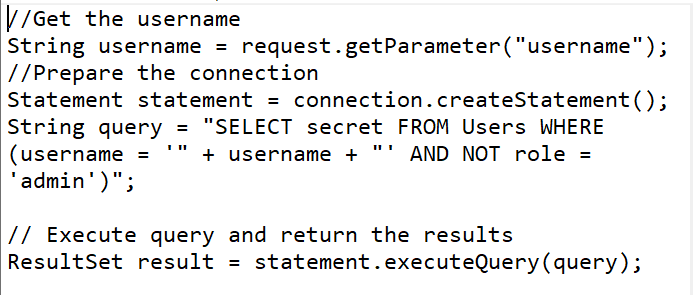
Attempt the following questions:-

Perform static code analysis on the code below.

Determine what vulnerability exists in the code.

How would you mitigate the vulnerability in the code?



There is no code to validate or sanitize the input of the variable ‘username’ which means that the user can input malicious inputs which will query straight to the database. The code is vulnerable to attacks such as XSS and SQL Injection.

To prevent this, input validation / sanitization could be used to ensure that all user input will not be malicious.