A Sample J2EE App using Form Based Authentication and a Style Sheet

Mike Kearney

Lee-Win Tai

© Copyright IBM Corporation, 2007

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

AIX*
CICS*
e-business logo*
IBM*
IBM eServer
IBM logo*
IMS
OS/390*
RACF*
S/390*
WebSphere*
z/OS*
zSeries*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

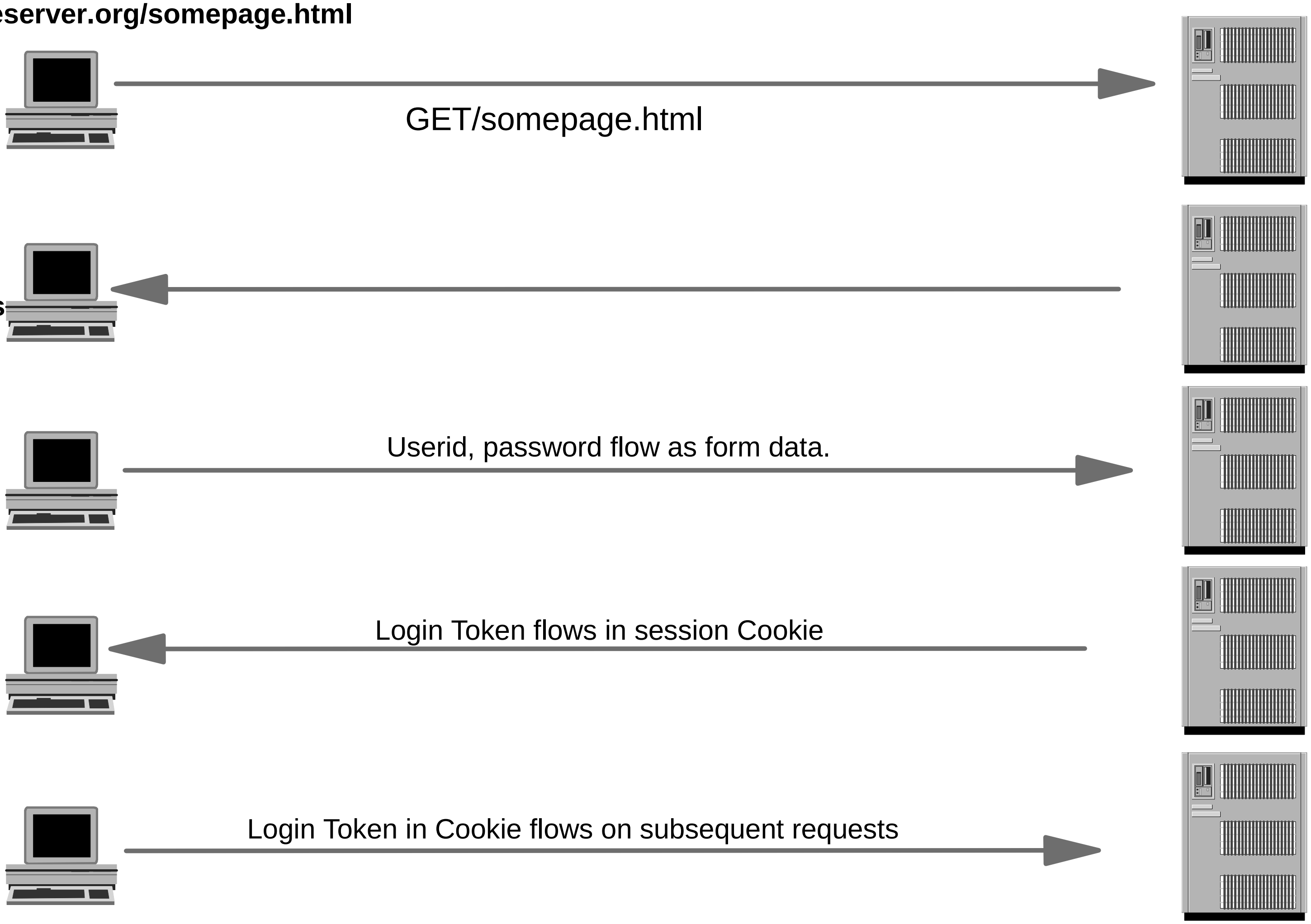
© Copyright IBM Corporation, 2007

This article describes how to configure a J2EE application to use Form Based Authentication (FBA), including a login page with a style sheet.

© Copyright IBM Corporation, 2007

WebSphere Application Server supports the J2EE standard for authentication called Form Based Authentication (FBA).

Client enters url at browser:
http://someserver.org/somepage.html



GET/somepage.html

Server determines that a userid, password are required.

User fills in userid, password, clicks submit button.

