**Lab 9: SQL injection - SQL injection UNION attacks**

**Objective**:

* This lab focuses on exploring and understanding Union-Based SQL Injection attacks. Participants will engage with a simulated web application that is vulnerable to SQL injection, specifically through the misuse of the UNION SQL operator. The objective is to learn how to identify, exploit, and subsequently defend against Union-Based SQL Injection vulnerabilities.

In this lab, students need to:

* Answer the following questions:
  + What is a Union-Based SQL Injection attack, and how does it differ from other types of SQL injection attacks?
  + Explain the role of the UNION SQL operator in this type of attack and how it can be used to extract data from a database that is not typically accessible through the intended use of a web application.
* Perform challenge:
  + [SQL injection UNION attack, determining the number of columns returned by the query](https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns)
* Explain and capture all steps (full windows screen capture).

Submit a report addressing all the questions mentioned above in either **PDF** or **Markdown** format. Additionally, include a **video** demonstrating the detailed process of your work to ensure the authenticity of your lab exercise.

The report file name must be **Class\_YourStudentID \_YourName\_Lab9**