

練習

網路應用程式安全機制

鄭安翔

ansel_cheng@hotmail.com

Lab 1

- 修改 **ContactInfo** 網路應用專案
 - 不包含**Filter**機制 (與第九章練習完成結果相同)
 - 以內建安全機制保護要求使用者登入
- **Tomcat** 中設定使用者帳號及角色
 - `<TOMCAT_HOME>\conf\tomcat-users.xml`
 - 新增腳色
 - 新增使用者帳號並指定角色

Lab 1

- 部署描述檔設定安全機制
 - 新增部署描述檔(web.xml)
 - web.xml中選擇 security標籤
 - 展開Login Configuration, 選擇 basic
 - 宣告安全性腳色
 - 展開Security Roles
 - 新增安全性角色user

Lab 1

- ❑ 宣告安全性限制條件

- web.xml security標籤中Security Constraints 資料夾

- 新增Security Constraint

- ❑ Display Name 欄位輸入 Constraint1

- 新增網路資源集合

- ❑ Web Resource Collections 按新增按鈕

- ❑ Resource Name 欄位輸入 MyResource

- ❑ URL Patterns 欄位輸入 /SelectCustomer

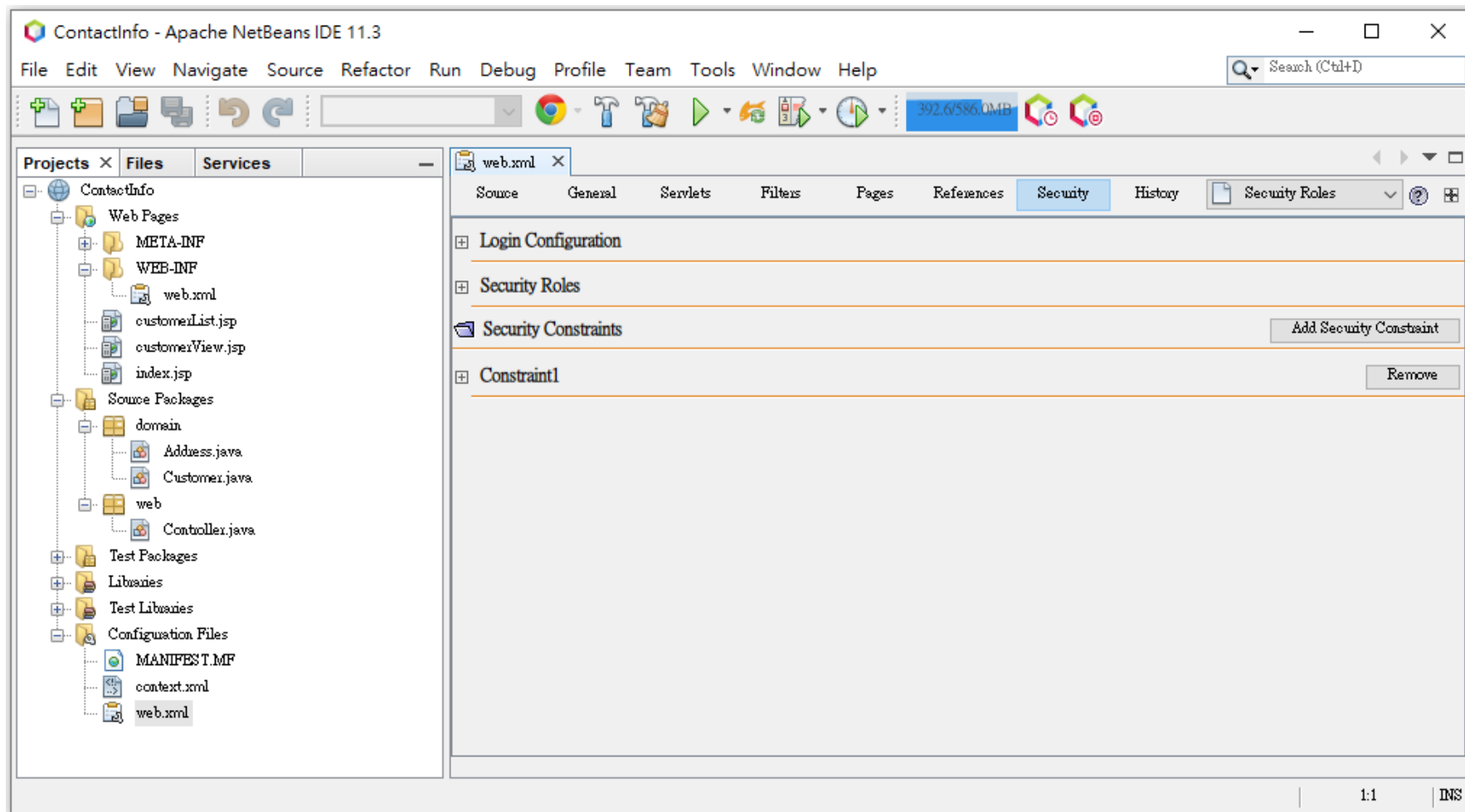
- 設定資源集合可操作之安全性角色

- ❑ 勾選 Enable Authentication Constraints

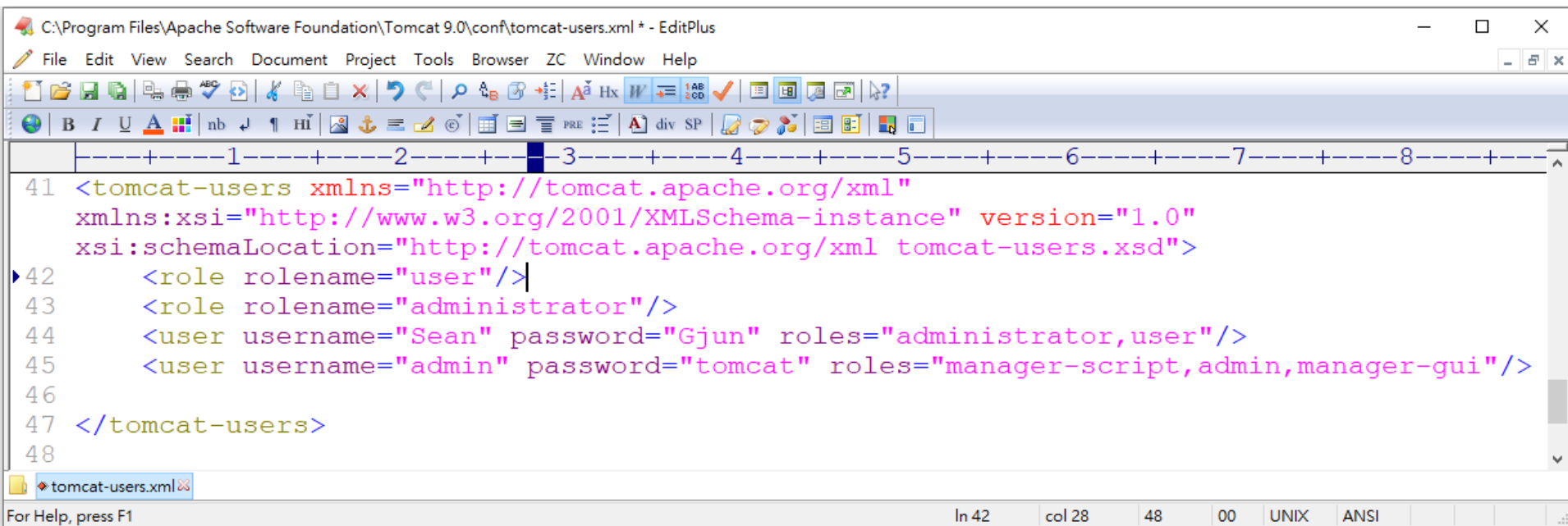
- ❑ 編輯 Role Name, 輸入 user

- 測試、執行

開啟 ContactInfo 網路應用專案

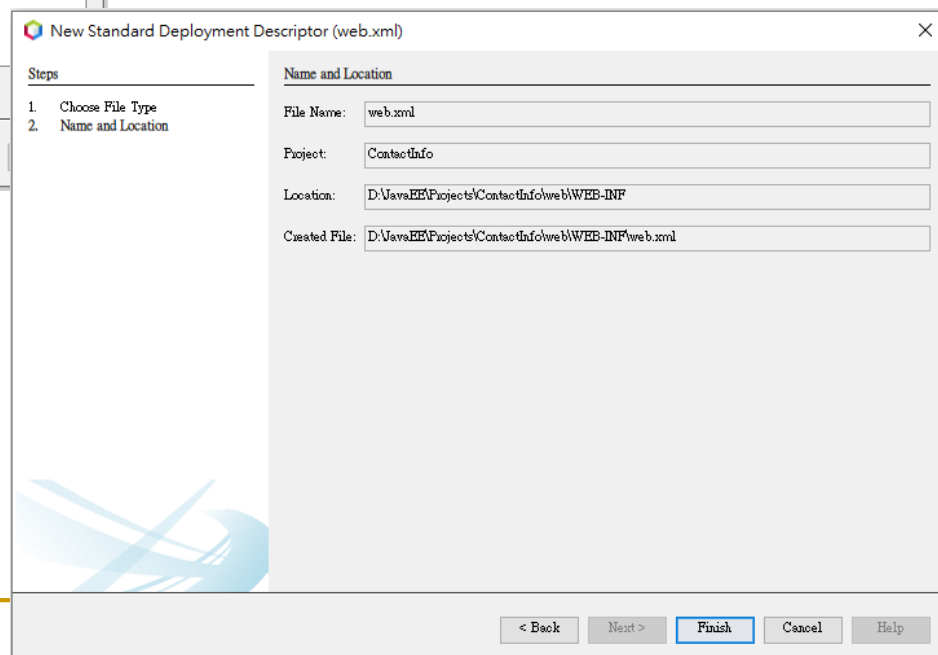
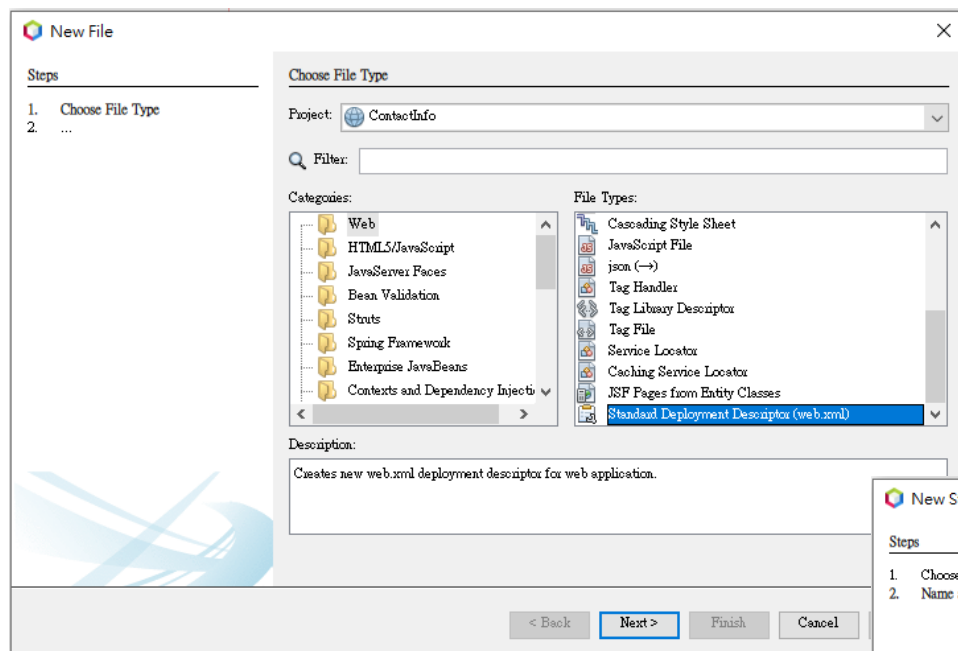


