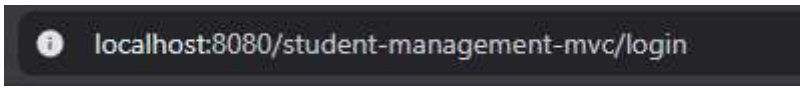
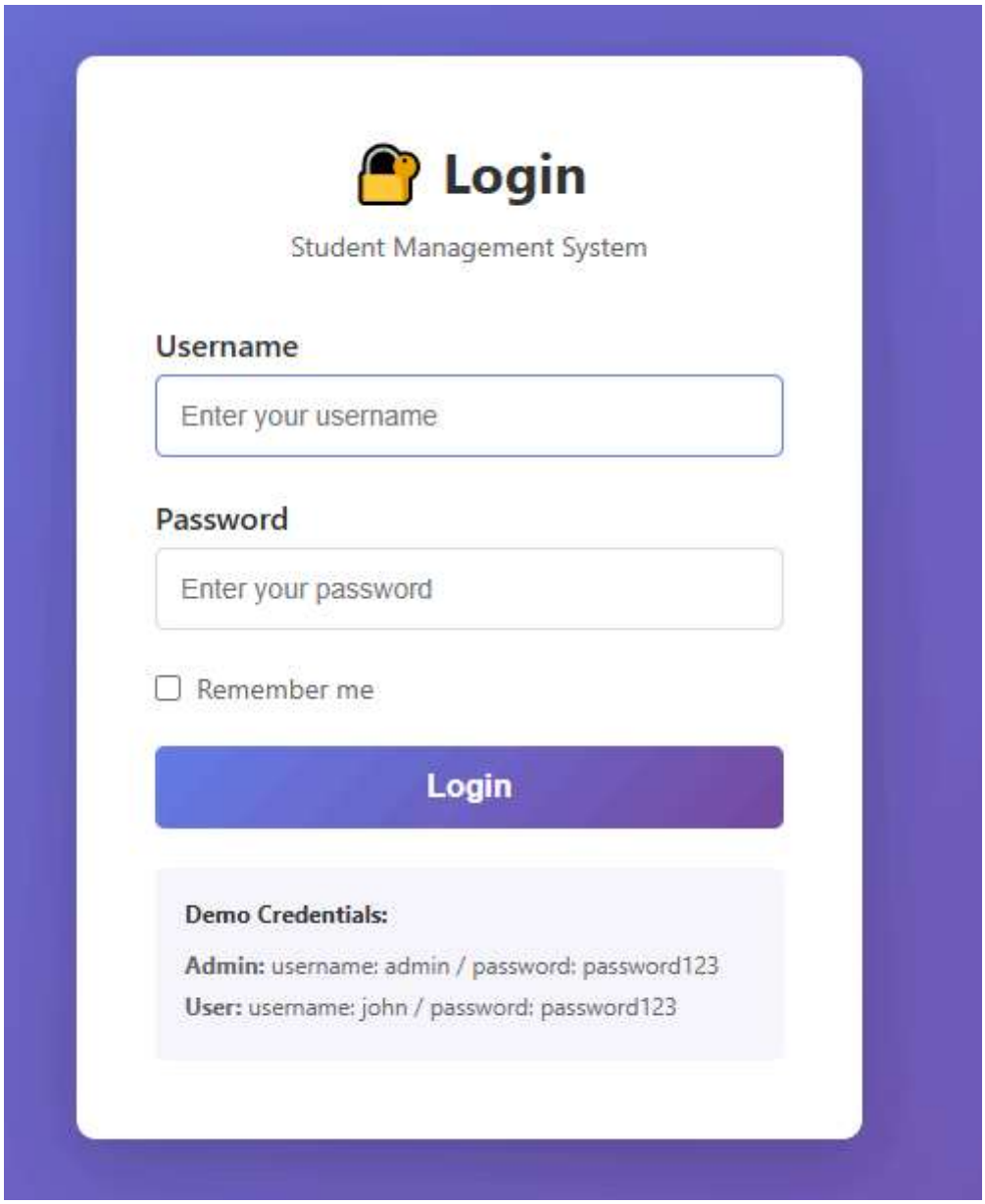
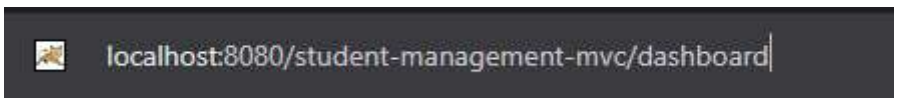
Exercise 5: AuthFilter

