Assignment 4: Secure Session Management

Students: Joanna C. S. Santos and Yue Hua

1. Domain

The application is a simple private blog Web site in which there are a posts (blog entries) that can be read by authenticated users. One requirement for this application is that only administrators can create new posts in the blog.

2. Design

The application has a MVC (Model-View-Controller) pattern in which the Servlet classes are the *controllers*, the JSP pages are the *views* and the *models* are the classes that communicates with a SQLite database for retrieving information related to user accounts and blog posts. Figure 1 shows the architecture of the application.

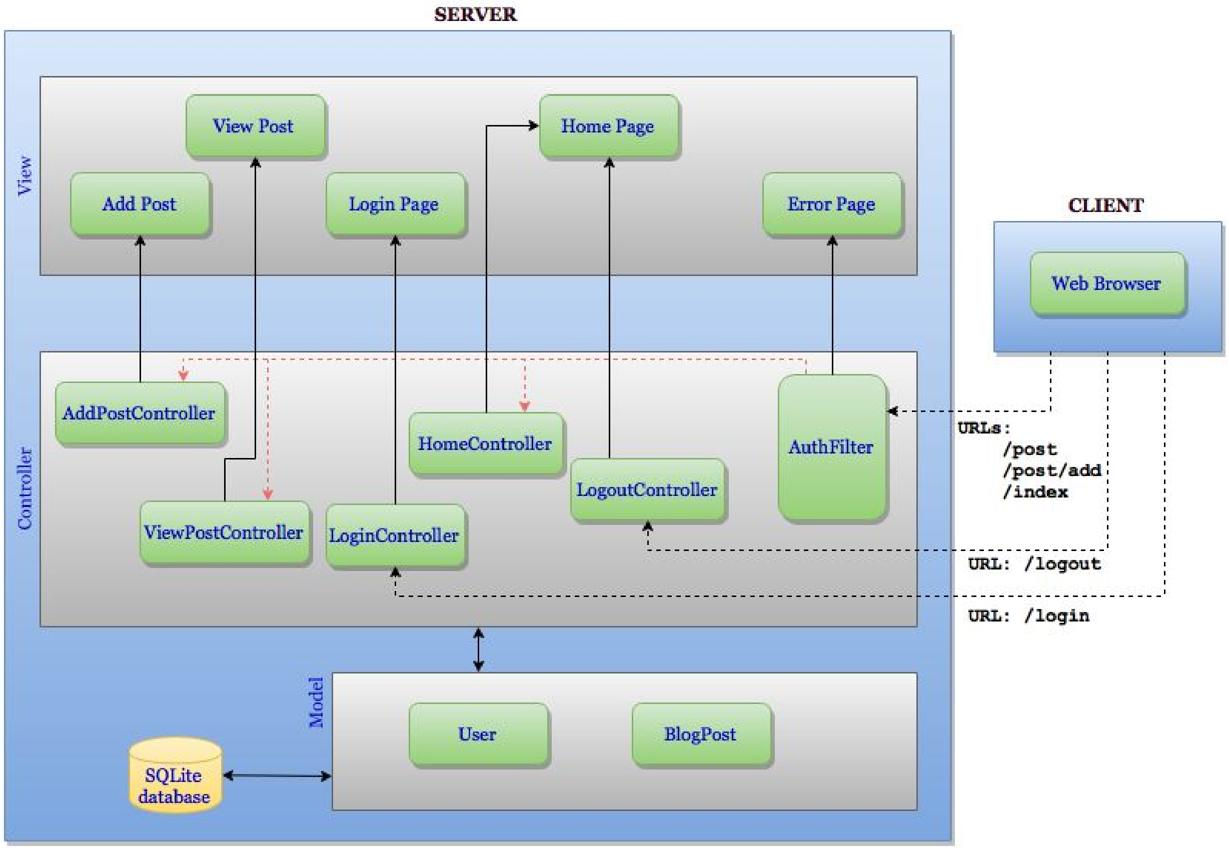


Figure 1: Web application architecture

To implement the secure session management, we used an object of the `HttpSession` (available in the JavaEE APIs). Thus, we stored the username of the logged in user in this session object.

The non-functional requirement of only authorized users can read and/or create blog posts was achieved through a Role-Based Access Control approach. To do so, we created a database which stores the following information for each user account: `id`, `role`, `username`, and `password`. The `role` is an integer that can be either be equals to `1` or `2` and identifies whether the user has an `admin` role or a `reader` role. , respectively.