Tomcat中設定腳色及使用者帳號

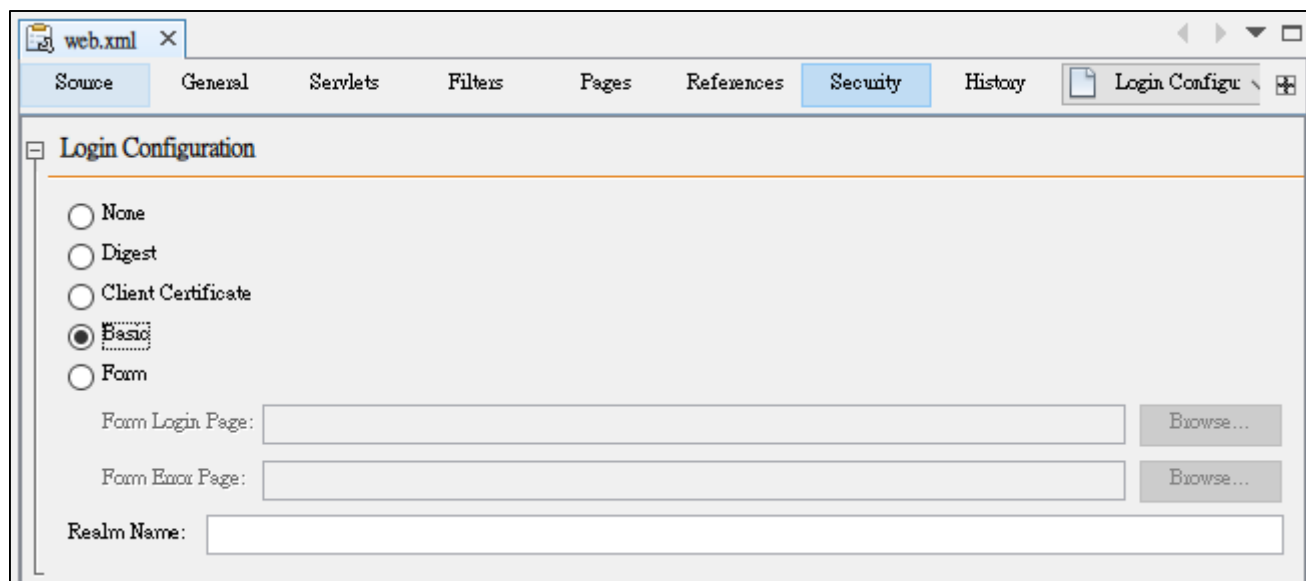


```
C:\Program Files\Apache Software Foundation\Tomcat 9.0\conf\tomcat-users.xml * - EditPlus
File Edit View Search Document Project Tools Browser ZC Window Help
-----1-----2-----3-----4-----5-----6-----7-----8-----
41 <tomcat-users xmlns="http://tomcat.apache.org/xml"
42     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="1.0"
43     xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd">
44     <role rolename="user"/>
45     <role rolename="administrator"/>
46     <user username="Sean" password="Gjun" roles="administrator,user"/>
47     <user username="admin" password="tomcat" roles="manager-script,admin,manager-gui"/>
48 </tomcat-users>
tomcat-users.xml
For Help, press F1
In 42 col 28 48 00 UNIX ANSI
```

新增部署描述檔



設定身份驗證模式



The screenshot shows an IDE window titled "web.xml" with several tabs: Source, General, Servlets, Filters, Pages, References, Security, History, and Login Configur... The Security tab is active, displaying the "Login Configuration" section. This section contains five radio buttons for authentication modes: None, Digest, Client Certificate, Basic (which is selected), and Form. Below these are two text input fields: "Form Login Page:" and "Form Error Page:", each followed by a "Browse..." button. At the bottom, there is a "Realm Name:" label followed by a text input field.

web.xml

Source General Servlets Filters Pages References Security History Login Configur...

Login Configuration

☐ None
☐ Digest
☐ Client Certificate
☒ Basic
☐ Form

Form Login Page: Browse...

Form Error Page: Browse...

Realm Name:

宣告安全性腳色

The screenshot shows the 'Security' tab for a 'web.xml' file. The 'Login Configuration' section has radio buttons for 'None', 'Digest', 'Client Certificate', 'Basic' (selected), and 'Form'. Below these are text fields for 'Form Login Page:', 'Form Error Page:', and 'Realm Name:'. The 'Security Roles' section contains a table with columns 'Role Name' and 'Description'. Below the table are buttons for 'Add...', 'Edit...', and 'Remove'. The 'Add...' button is circled in red. At the bottom, there is a section for 'Security Constraints' with an 'Add Security Constraint' button.

web.xml

Source General Servlets Filters Pages References Security History Security Roles

Login Configuration

☐ None
☐ Digest
☐ Client Certificate
☒ Basic
☐ Form

Form Login Page:
Form Error Page:
Realm Name:

Security Roles

Role Name	Description
<input type="button" value="Add..."/>	<input type="button" value="Edit..."/>
<input type="button" value="Remove"/>	

Security Constraints

The 'Add Security Role' dialog box has a title bar with a close button. It contains two input fields: 'Role Name' with the text 'user' and 'Description' which is empty. At the bottom right are 'OK' and 'Cancel' buttons.

Add Security Role

Role Name: user
Description:

新增安全性限制

The screenshot shows the 'Security' tab of a web.xml configuration file. The 'Login Configuration' section has radio buttons for 'None', 'Digest', 'Client Certificate', 'Basic' (selected), and 'Form'. Below these are fields for 'Form Login Page' and 'Form Error Page', each with a 'Browse...' button. The 'Realm Name' field is also present. The 'Security Roles' section contains a table with one role named 'user'. At the bottom, the 'Security Constraints' section has a red circle around the 'Add Security Constraint' button.

web.xml

Source General Servlets Filters Pages References Security History Security Roles

Login Configuration

☐ None
☐ Digest
☐ Client Certificate
☒ Basic
☐ Form

Form Login Page: Browse...

Form Error Page: Browse...

Realm Name:

Security Roles

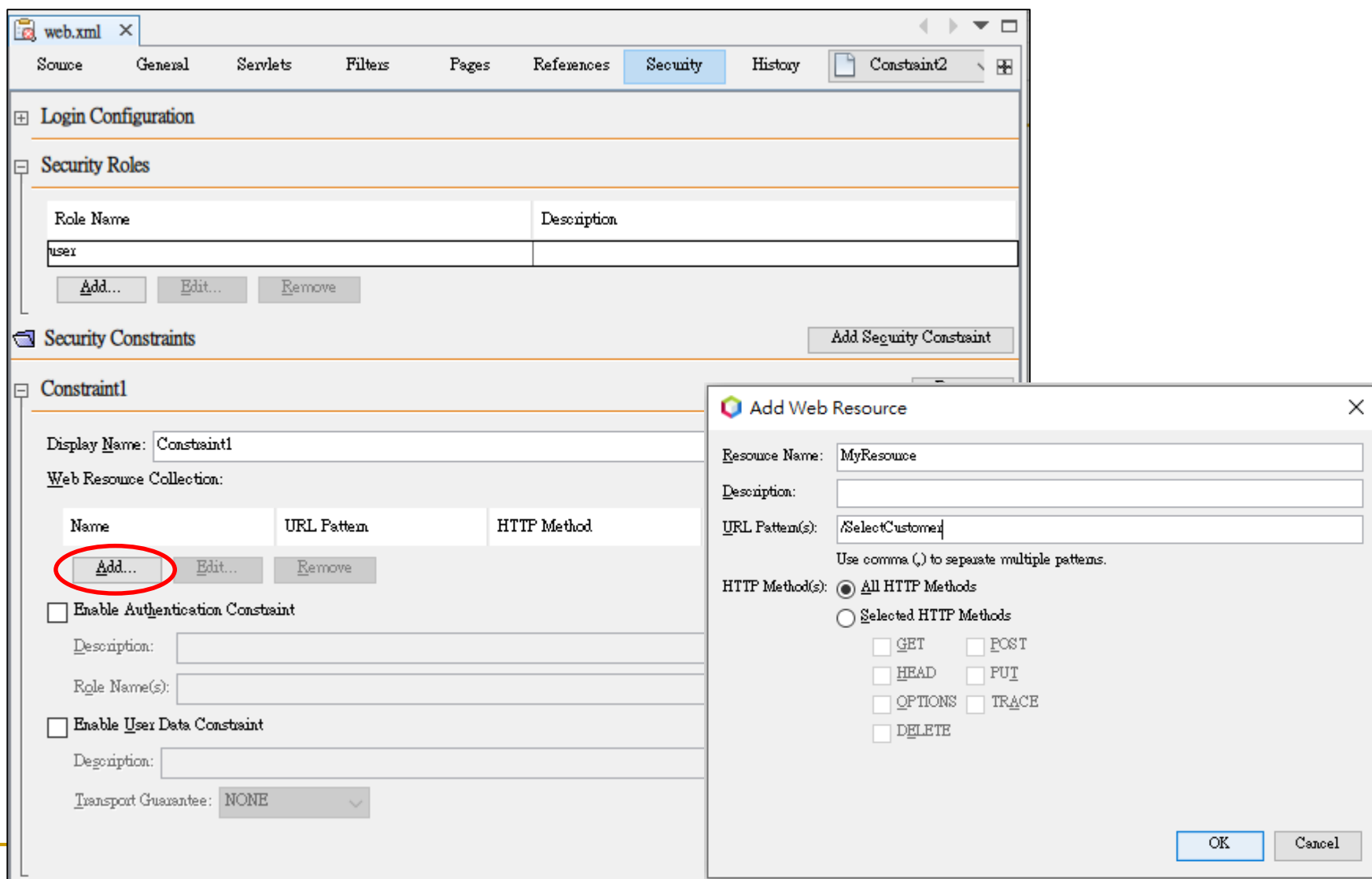
Role Name	Description
user	

Add... Edit... Remove

Security Constraints

Add Security Constraint

新增網路資源集合



宣告身分驗證限制條件

The screenshot shows the Eclipse IDE with the `web.xml` file open. The **General** tab is selected, showing the **Security Roles** section. A table lists the role `user`. Below it, the **Security Constraints** section shows a constraint named `Constraint1` with a display name of `Constraint1` and a web resource collection containing `MyResource` with URL pattern `/SelectCustomer`. The **Enable Authentication Constraint** checkbox is checked and circled in red. The **Edit** button for this constraint is also circled in red. An **Edit Role Names** dialog is open, showing the `user` role in the **All Roles** list on the right. The **Add >** button is highlighted with a dashed blue border.

web.xml **General** **Servlets** **Filters** **Pages** **References** **Security**

Login Configuration

Security Roles

Role Name	Description
user	

Add... **Edit...** **Remove**

Security Constraints

Constraint1

Display Name: `Constraint1`

Web Resource Collection:

Name	URL Pattern	HTTP Method
MyResource	/SelectCustomer	

Add... **Edit...** **Remove**

☒ **Enable Authentication Constraint**

Description:

Role Name(s):

☐ **Enable User Data Constraint**

Description:

Transport Guarantee: **NONE**

Edit

Edit Role Names

All Roles

user

Add >

< Remove

OK **Cancel**

web.xml

SourceGeneralServletsFiltersPagesReferencesSecurityHistory

Constraint1

Login Configuration

☐None

☐Digest

☐Client Certificate

☒Basic

☐Form

Form Login Page:

Form Error Page:

Realm Name:

Security Roles

Role Name	Description
user	

Add...

Edit...

Remove

Security Constraints

Add

Constraint1

Display Name: Constraint1

Web Resource Collection:

Name	URL Pattern	HTTP Method	Description
MyResource	/SelectCustomer		

Add...

Edit...

Remove

☒ Enable Authentication Constraint

Description:

Role Name(s): user

☐ Enable User Data Constraint

Description:


Transport Guarantee: NONE

web.xml

SourceGeneralServletsFiltersPagesReferencesSecurityHistory

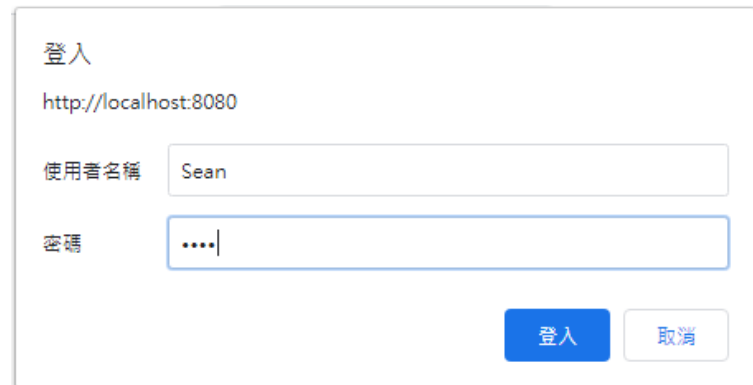
```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <web-app version="3.1" xmlns="http://xmlns.jcp.org/xml/ns/javaee"
3
4   <session-config>
5     <session-timeout>
6       30
7     </session-timeout>
8   </session-config>
9   <security-constraint>
10     <display-name>Constraint1</display-name>
11     <web-resource-collection>
12       <web-resource-name>MyResource</web-resource-name>
13       <description/>
14       <url-pattern>/SelectCustomer</url-pattern>
15     </web-resource-collection>
16     <auth-constraint>
17       <description/>
18       <role-name>user</role-name>
19     </auth-constraint>
20   </security-constraint>
21   <login-config>
22     <auth-method>BASIC</auth-method>
23   </login-config>
24   <security-role>
25     <description/>
26     <role-name>user</role-name>
27   </security-role>
28 </web-app>
```

測試、執行



客戶查詢

輸入客戶編號(輸入0查詢所有客戶):