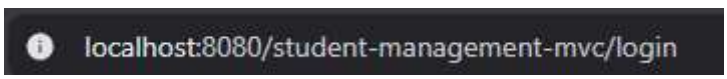
- Allow access to public urls:





- Redirect to login if url is not public:



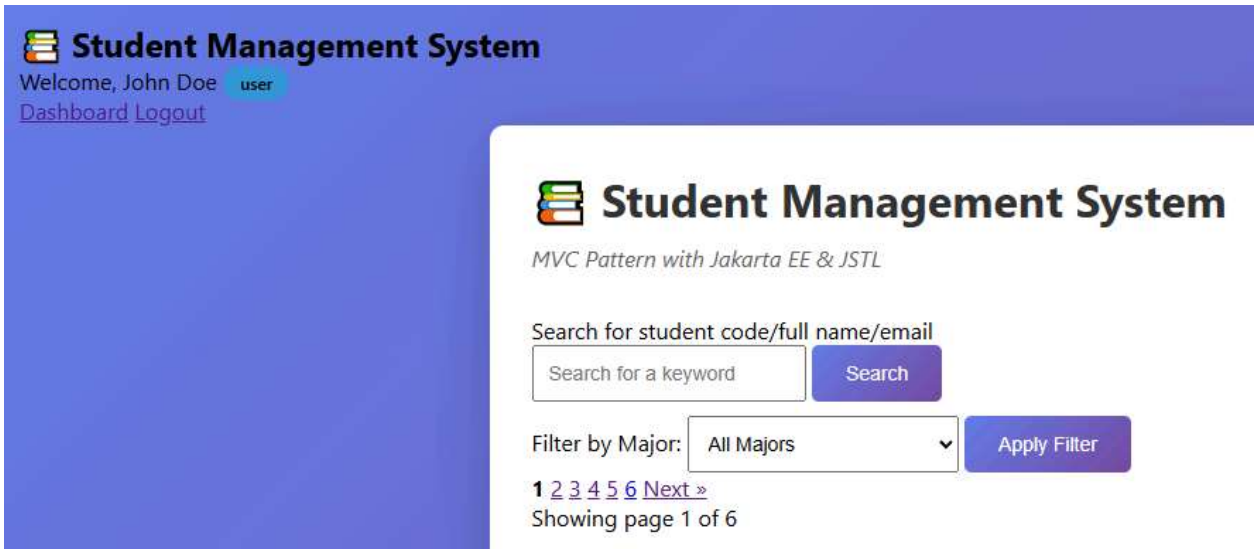


- How it works: When accessing public urls, the filter will allow the request to reach the servlet. When accessing non-public paths like /dashboard or /student, the filter will check first if a session exists, if there is a session that means the user is logged in and the filter will let the request go to the servlet.

