CEGEP VANIER COLLEGE
CENTRE FOR CONTINUING EDUCATION
Cybersecurity
420- 950-VA

Teacher: Samir Chebbine **Lab 4** **Feb 28, 2025**

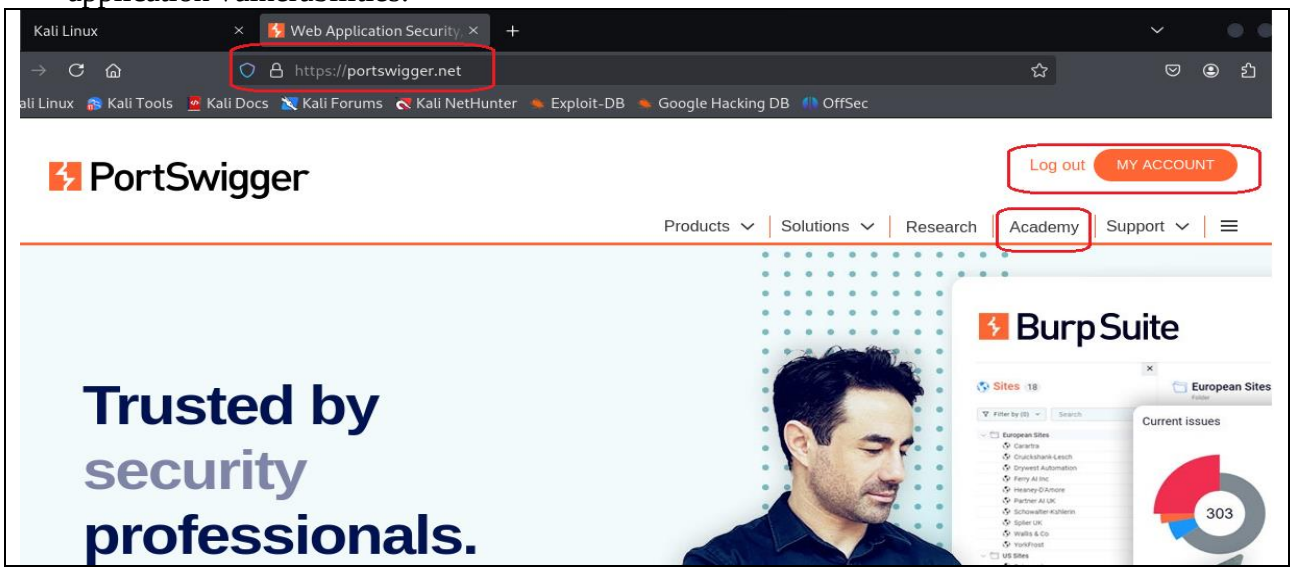
Lab 4: Web Security - SQL Injection Attacks

Complete all these following sections as explained in **class.** All *steps* were presented during class time.