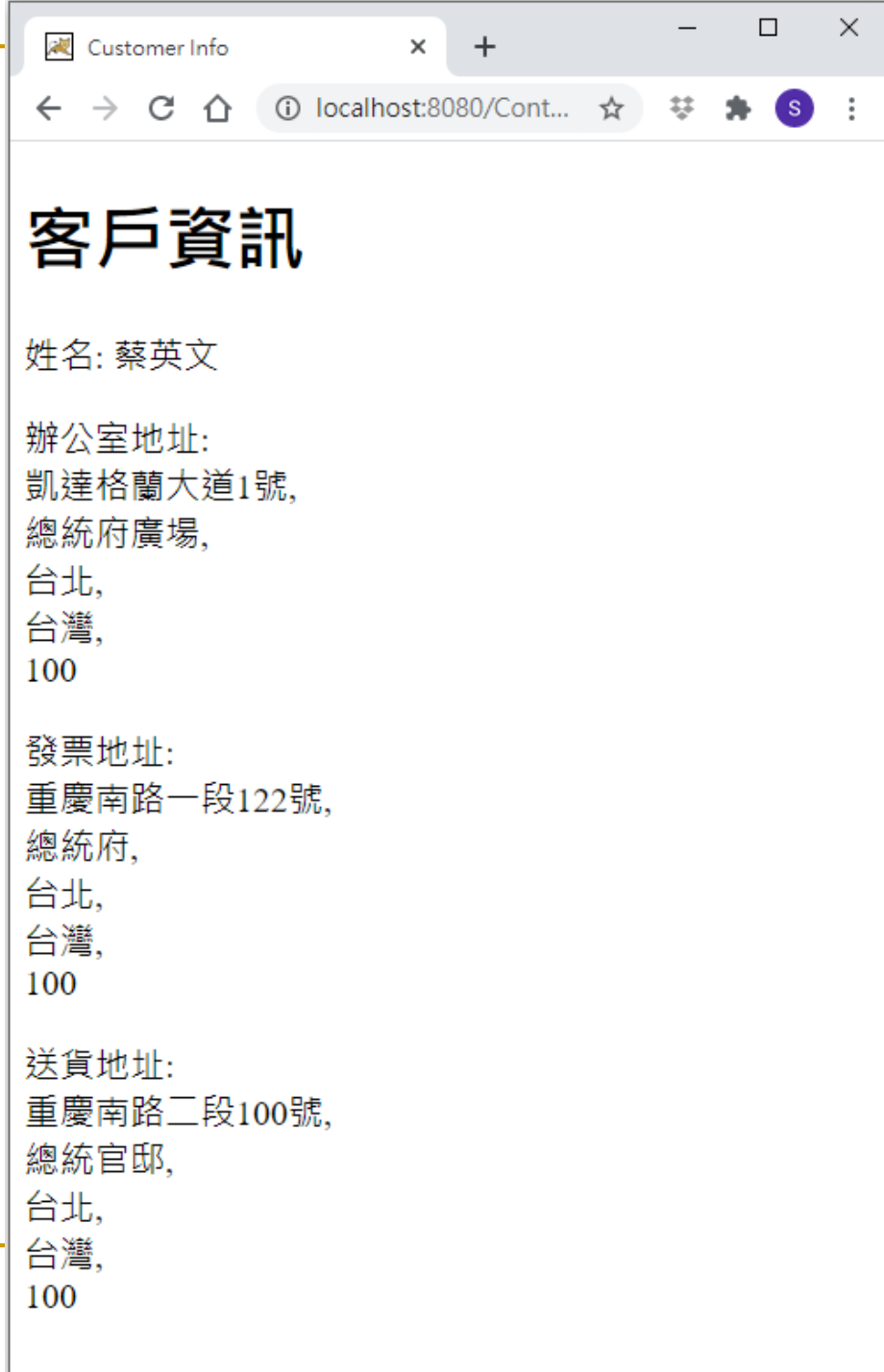
登入

http://localhost:8080

使用者名稱

密碼

測試、執行



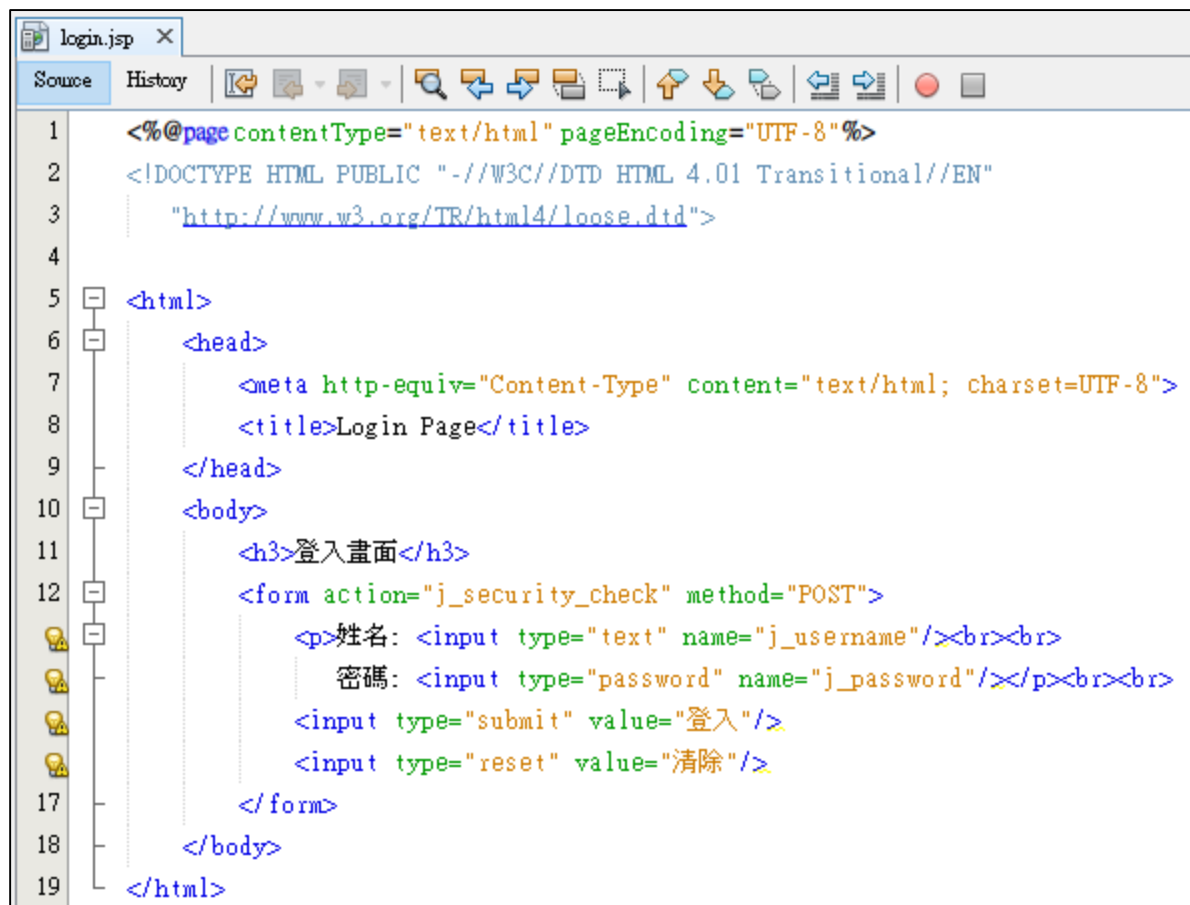
Lab 2

- 修改登入機制，使用自訂登入畫面
 - 新增 login.jsp
 - Form Action = “j_security_check”
 - User Name 欄位名稱為 j_username
 - Password欄位,名稱為j_password
 - 提供 submit 及 reset 按鈕, 分別顯示為 login 及 clear
 - 編輯 web.xml, 使用 login.jsp 作為登入頁面
 - 展開Login Configuration, 選擇 form
 - Form Login Page 選擇 login.jsp
 - Form Error Page 也選擇 login.jsp

