**Lab 14: Cross-site scripting - Reflected**

**Objective**:

* This lab is dedicated to exploring Reflected Cross-Site Scripting (XSS) vulnerabilities, where malicious scripts are injected into a web application and reflected back to the user's browser. Participants will interact with a simulated web application that is vulnerable to reflected XSS attacks. The objective is to understand how to identify and exploit these vulnerabilities, as well as to learn effective mitigation techniques to protect web applications from such attacks.

In this lab, students need to:

* Answer the following questions:
  + What is Reflected Cross-Site Scripting (XSS), and how does it differ from other types of XSS attacks like Stored XSS and DOM-Based XSS?
  + Explain how Reflected XSS works, including how malicious scripts are injected and executed in the victim's browser, and discuss the typical attack vectors for this type of vulnerability.
* Perform challenge:
  + [Reflected DOM XSS](https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-dom-xss-reflected)
* 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\_Lab14**