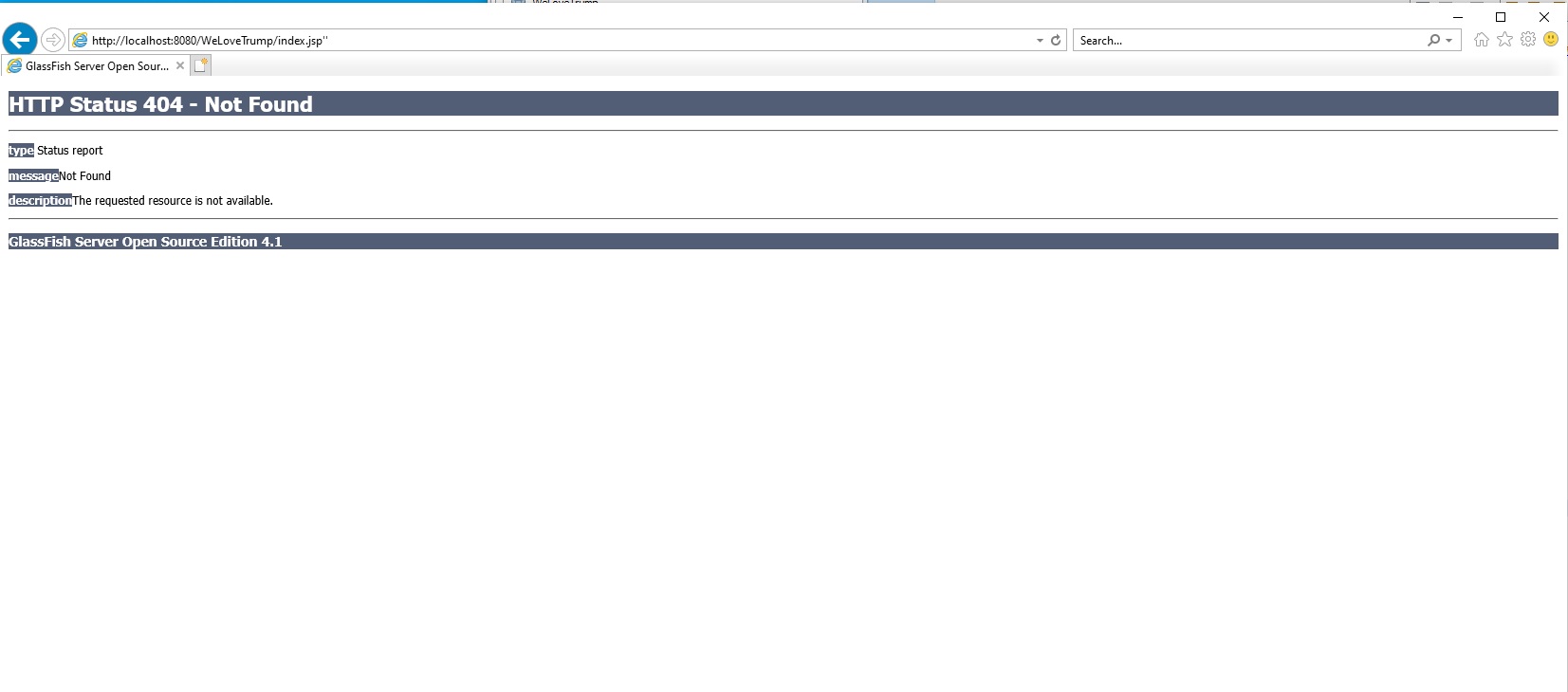


Fixed by compared parameter id with session id on line 44 by adding to if statement && id.equals(session.getAttribute("userid"))



**Page not found error 404**

At the end of url trying to add unexpected symbol, or enter not existing page displays web servers some details



to fix it I add in to WEB-INF >web.xml <error-page> element to handle missing page error:

<error-page>

<error-code>404</error-code>

<location>/Error.jsp</location>

</error-page>

And created Error.jsp so it display that error accrued but didn’t specified what kind of error

