**Lab 6**

**Name:** Trần Gia Khôi

**ID:** ITITIU21231

**Exercise 5: Authentication Filter**

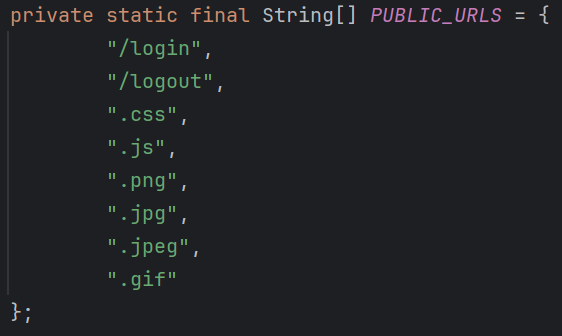
**Task 5.1: Create AuthFilter**

Filter intercepts all reques



In this line, by using urlPatterns = {“/\*”}, the filter ensures intercepts all requests

Public URLs allowed



This is a definition of public URLs

A screen shot of a computer code

AI-generated content may be incorrect.

Check whether *path* is a public URL or not. If it is then allow access to public URLs then return to prevent further execution.

Protected URLs blocked

A screen shot of a computer code

AI-generated content may be incorrect.

Firstly it will check session then ask whether user logged in or not. If user logged in then filter will allow access to the blocked URLs. If user did not log in, then simply redirect to login page.

Redirect to login works

A black background with white text

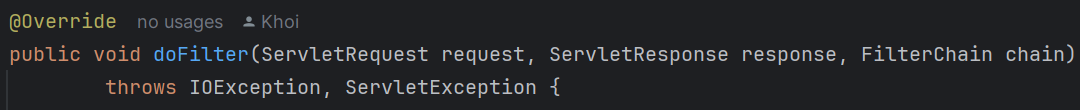
AI-generated content may be incorrect.

This is the part when users are redirected to login page

Filter properly configured







A black background with blue and orange text

AI-generated content may be incorrect.

Based on the WebFilter annotation and 3 methods, which are *init()*, *doFilter(),* and *destroy()* has been override and implemented, the filter has been correctly configured.

**Testing:**

A screenshot of a computer

AI-generated content may be incorrect.

I tried to access the “/student” without login and then hit Enter

A screenshot of a computer

AI-generated content may be incorrect.

It redirect me back to login page, since I am not authenticated at all.

A screenshot of a computer

AI-generated content may be incorrect.

And when I username and password to login and hit Enter

A screenshot of a computer

AI-generated content may be incorrect.

Then I can access “/student” perfectly

**Exercise 6: Admin Authorization Filter**

**Task 6.1: Create AdminFilter**

Filter checks admin role

A screen shot of a computer code

AI-generated content may be incorrect.

Firstly, it will get the session and check for the user. If user is an admin role, then allow access.

The *user.isAdmin()* is the key to verifies the admin role

Admin actions identified







A screenshot of a computer program

AI-generated content may be incorrect.

A computer screen with text

AI-generated content may be incorrect.

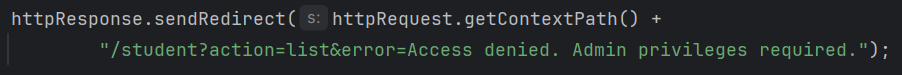
Firstly, it will define actions that only can be done by admin. Then the filter will get action from request and check whether that action requires admin.

Non-admin blocked correctly



In this case the filter see that there is no session, means that there are no user or user did not login yet, so it will redirect user back to the login page.

Error message displayed



By redirecting user back to the login page, it will also send an error message, which is “Access denied…”.

**Testing**

A screenshot of a computer

AI-generated content may be incorrect.

In this case, I logged in as admin and the “Edit” and “Delete” button is show

A screenshot of a computer

AI-generated content may be incorrect.

I delete student “Nguyen Duc Anh”