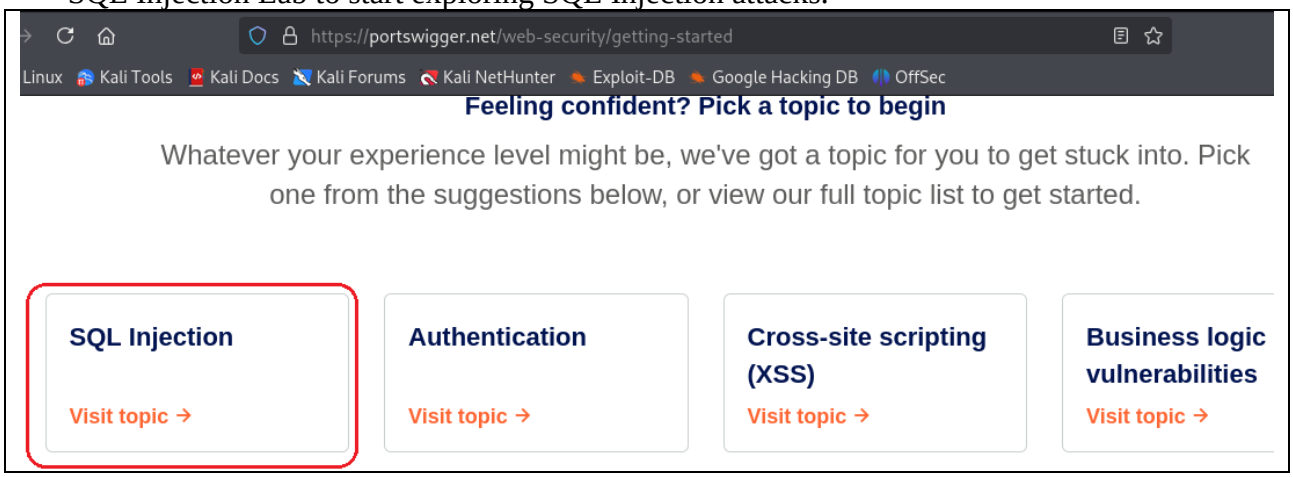
Create and Submit a Word file ***Lab4CybersecurityYourName.doc*** which contains answers of Book Exercises and output screenshots for every project. Submit all Python scripts.

1. **PortSwigger Web Security:**

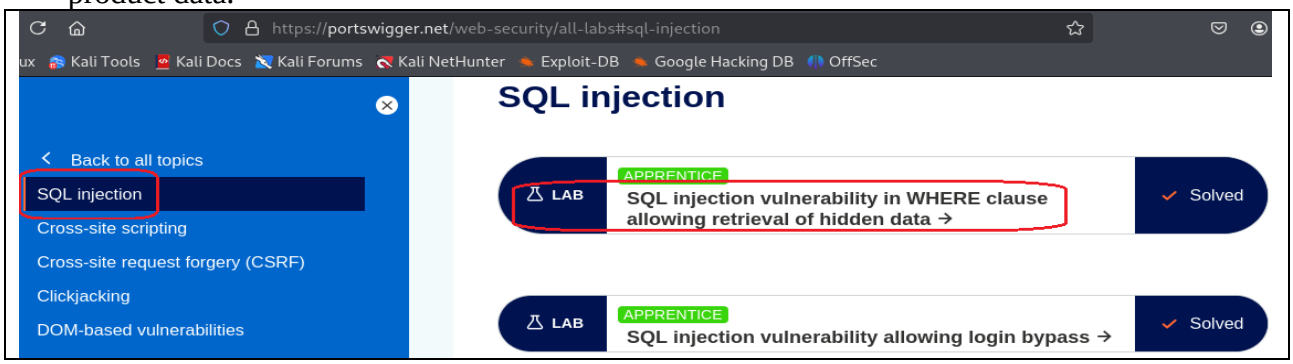
a) Navigate to https://portswigger.net/ and create free account profile to test different web application vulnerabilities.