Lab 2

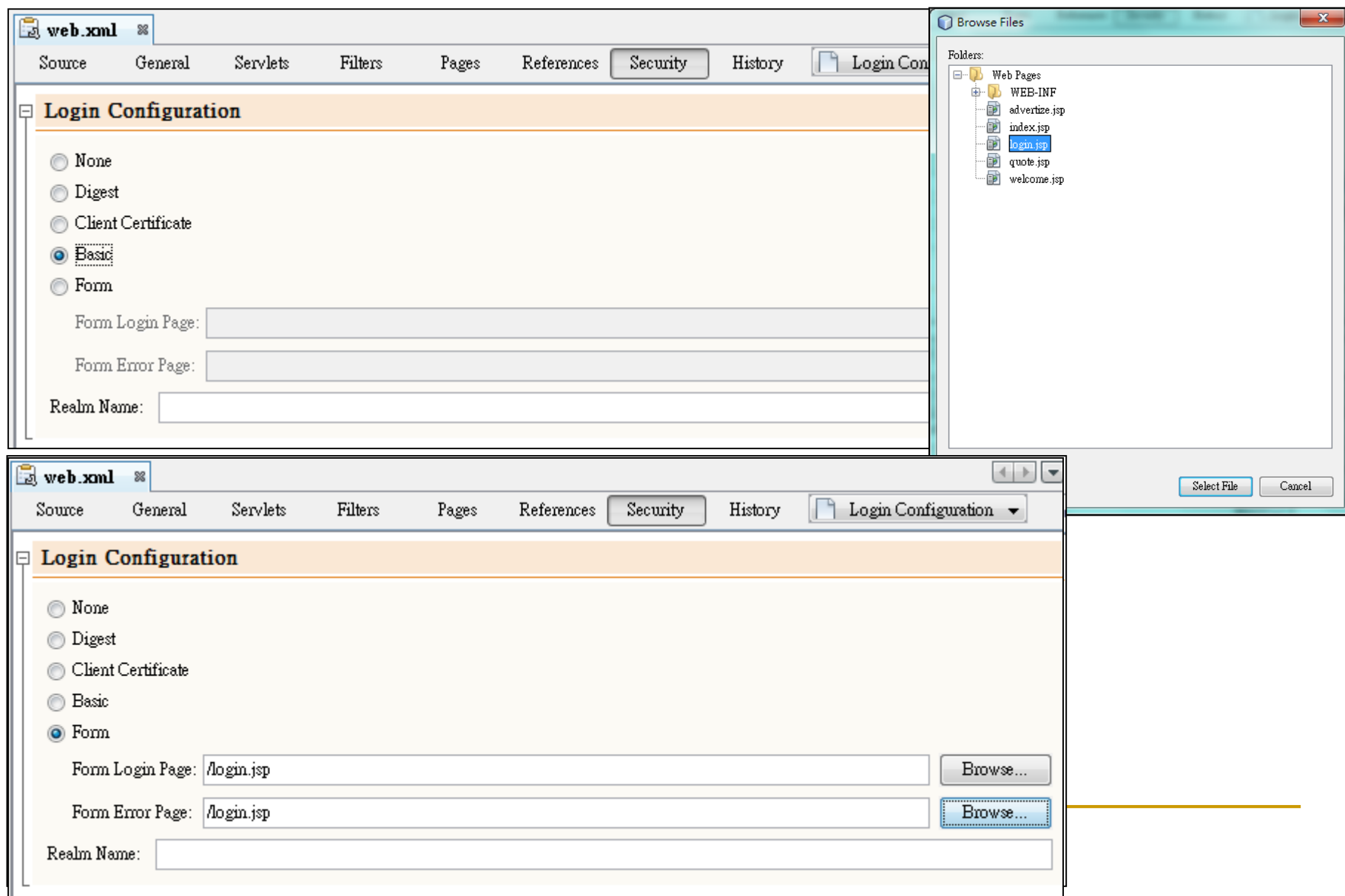
- 取得使用者登入名稱
 - 修改 `web.Controller.java`
 - 取得session 物件
 - 若session中無user屬性
 - 由request請求中取得UserPrincipal物件,
 - 由Principal物件取得name
 - 加入session屬性(user, name)
 - 修改 `customerList.jsp` 及 `customerView.jsp` 檔案
 - 在內容之前,顯示問候user資訊
- 測試、執行

使用自訂登入畫面 – login.jsp

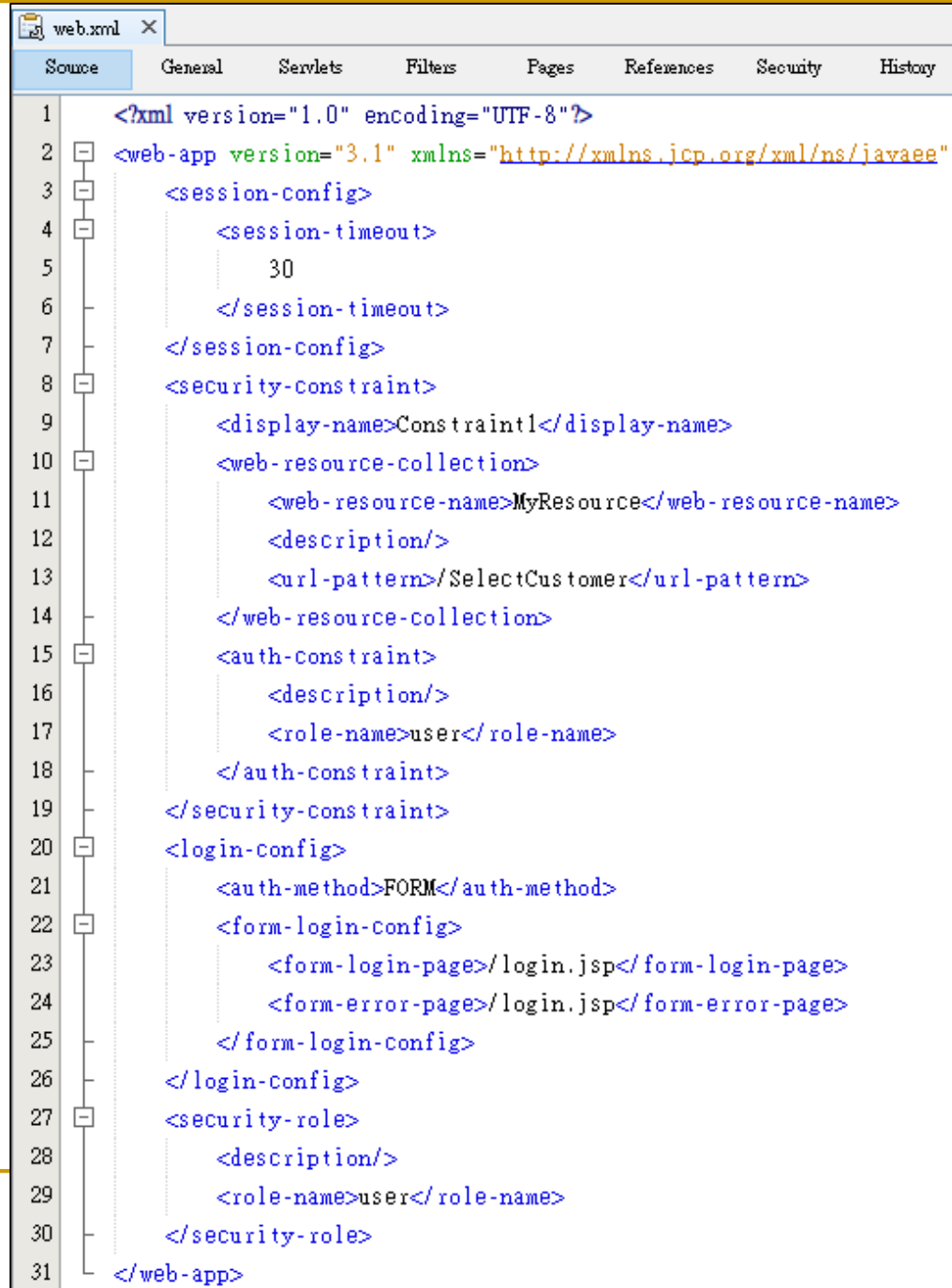


```
1 <%@page contentType="text/html" pageEncoding="UTF-8"%>
2 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
3   "http://www.w3.org/TR/html4/loose.dtd">
4
5 <html>
6   <head>
7     <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
8     <title>Login Page</title>
9   </head>
10  <body>
11    <h3>登入畫面</h3>
12    <form action="j_security_check" method="POST">
13      <p>姓名: <input type="text" name="j_username"/><br><br>
14        密碼: <input type="password" name="j_password"/></p><br><br>
15        <input type="submit" value="登入"/>
16        <input type="reset" value="清除"/>
17    </form>
18  </body>
19 </html>
```