Server redirects client to login page with userid, password form. Server creates cookie with original url.

Userid, password flow as form data.

Server validates userid, password, creates Login Token, or error page.

Browser caches Cookie.

Login Token flows in session Cookie

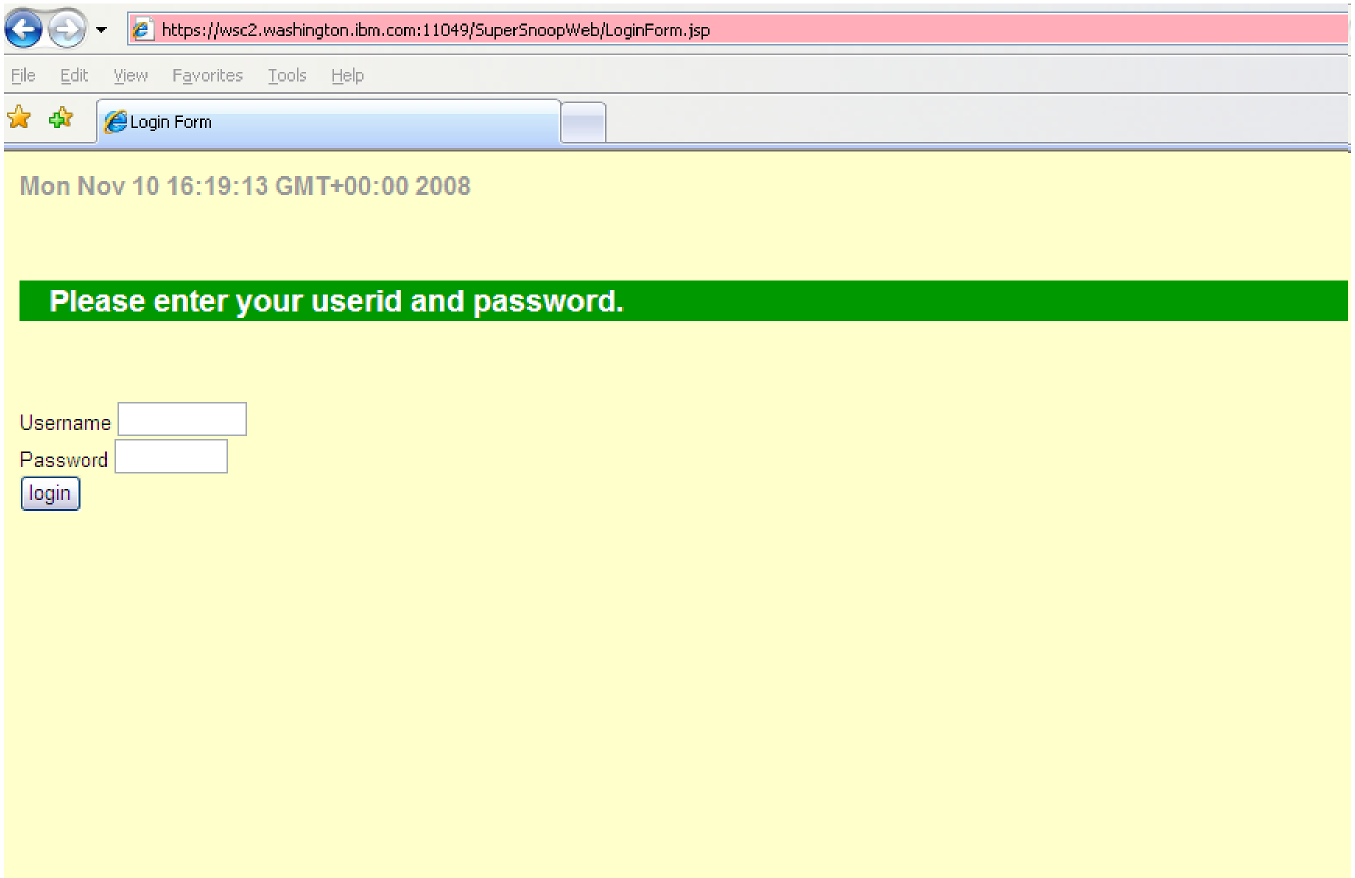
Server returns Login Token, redirects client to original url.

Login Token in Cookie flows on subsequent requests

Server processes Login Token, request.

© Copyright IBM Corporation, 2007

Form Based Authentication allows the Java developer to control the 'look and feel' of the login page.
A style sheet (.css file) controls the character set and background colors in this example:



https://wsc2.washington.ibm.com:11049/SuperSnoopWeb/LoginForm.jsp
File Edit View Favorites Tools Help
Login Form

Mon Nov 10 16:19:13 GMT+00:00 2008

Please enter your userid and password.