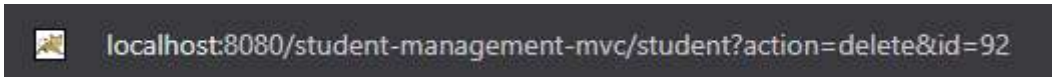
Exercise 6: AdminFilter

- How it works: Whenever the client sends a request with a url that begins with /student, the AdminFilter will intercept the request to check if the action parameter is admin action or not. Then if the action is an admin action, the filter will check if a session exists (logged in or not) and then check if the user of that session has an admin role or not. If the user is admin then the filter will let the request go to the servlet, otherwise the filter will redirect to list-student.jsp with an error message.
- Example:

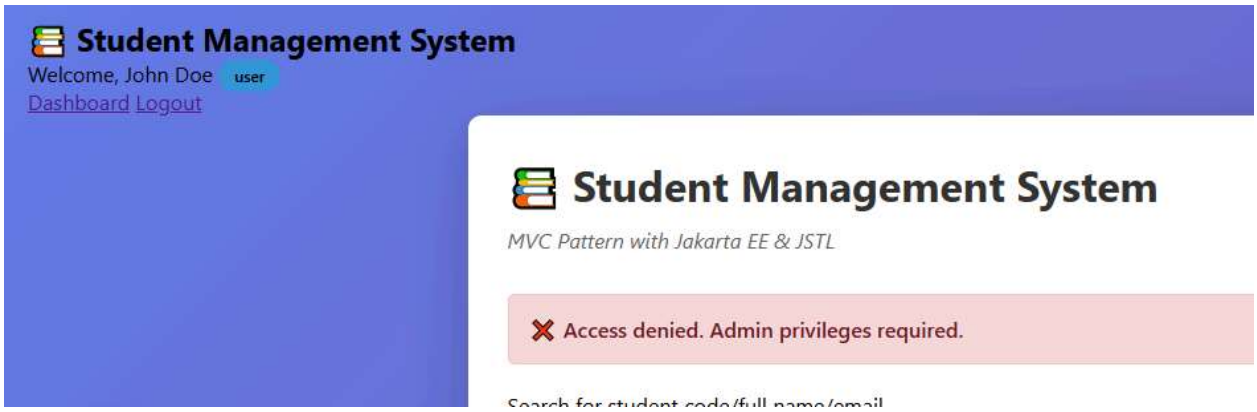
Log in as normal user:



Try to do delete action in search bar:

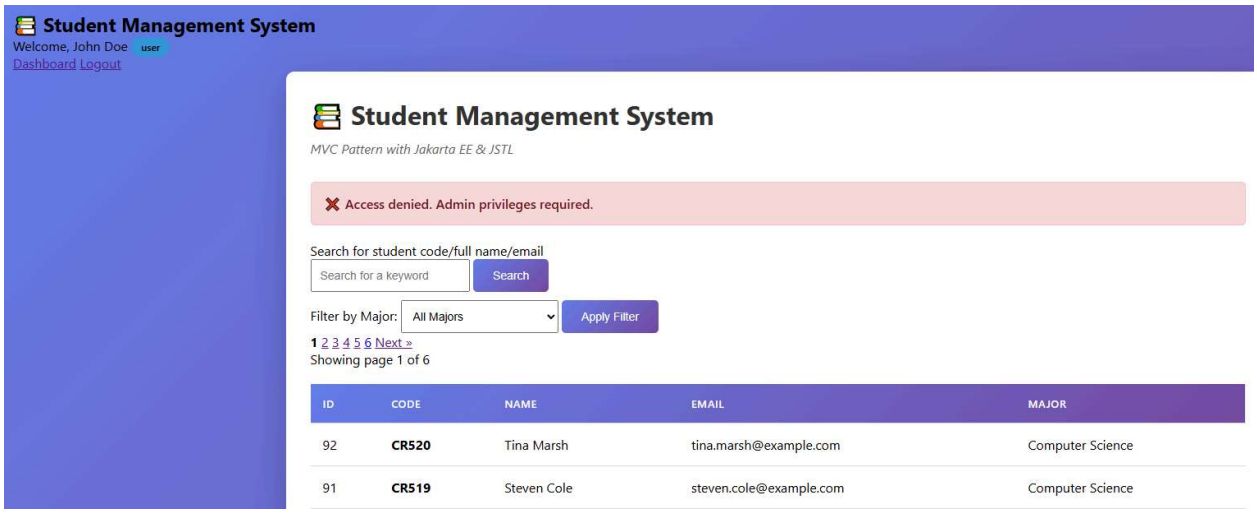


Denied:

