**Dharmsinh Desai University, Nadiad**

**Department of Information Technology**

**Advanced Java Technology, IT619**

**B.Tech. IT, Sem: VI**

**Experiment – 08**

**Submitted By**

**Roll No.:IT076**

**Name:Dishant Modh**

**Aim:**  Write steps to provide Basic Authentication to a Web Application. The

application has two secure directories (secureAdmin and secureUser) corresponding to

two users – Admin and User. Theapplication has two html files: (i) pageA.html

under SecureAdmin directory and (ii) pageU.html under secureUser directory.

**Code:-**

**Steps:**

**· Creating Web Project Setup:**

**1. Create a New Java Web Project.**

**2. Under Web Pages directory create new folders with name secureAdmin and secureUser.**

**3. Under secureAdmin directory create pageA.html, under secureUser directory create pageU.html and under Web Pages directory create index.html and provide link of pageA.html and pageU.html**

**· Server Configurations Setup:**

**1. Now, Services > Server, right click on Glassfish Server and start server.**

**2. Right Click the Glassfish server and select View Domain Admin Console.**

**3. Now, goto Configuration > server-config > security > Realms > file, click Manage Users and two users one for admin and second for user.**

**· Setup for web.xml:**

**1. Now, goto Configuration Files, add web.xml file if not present.**

**2. Goto Security > Login Configuration, select Basic radio button and enter file in Realm Name.**

**3. Goto Security Role and add Role Name Admin and User.**

**4. Goto Security Constraints > Add Security constraint, add constraints for both Admin and User**

**5. Now, add constraint name, after this press add button of Web Resource Collection.**

**6. Give resource name, url pattern(for admin:/secureAdmin/\* and user:/secureUser/\*) and select appropriate HTTP methods and hit OK.**

**7. Now, check Enable Authentication constraint and select Role Name.**

**· Setup for Application server based web.xml(glassfish-web.xml):**

**1. Now, goto Configuration Files, add glassfish-web.xml if not present.**

**2. Goto Security > Security Role Mapping, click Add Security Role Mapping.**

**3. Give Security Role Name(Admin and User) and add principal which is created when we configure the server and save the file.**

**· Now, clean and build the project, deploy the project and test the project.**

1. **web.xml**

<?xml version="1.0" encoding="UTF-8"?>

<web-app version="3.1" xmlns="http://xmlns.jcp.org/xml/ns/javaee" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee http://xmlns.jcp.org/xml/ns/javaee/web-app\_3\_1.xsd">

<session-config>

<session-timeout>

30

</session-timeout>

</session-config>

<security-constraint>

<display-name>adminConstraint1</display-name>

<web-resource-collection>

<web-resource-name>adminresource</web-resource-name>

<description/>

<url-pattern>/SecAdmin/\*</url-pattern>

</web-resource-collection>

<auth-constraint>

<description/>

<role-name>Admin</role-name>

</auth-constraint>

</security-constraint>

<security-constraint>

<display-name>userConstraint</display-name>

<web-resource-collection>

<web-resource-name>userresource</web-resource-name>

<description/>

<url-pattern>/SecUser/\*</url-pattern>

</web-resource-collection>

<auth-constraint>

<description/>

<role-name>User</role-name>

</auth-constraint>

</security-constraint>

<login-config>

<auth-method>BASIC</auth-method>

<realm-name>file</realm-name>

</login-config>

<security-role>

<description/>

<role-name>Admin</role-name>

</security-role>

<security-role>

<description/>

<role-name>User</role-name>

</security-role>

</web-app>

1. **glassfish-web.xml**

<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE glassfish-web-app PUBLIC "-//GlassFish.org//DTD GlassFish Application Server 3.1 Servlet 3.0//EN" "http://glassfish.org/dtds/glassfish-web-app\_3\_0-1.dtd">

<glassfish-web-app error-url="">

<security-role-mapping>

<role-name>Admin</role-name>

<principal-name>testadmin</principal-name>

</security-role-mapping>

<security-role-mapping>

<role-name>User</role-name>

<principal-name>testuser</principal-name>

<principal-name>testadmin</principal-name>

</security-role-mapping>

<class-loader delegate="true"/>

<jsp-config>

<property name="keepgenerated" value="true">

<description>Keep a copy of the generated servlet class' java code.</description>

</property>

</jsp-config>

</glassfish-web-app>

1. **pageA.html**

<!DOCTYPE html>

<html>

<head>

<title>Secure Admin</title>

<meta charset="UTF-8">

<meta name="viewport" content="width=device-width, initial-scale=1.0">

</head>

<body>

<div>Secure Admin Area</div>

</body>

</html>

1. **pageU.html**

<!DOCTYPE html>

<html>

<head>

<title>Secure User</title>

<meta charset="UTF-8">

<meta name="viewport" content="width=device-width, initial-scale=1.0">

</head>

<body>

<div>Secure User Area</div>

</body>

</html>

1. **index.html**

<!DOCTYPE html>

<html>

<head>

<title>Secure Application</title>

<meta charset="UTF-8">

<meta name="viewport" content="width=device-width, initial-scale=1.0">

</head>

<body>

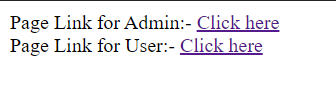
<div>Page Link for Admin:- <a href="SecAdmin/pageA.html">Click here</a></div>

<div>Page Link for User:- <a href="SecUser/pageU.html">Click here</a></div>

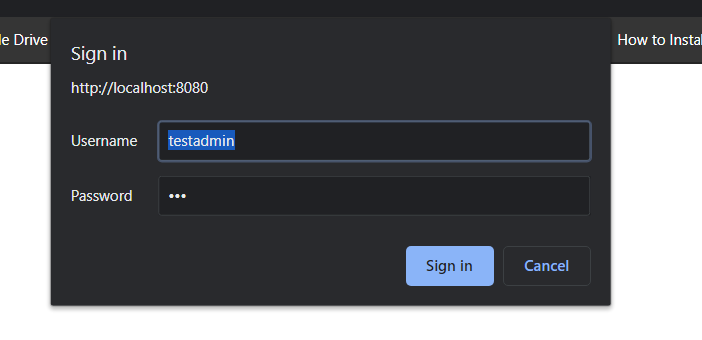
</body>

</html>

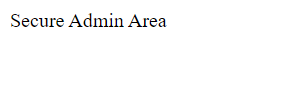
**Input/Output:**

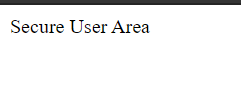
****

**1.1 Main Server**

****

**1.2 When we click on Admin**

****

****