To perform Authentication and Authorization in the Web application, we implemented a *Filter*, which intercepts requests directed to specific URLs (shown in Figure 1). This filter ensures that only administrators can create new blog posts and only authenticated users (`readers` or `admins`) can read blog posts. If the user is authorized to perform the task, the filter forwards the HTTP request to the appropriate controller (Servlet class). Otherwise, this filter will respond with a HTTP 403 error (*Forbidden Request*) and shows an error page.

3. Results

When users access the Web site, they are redirected to a login page in which they shall provide their username and password (Figure 2). After a successful login, a list of the blog posts is shown to the user (Figure 3).

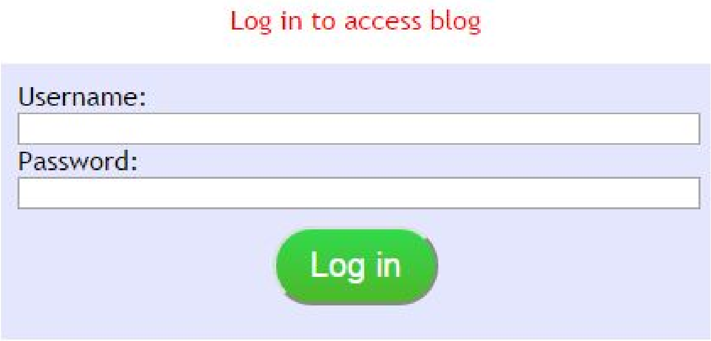
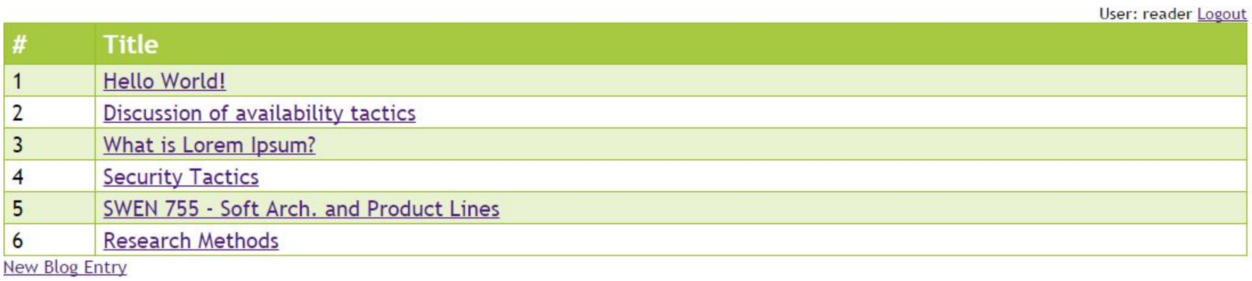


Figure 2: Login Web Page



User: reader Logout

#	Title
1	Hello World!
2	Discussion of availability tactics
3	What is Lorem Ipsum?
4	Security Tactics
5	SWEN 755 - Soft Arch. and Product Lines
6	Research Methods

New Blog Entry

Figure 3: Web Page for listing the posts of the blog

In the case the user is an `admin`, if the user clicks in “New Blog Entry”, it is going to open the Web page for creating a new Blog Post (Figure 4). If the user is a `reader`, however, an error message is displayed saying that the user cannot perform the task.

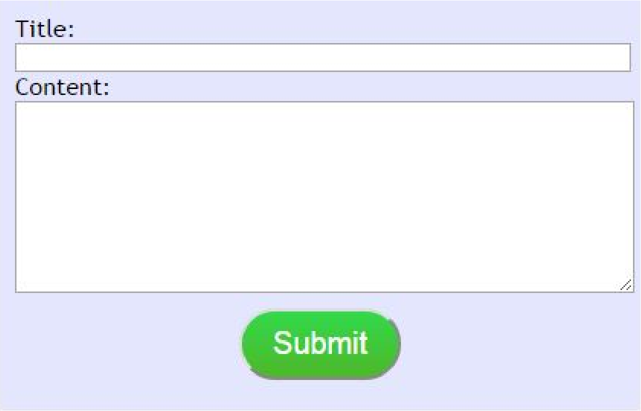


Figure 4: Web Page for creating a new blog post

To test the system, we created the user accounts presented in Table 1.

User Id	Role	Username	Password
1	READER	reader	123456
2	ADMIN	admin	123456
3	READER	joanna	123456
4	READER	yue	123456
5	ADMIN	john	123456

Table 1: User accounts created for testing the Secure Session Management