**Lab 10: Blind SQL injection - Timebase SQL Injection**

**Objective**:

* This lab is dedicated to exploring Time-Based SQL Injection, a subtype of SQL injection attacks where the attacker can infer information from a database by observing the response time of the web application. Participants will interact with a simulated web application that has a time-based SQL injection vulnerability. The goal is to understand the mechanics of this attack, identify vulnerabilities, exploit them, and learn effective mitigation strategies.

In this lab, students need to:

* Answer the following questions:
  + What distinguishes Time-Based SQL Injection from other SQL injection techniques? Explain how an attacker can use time delays in SQL queries to extract information from a database, and why this method is particularly useful when dealing with blind SQL injection scenarios where no data is returned in the web application's responses.
  + Describe the process of executing a Time-Based SQL Injection attack on a vulnerable web application. What are the key steps in crafting a SQL query that causes a deliberate delay in the database response.
* Perform challenge:
  + [Blind SQL injection with time delays](https://portswigger.net/web-security/sql-injection/blind/lab-time-delays)
* 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\_Lab10**