**Lab 17: Race conditions vulnerabilities**

**Objective**:

* This lab is designed to explore Race Conditions vulnerabilities in web applications and systems. Participants will interact with a simulated environment where specific processes or actions are prone to race conditions. The objective is to understand how race conditions occur, identify their impact on application security and data integrity, exploit these vulnerabilities, and learn effective strategies to prevent them.

In this lab, students need to:

* Answer the following questions:
  + What are Race Conditions vulnerabilities, and how do they differ from other types of vulnerabilities in web applications? Explain the concept of a race condition, including how concurrent processes or threads can lead to unexpected or insecure states.
  + Describe the process of exploiting a Race Conditions vulnerability in a web application or system. What techniques can an attacker use to induce a race condition, and how can such vulnerabilities lead to security breaches or data corruption?
* Perform challenge:
  + [Limit overrun race conditions](https://portswigger.net/web-security/race-conditions/lab-race-conditions-limit-overrun)
* 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\_Lab17**