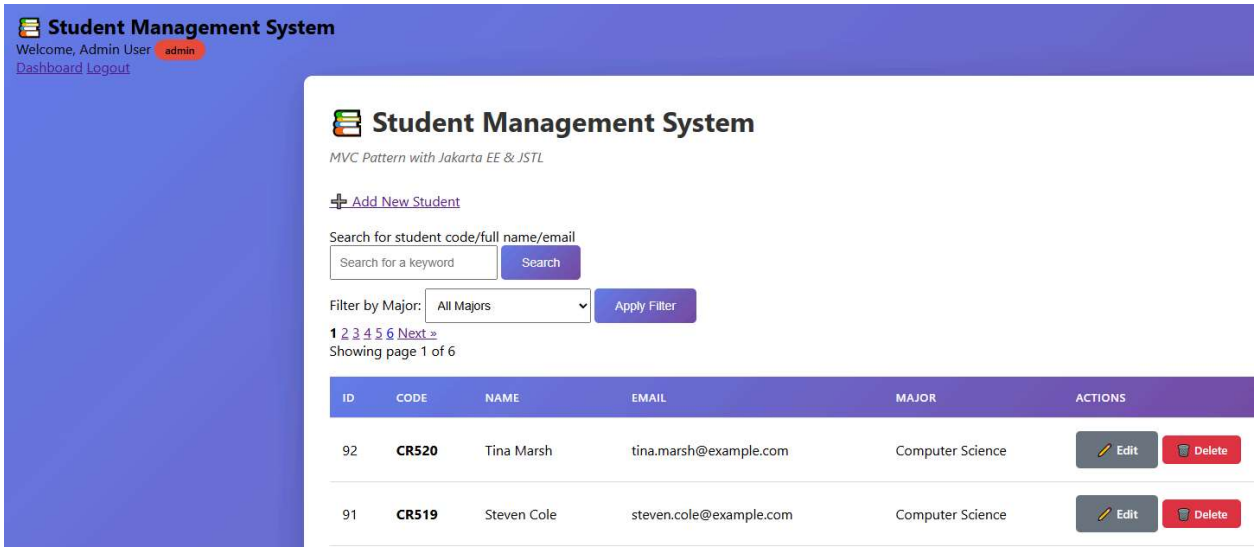


Exercise 7: Role-based UI

- For normal users, no action column and add student button:

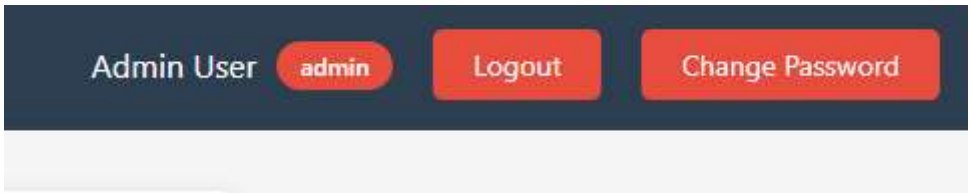


- For admin users, all functionalities:

