**Lab 11: Blind SQL injection - Error SQL Injection**

**Objective**:

* This lab focuses on Error-Based SQL Injection, a method where attackers induce database errors to gather information about the database structure and contents. Participants will work with a simulated web application that is deliberately configured with error-based SQL injection vulnerabilities.

In this lab, students need to:

* Answer the following questions:
  + What is an Error-Based SQL Injection attack, and how does it differ from other types of SQL injection?
  + Explain the concept of using database errors to extract information, and describe the typical signs that a web application might be vulnerable to this type of attack.
* Perform challenge:
  + [Blind SQL injection with conditional errors](https://portswigger.net/web-security/sql-injection/blind/lab-conditional-errors)
* 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\_Lab11**