設定自訂登入畫面

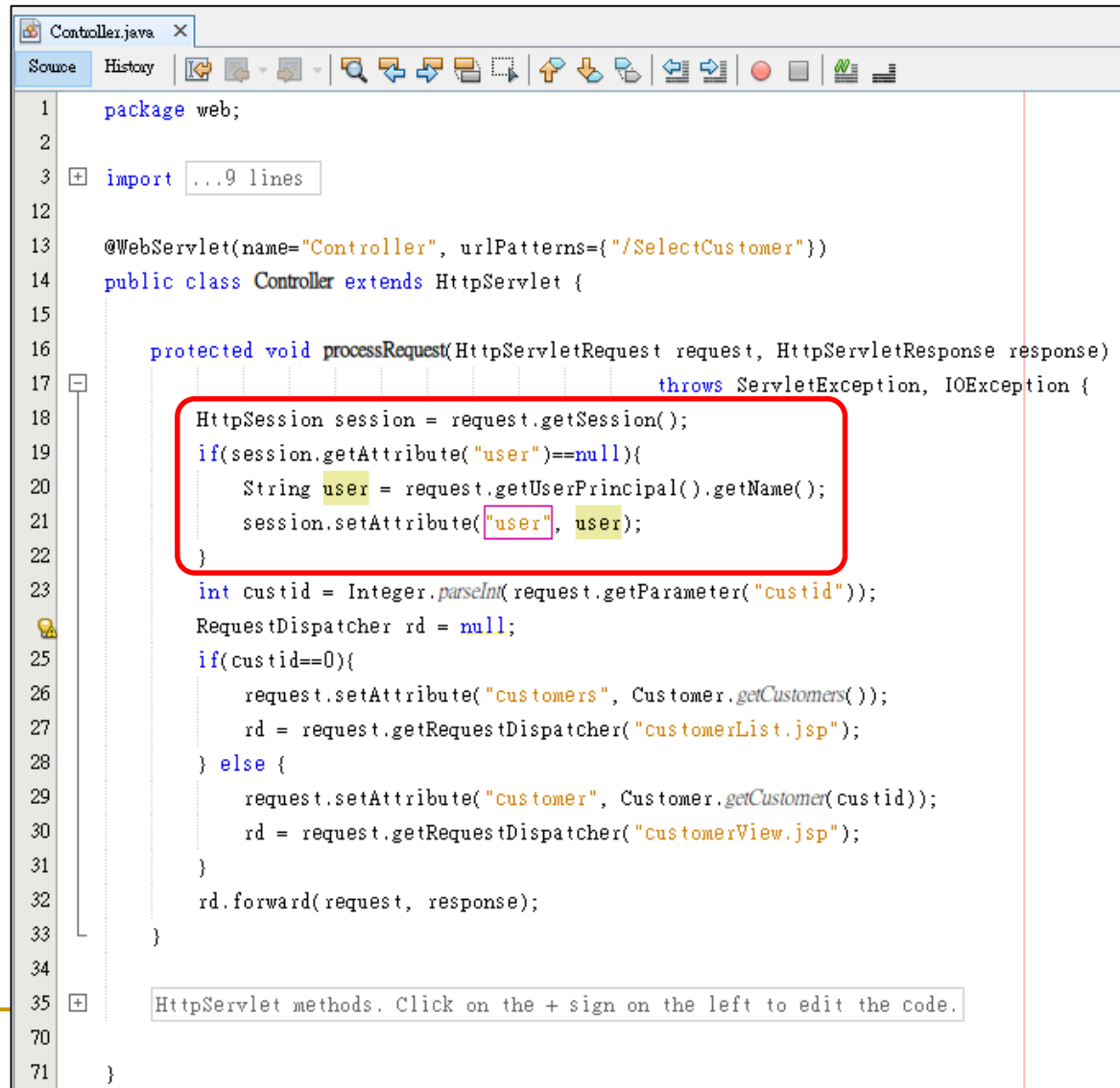


web.xml



```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <web-app version="3.1" xmlns="http://xmlns.jcp.org/xml/ns/javaee"
3 <session-config>
4 <session-timeout>
5 30
6 </session-timeout>
7 </session-config>
8 <security-constraint>
9 <display-name>Constraint1</display-name>
10 <web-resource-collection>
11 <web-resource-name>MyResource</web-resource-name>
12 <description/>
13 <url-pattern>/SelectCustomer</url-pattern>
14 </web-resource-collection>
15 <auth-constraint>
16 <description/>
17 <role-name>user</role-name>
18 </auth-constraint>
19 </security-constraint>
20 <login-config>
21 <auth-method>FORM</auth-method>
22 <form-login-config>
23 <form-login-page>/login.jsp</form-login-page>
24 <form-error-page>/login.jsp</form-error-page>
25 </form-login-config>
26 </login-config>
27 <security-role>
28 <description/>
29 <role-name>user</role-name>
30 </security-role>
31 </web-app>
```

