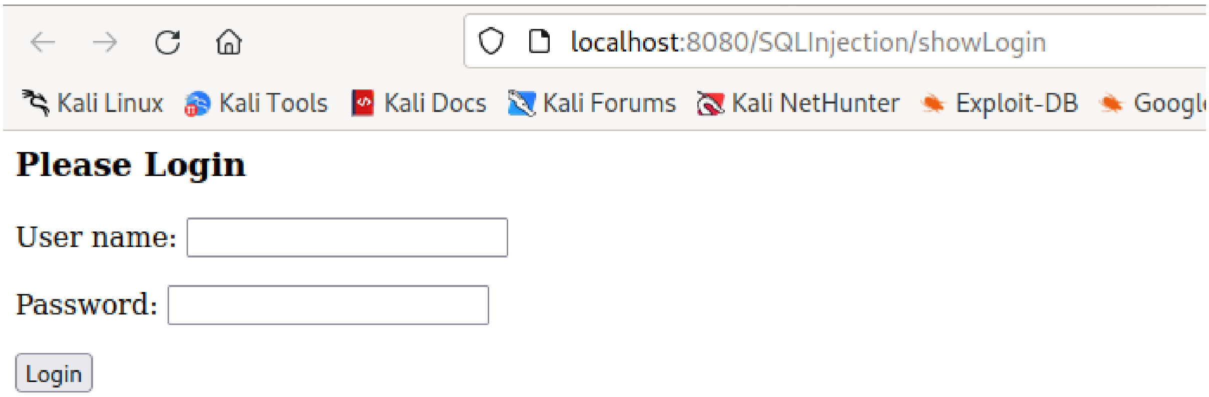
SIT 218/738: Secure coding

Pass task 5.1P: SQL injection (Part 1)(Updated)

Note: Complete the steps provided in "**Ontrack Task5.1P Start Activity"** on CloudDeakin before completing this task.

Objective
In this task you will use the SQL injection technique to bypass the authentication mechanism used in a web application. You will also identify the reasons for this attack to be successful.

Overview
Task1: The SQLInjection webapp in the SIT218VM is vulnerable to SQL injection attacks. One of the users configured in the webapp has the username 'Alice'. Craft a SQL injection code to bypass the authentication of the web app. You must continue from the steps given under the "**SQL injection test in webapp**" in the "Ontrack Task 5.1P Start activity" document and start the SQLInjection webapp in the SIT218VM.



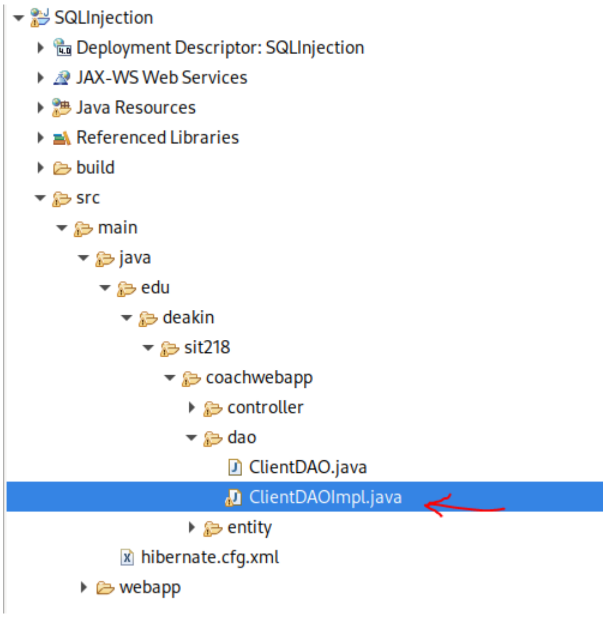
Please Login

User name:

Password:

Once the above page is loaded, try to bypass the authentication.

Task2: Highlight the vulnerable code in the functions **existsClient()** and **areCredentialsCorrect() in ClinetDAOImpl.java file**. Use the following screenshot to locate the vulnerable code file in the SQLInjection webapp in the SIT218VM.



```
SQLInjection
  Deployment Descriptor: SQLInjection
  JAX-WS Web Services
  Java Resources
  Referenced Libraries
  build
  src
    main
      java
        edu
          deakin
            sit218
              coachwebapp
                controller
                dao
                  ClientDAO.java
                  ClientDAOImpl.java
                entity
          hibernate.cfg.xml
      webapp
```

Submission Requirements:

Submit one PDF file containing the following information:

1. The input SQL injection code which is used to bypass the authentication using an username ‘Alice’.
2. Screenshot that shows a successful bypassing of authentication by the above SQL Injection attack (1).
3. The code in the webapp that is vulnerable and a brief explanation of this vulnerability.