Lab Activities 2: Cross-Site Scripting (XSS) Vulnerabilities
Due Date: 30 MAY 2025

Lab Objectives:
By the end of this lab session, students will be able to:

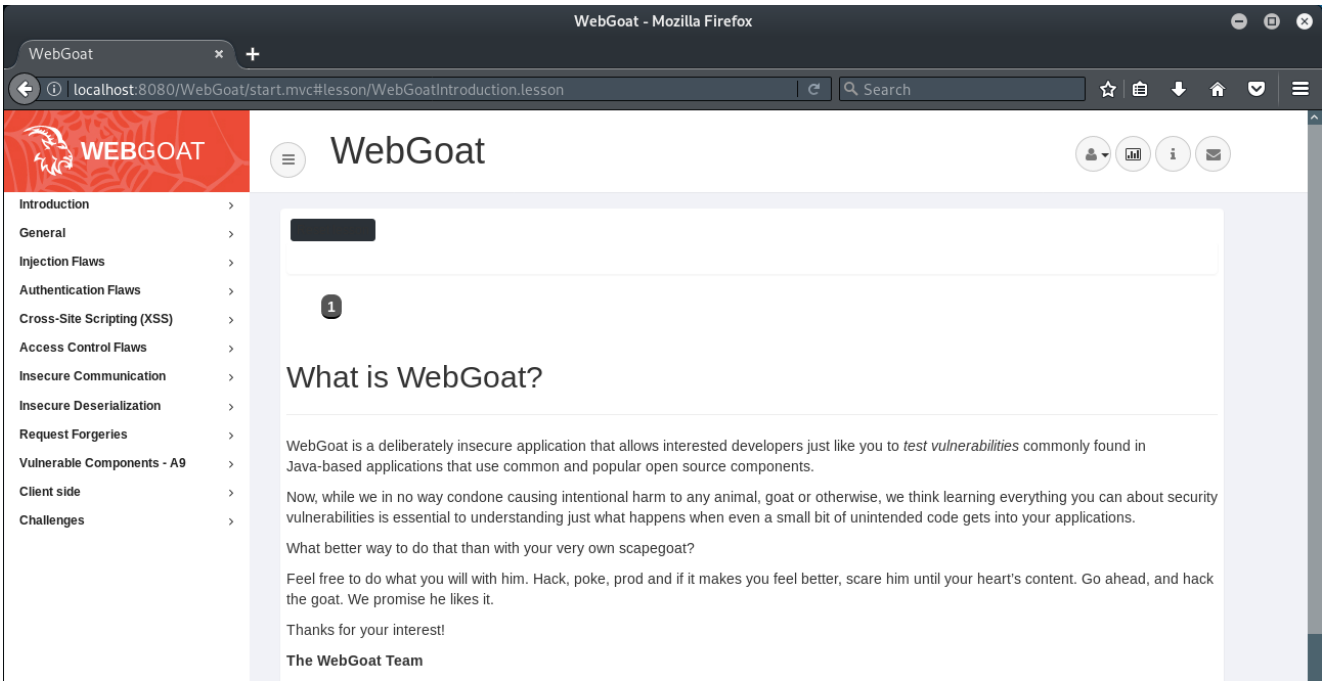
1. Understand the concept of Cross-Site Scripting (XSS).
2. Identify different types of XSS vulnerabilities.
3. Exploit a sample application vulnerable to XSS.
4. Learn basic mitigation techniques to prevent XSS attacks.

Pre-Requisites
Before starting:

- Install and run WebGoat via Docker or as a standalone Java application.
- Access WebGoat at: http://localhost:8080/WebGoat
- Login credentials:
  - Username: guest
  - Password: guest

  Reference: https://www.youtube.com/watch?v=gxID0acwBgc

Lab Activities:



Activity 1: Reflected XSS

Discussion:

- What causes the reflected XSS in this page?
- How does the browser interpret the injected script?

Activity 2: Stored XSS

Discussion:

- Why is stored XSS more dangerous than reflected?
- How can session hijacking happen through this?

Activity 3: DOM-Based XSS

Discussion:

- How does client-side JavaScript contribute to DOM-based XSS?
- Identify the script in page source that processes the fragment.

Post-Lab Task:

Write a short report (1-2 pages) answering the following:

- Complete all three types of XSS discussions.
- Provide screenshots for each activity.
    - The input (what you typed).
    - The output (browser alert or result).
- Propose 3 mitigation strategies to prevent XSS in web applications.
- Submit your report to the e-learning.

REFERENCE: https://www.youtube.com/watch?v=YbOM4ek3IOc

[END OF LAB]