A screenshot of a computer

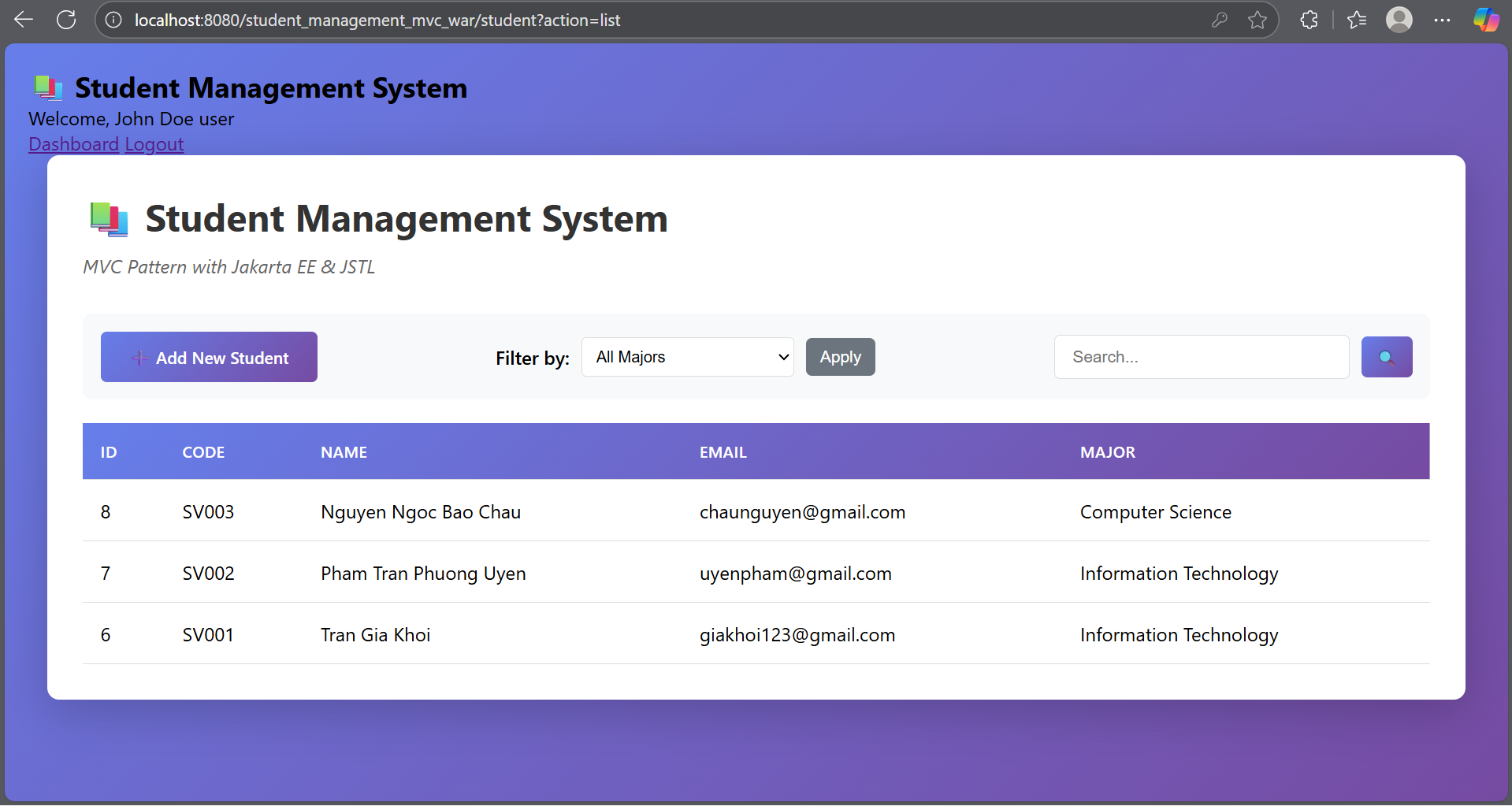
AI-generated content may be incorrect.

It works perfectly

A screenshot of a computer screen

AI-generated content may be incorrect.

This time I logged in as a user



And I cannot edit or delete any student in the table 

I tried to access the URL “/student?action=delete&id=1”

A screenshot of a computer

AI-generated content may be incorrect.

And it shows me an error, which is “Access denied”

**Exercise 7: Role-Based UI**

**Task 7.1: Update Student List View**

Navigation bar with user info

A computer screen shot of a program code

AI-generated content may be incorrect.

This is the navigation bar where user info is displayed. The info is displayed through “sessionScope.fullName” and “sessionScope.role”.

Role badge displayed



Add button shown for admin only

A computer screen shot of text

AI-generated content may be incorrect.

It will check “session.Scope”, if its role is “admin”, then the “Add new Student” button will be shown.

Edit/Delete buttons for admin only

A screen shot of a computer program

AI-generated content may be incorrect.

Again it will check “sessionScope.role eq ‘admin’” to see whether that is admin or not. If it is admin, then the “Edit” and “Delete” button will be shown.

Error messages displayed

A screen shot of a computer program

AI-generated content may be incorrect.