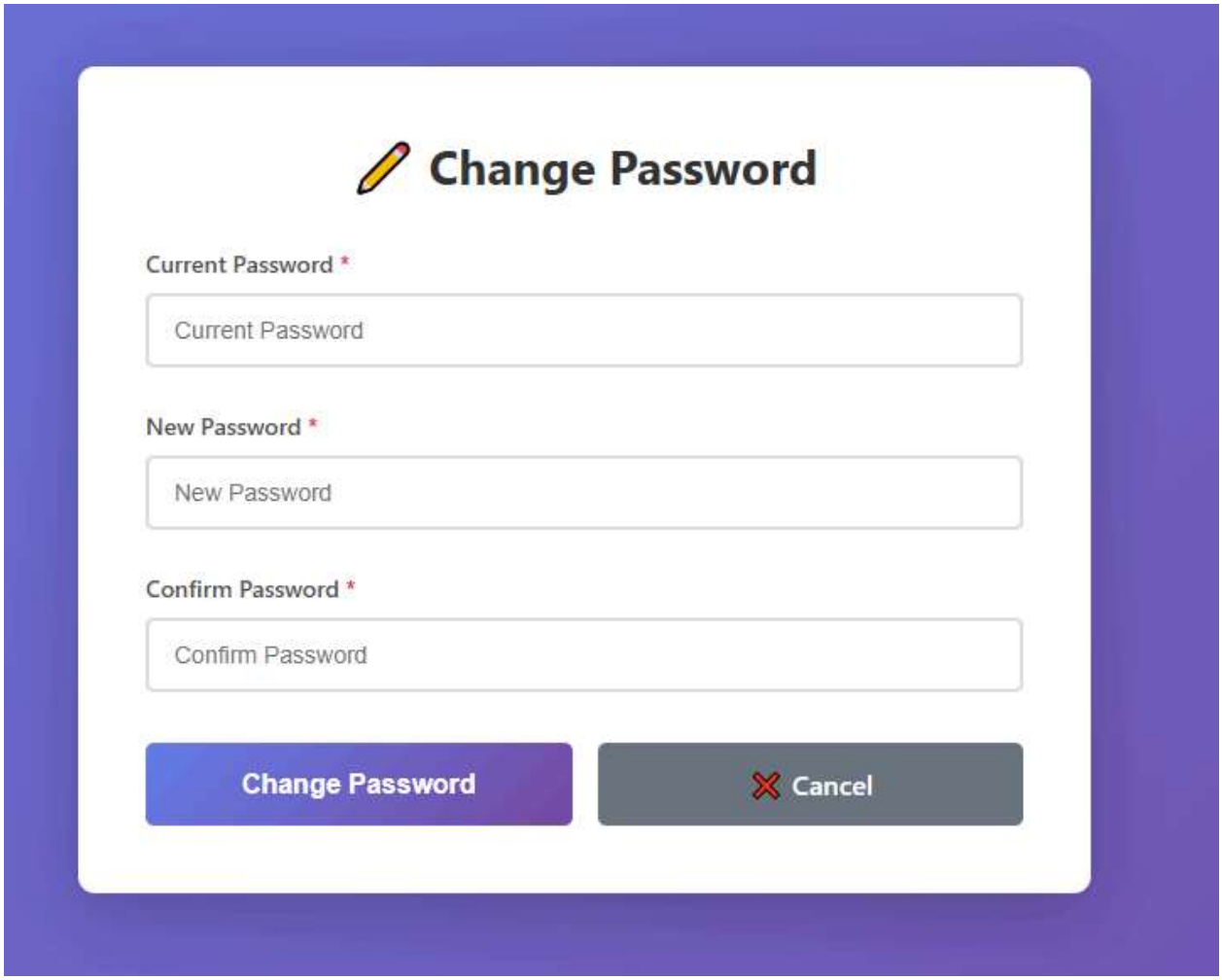


Exercise 8: Add change password functionality

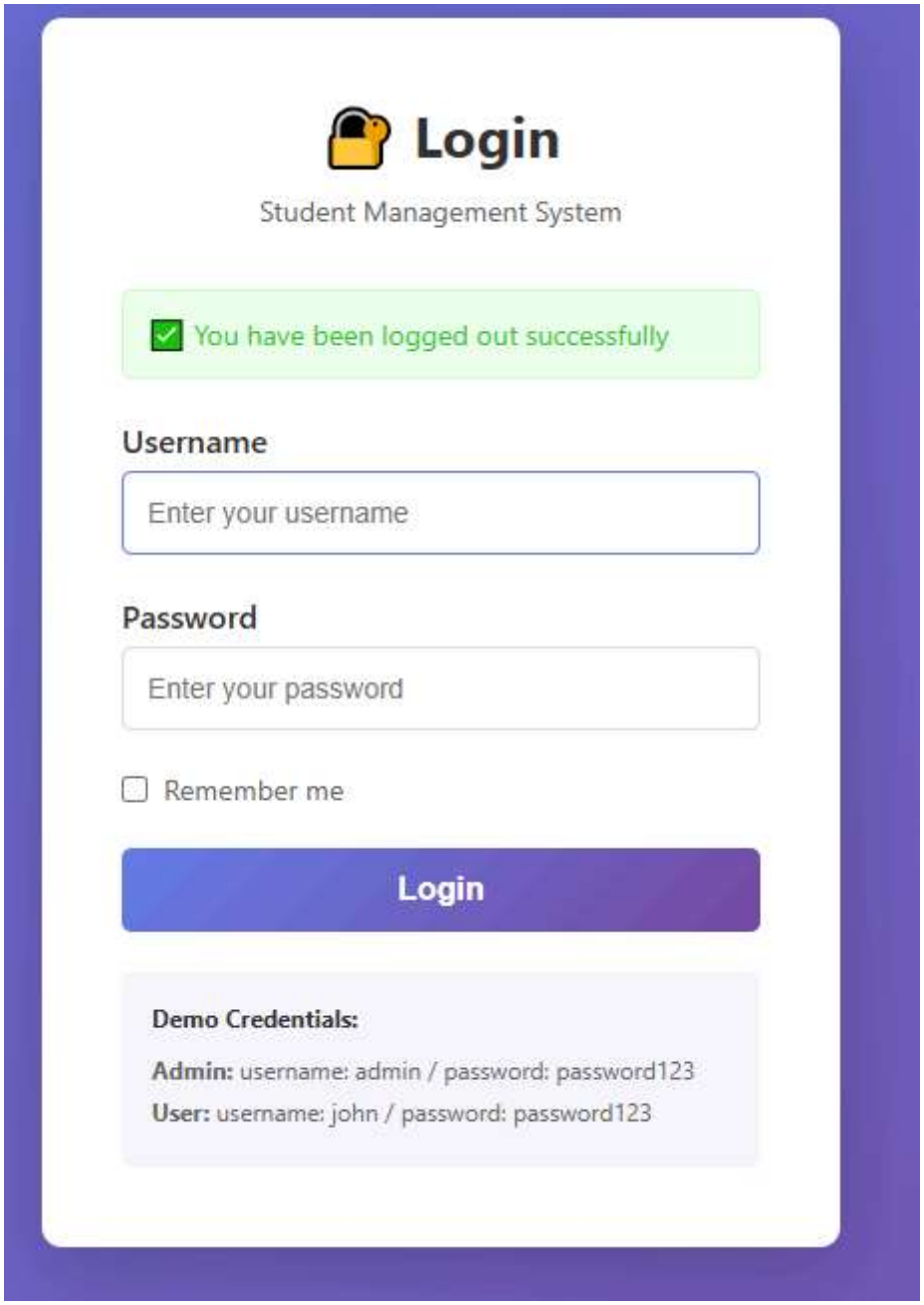
- Add change password button to dashboard:



- Change password page:



- Logout after changing password:



- How this works: When logged in, any user can click the change password button in the dashboard. That will send a GET request to the change password controller and the controller will forward to the change password page. After filling in the fields and pressing Change Password, a POST request will be sent to the controller, which will first check if the user is logged in, then validate all fields and finally invoke userDAO.updatePassword with the hashed value of the new password. If the method returns true, the controller will logout the user.