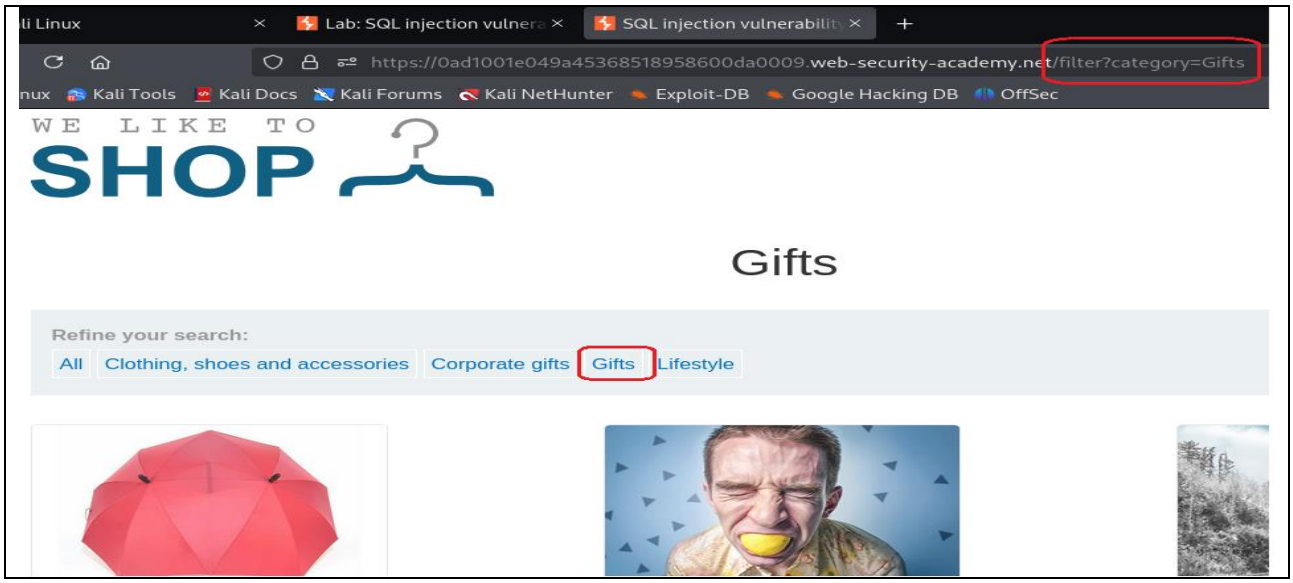
b) **SQL Injection Labs:** Press on Academy button menu to access different listed labs. Choose SQL Injection Lab to start exploring SQL Injection attacks.



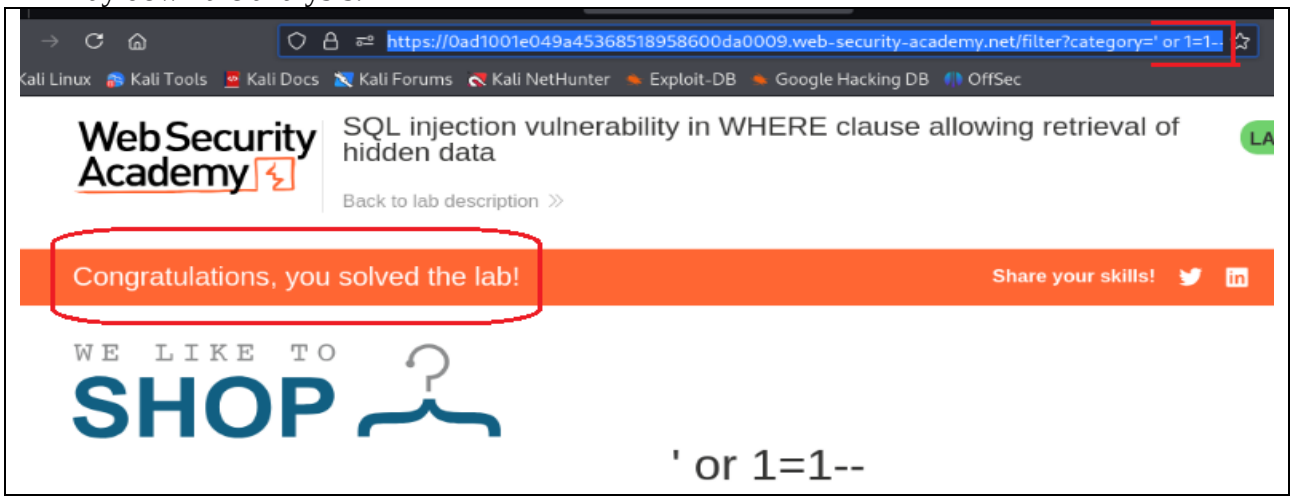
c) **Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data:** Select this lab and figure out the vulnerability in WHERE clause allowing retrieval of hidden product data.



d) The web application allows retrieval of only released products, and you need to display the unreleased products using SQL WHERE clause when filtering product category as shown hereafter.