Username
Password

© Copyright IBM Corporation, 2007

A Checklist for Configuring FBA

1. Determine what Roles will be allowed to use your application.
2. Define RACF EJBROLE profiles to match your role names.
   - Include security domain name as a prefix.
   - EJBROLE profiles are case-sensitive.
   - Give users or groups READ access to the appropriate EJBROLE profile.
   - Raclist and refresh the EJBROLE class.

© Copyright IBM Corporation, 2007

A Checklist for Configuring FBA (cont.)

3. Create a Login page and an Error page
   - Form on Login Page must contain
     - j_username
     - j_password
   - Action on Login Form must be
     - j_security_check
   - Page can be HTML or a JSP.
4. Indicate that Form Based Authentication is Required.
   - Specify the name of your Login Page, Error Page.

© Copyright IBM Corporation, 2007

A Checklist for Configuring FBA (cont.)

5. Create a Security Constraint and Web Resource Collection to 'declare' each Applications security policy.
   - Specify URL(s) to be protected.
   - Specify HTTP methods to be protected.
   - Specify Role(s) authorized to access URLs.
6. Create a User Data Constraint with a Transport Guarantee of 'Confidential' to force the use of SSL for the Application. Optional but recommended to protect the userid/password.

© Copyright IBM Corporation, 2007

The style sheet is referenced from the login page html. In this example, the login page is LoginForm.jsp.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<HTML>
<HEAD>
<%@ page
language="java"
contentType="text/html; charset=UTF-8"
pageEncoding="UTF-8"
%>
<META http-equiv="Content-Type" content="text/html; charset=UTF-8">
<META name="GENERATOR" content="IBM WebSphere Studio">
<TITLE>Login Form</TITLE>
<link href='sample.css' rel="styleSheet" type="text/css">
</HEAD>
<BODY>
<h3><%= new java.util.Date() %></h3>
<br>
<br>
<H2>Please enter your userid and password.</H2>
<form method="post" action="j_security_check"><br>
<br>Username <input type="text" name="j_username" maxlength="8" size="8">
<br>Password <input type="password" name="j_password" maxlength="8" size="8">
<br><input type="submit" value="login"><BR>
</form>
</BODY>
</HTML>
```

To allow the style sheet, gif, jpeg, or other content to be displayed along with the login page, they must not be covered by the security constraint that protects the rest of the application.

You can accomplish this by creating a servlet mapping that maps the servlet url to a url protected by a security constraint. The login page and style sheet will remain unprotected, which is necessary for them to work properly.

Example on next page.

© Copyright IBM Corporation, 2007

In this example, taken from the web.xml file, the servlet url, SuperSnoop, is mapped to /secure/SuperSnoop. The url pattern in the security constraint protects /secure/*

```
- <servlet>
  <servlet-name>SuperSnoop</servlet-name>
  <display-name>SuperSnoop</display-name>
  <servlet-class>com.ibm.washington.SuperSnoop</servlet-class>
  </servlet>
```

mapping

```
- <servlet-mapping>
  <servlet-name>SuperSnoop</servlet-name>
  <url-pattern>/secure/SuperSnoop</url-pattern>
  </servlet-mapping>
- <security-constraint>
  <display-name>Manager</display-name>
- <web-resource-collection>
  <web-resource-name>Manager</web-resource-name>
  <description />
```

protected

```
  <url-pattern>/secure/*</url-pattern>
  <http-method>GET</http-method>
  <http-method>PUT</http-method>
  <http-method>HEAD</http-method>
  <http-method>TRACE</http-method>
  <http-method>POST</http-method>
  <http-method>DELETE</http-method>
  <http-method>OPTIONS</http-method>
  </web-resource-collection>
```

© Copyright IBM Corporation, 2007

A Checklist for Configuring FBA (cont.)

7. Link Servlet Roles (Programmatic security) to RACF Roles, if necessary.
8. Deploy the Application.

© Copyright IBM Corporation, 2007

About the sample .ear file.

- supersnoop-20081007-form.ear is configured to use FBA.
- It has no external data or application requirements. Just a working WebSphere Application Server V5, V6 or V7.
- It requires that users have the Manager role.
- It uses a transport guarantee to force the use of SSL.
- The url to access the application is: http://server/SuperSnoopWeb/secure/SuperSnoop

© Copyright IBM Corporation, 2007

Comments, Questions, Problems?:
Your feedback on this document will be greatly appreciated. Please direct all comments, questions or problems to:

Mike Kearney, c/o
IBM Corp.
Room 2K052
800 North Frederick Ave.
Gaithersburg, MD 20879

Or via email to kearney@us.ibm.com
Or via phone: (301) 240-3760

© Copyright IBM Corporation, 2007