IFS4103: Graded Lab Tasks 4 (SQL Injection – 1.5 marks)

For this GLT 4, which is our last GLT, you want to perform **SQL Injection attack steps** as described in **Lab 5**. For the tasks below, as explained in Lab 5 as well, just target **http://<*IP-address*>/dvwa/vulnerabilities/sqli** of the DVWA application.

Please perform the following two tasks:

- **Task 4-1 (0.75 marks – Manual attack)**: Attach a screenshot (in *colour*) showing the output from entering "`IFS4103' and 1=2 union select null, database() #`". The displayed target app's **database name** should be visible in your screenshot.
- **Task 4-2 (0.75 marks – Automated attack using sqlmap)**: Attach a screenshot (in *colour*) showing the output from dumping the content of the **`user_id`**, **`user`**, and **`password`** columns in the **`users`** table.

Like the previous GLTs, please follow these **instructions** for your submission:

- Please put the requested screenshots in a self-contained **PDF file** by using your **name and matric number** as part of your file name, e.g. JackLee-A012345-**GLT4**.pdf. Your report PDF should also contain your name and matric number on its first page.
- Upload your PDF file via "**`Graded Lab Tasks 4`**" Canvas Assignment by **Sunday, 17 March 2024, 23:59 SGT**. Note that this deadline is a ***firm & final* deadline**. There will be ***no*** deadline extensions given. As such, you are advised to submit **well before** the cut-off time so as to avoid any technical issues with Canvas access or your uploading!

Happy probing & dumping!