web.Controller.java



```
1 package web;
2
3 import ...9 lines
4
12
13 @WebServlet(name="Controller", urlPatterns={"/SelectCustomer"})
14 public class Controller extends HttpServlet {
15
16     protected void processRequest(HttpServletRequest request, HttpServletResponse response)
17         throws ServletException, IOException {
18         HttpSession session = request.getSession();
19         if(session.getAttribute("user")==null){
20             String user = request.getUserPrincipal().getName();
21             session.setAttribute("user", user);
22         }
23         int custid = Integer.parseInt(request.getParameter("custid"));
24         RequestDispatcher rd = null;
25         if(custid==0){
26             request.setAttribute("customers", Customer.getCustomers());
27             rd = request.getRequestDispatcher("customerList.jsp");
28         } else {
29             request.setAttribute("customer", Customer.getCustomer(custid));
30             rd = request.getRequestDispatcher("customerView.jsp");
31         }
32         rd.forward(request, response);
33     }
34
35     HttpServlet methods. Click on the + sign on the left to edit the code.
36
70
71 }
```

customerView.jsp

```
customerView.jsp x
Source History
1 <%@page contentType="text/html" pageEncoding="UTF-8"%>
2 <%@taglib prefix="c" uri="http://java.sun.com/jsp/jstl/core"%>
3
4 <!DOCTYPE html>
5 <html>
6 <head>
7     <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
8     <title>Customer Info</title>
9 </head>
10 <body>
11     <h3>${user}, 你好!</h3>
12     <h3>客戶資訊</h3>
```


```
13
14
15
16
17
18
19
20
21
22
23
24
<c:choose>
    <c:when test = "${not empty customer}">
        <p>姓名: ${customer.name}</p>
        <cif test = "${not empty customer.officeAddress}">
            <p>辦公室地址:<br>
                ${customer.officeAddress.address1},<br>
                ${customer.officeAddress.address2},<br>
                ${customer.officeAddress.city},<br>
                ${customer.officeAddress.country},<br>
                ${customer.officeAddress.postcode}<br>
            </p>
        </cif>
        <cif test = "${customer.billingAddress ne null}">
            <p>發票地址:<br>
                ${customer["billingAddress"].address1},<br>
                ${customer["billingAddress"].address2},<br>
                ${customer["billingAddress"].city},<br>
                ${customer["billingAddress"].country},<br>
                ${customer["billingAddress"].postcode}<br>
            </p>
        </cif>
        <cif test = "${not empty customer.addresses[2]}">
            <p>送貨地址:<br>
                ${customer.addresses[2].address1},<br>
                ${customer.addresses[2].address2},<br>
                ${customer.addresses[2].city},<br>
                ${customer["addresses"][2].country},<br>
                ${customer["addresses"][2].postcode}<br>
            </p>
        </cif>
    </c:when>
    <c:otherwise>
        <h3>查詢的客戶不存在</h3>
    </c:otherwise>
</c:choose>
</body>
</html>
```

customerList.jsp

```
customerList.jsp x
Source History
1 <%@page contentType="text/html" pageEncoding="UTF-8"%>
2 <%@ taglib prefix="c" uri="http://java.sun.com/jsp/jstl/core" %>
3 <!DOCTYPE html>
4 <html>
5 <head>
6 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
7 <title>Customer List</title>
8 </head>
9 <body>
10 <h3>${user}, 你好!</h3>
11 <h3>客戶列表</h3>
```

```
12
13
14
15
16
17
18
19
20
21
22
23
24
<c:choose>
  <c:when test = "${not empty customers}">
    <c:forEach var="customer" items="${customers}">
      <p>姓名: ${customer.name}</p>
      <cif test = "${not empty customer.officeAddress}">
        <p>辦公室地址:
          ${customer.officeAddress.address1},
          ${customer.officeAddress.address2},
          ${customer.officeAddress.city},
          ${customer.officeAddress.country},
          ${customer.officeAddress.postcode}
        </p>
      </cif>
      <cif test = "${customer.billingAddress ne null}">
        <p>發票地址:
          ${customer["billingAddress"].address1},
          ${customer["billingAddress"].address2},
          ${customer["billingAddress"].city},
          ${customer["billingAddress"].country},
          ${customer["billingAddress"].postcode}
        </p>
      </cif>
      <cif test = "${not empty customer.addresses[2]}">
        <p>送貨地址:
          ${customer.addresses[2].address1},
          ${customer.addresses[2].address2},
          ${customer.addresses[2].city},
          ${customer["addresses"][2].country},
          ${customer["addresses"][2].postcode}
        </p>
      </cif>
    </c:forEach>
  </c:when>
  <c:otherwise>
    <h3>無客戶存在</h3>
  </c:otherwise>
</c:choose>
</body>
</html>
```

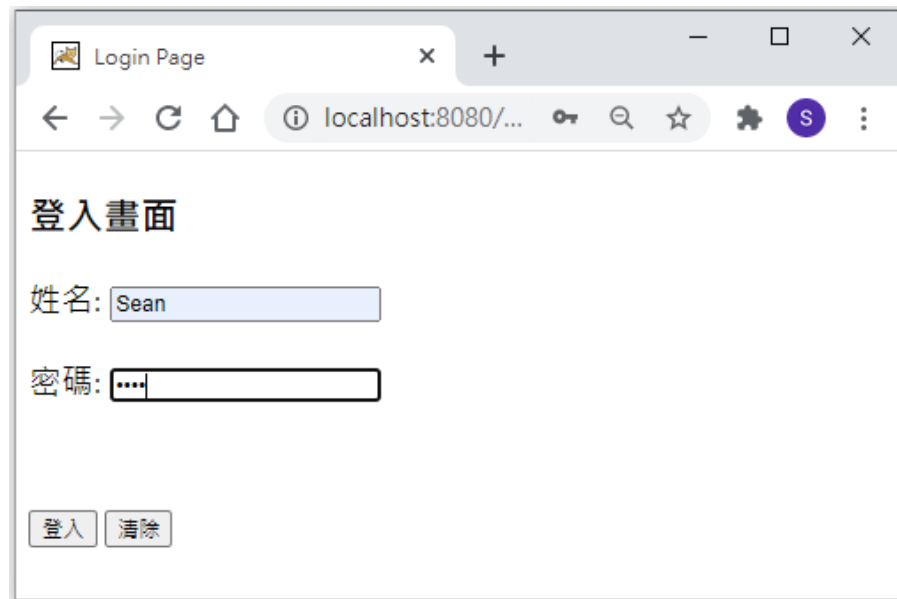
測試、執行



客戶查詢

輸入客戶編號(輸入0查詢所有客戶): 1

提交



登入畫面

姓名: Sean

密碼:

登入 清除

測試、執行

