**Lab 15: Cross-site scripting - Stored**

**Objective**:

* This lab is focused on Stored Cross-Site Scripting (XSS) vulnerabilities, a type of XSS where malicious scripts are permanently stored on the target server, such as in a database, and then rendered in a user's browser when the stored data is displayed. Participants will interact with a simulated web application that is vulnerable to stored XSS attacks.

In this lab, students need to:

* Answer the following questions:
  + What defines Stored Cross-Site Scripting (XSS), and how does it differ from Reflected XSS and DOM-Based XSS?
  + Explain the process of how malicious scripts are injected, stored, and subsequently executed in Stored XSS attacks, and discuss the potential consequences these attacks can have on both users and web applications.
* Perform challenge:
  + [Stored DOM XSS](https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-dom-xss-stored)
* 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\_Lab15**