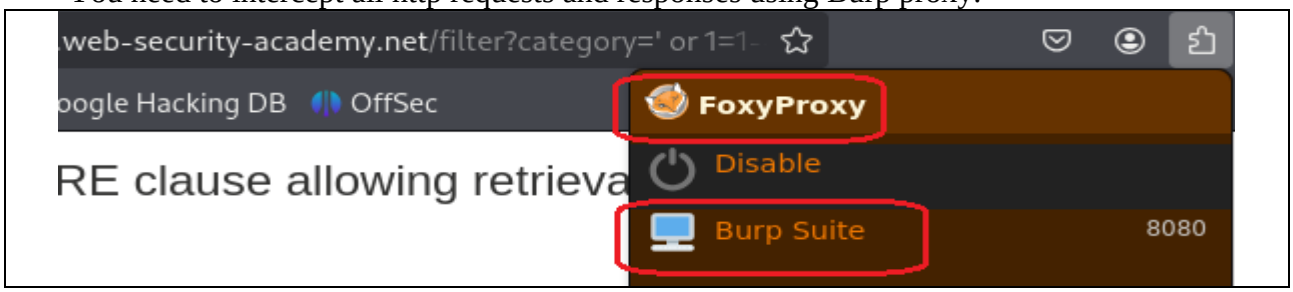
e) Create a text file explaining all steps toward solving the lab for displaying all released and unreleased products in above Web shopping application following the format shown in class.
Describe the problem:
Highlight the end goal:
Lay down the analysis:



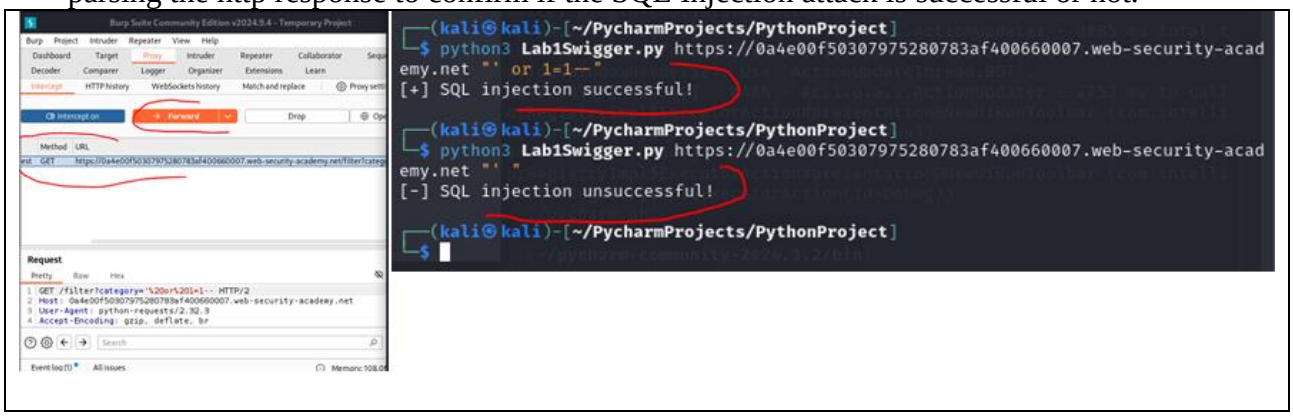
2. Burp Proxy to intercept http requests/responses:

a) Install FoxyProxy as browser extension that offers powerful proxy configuration functionality for switching between different configuration proxies within your browser.

b) Configure your browser to enable/disable the Burp Suite proxy using FoxyProxy extension. You need to intercept all http requests and responses using Burp proxy.



c) You need to script the above attack using Python by sending appropriate http request and parsing the http response to confirm if the SQL Injection attack is successful or not.



3. Lab: SQL injection vulnerability allowing login bypass/SQL Injection UNION attack

a) Redo question 1e) and 2c) to solve the following SQL Injection labs listed in PortSwigger web site.