**Practical 3**

**Cross Site Scripting (XSS)**

|  |
| --- |
| **Objectives:**  After completing this lab, you should be able to:   * Perform Cross-Site Scripting on a vulnerable webpage to modify data |

Exercise 1: WebGoat Exercises

**WebGoat is a deliberately insecure web application maintained by OWASP designed to teach web application security lessons.**

Navigate to Section (A7) Cross-Site Scripting (XSS), and complete exercises 1-8 and 12 (MCQ).

The exercises will guide you on performing reflected XSS.

**Exercise 2:**

Graphical user interface, text, application

Description automatically generated

**Exercise 7:**

**Graphical user interface, application

Description automatically generated**

**Exercise 12:**

**Graphical user interface, text, application

Description automatically generated**

Exercise 2: Mimosa

**Mimosa is an intentionally vulnerable online web application maintained by SP.**

Complete the newly released mimosa Cross Site Scripting challenges.

**Biography:**

Graphical user interface, text, application, email

Description automatically generated

Use inspect and modify the html code for the image.

**Christmas Workshop:**

**Graphical user interface, text, application

Description automatically generated**

<a href=”google.com”></a>

**Fakebook Bank**

Graphical user interface, text, application

Description automatically generated

Just enter html code for a simple login form.

**Syndica:**

Graphical user interface, text, application

Description automatically generated

Use eval and base64 encoder (atob to decode) to bypass filters. Use invalid characters to make the system drop request, which will then appear as html code.

**Xss basics:**

Graphical user interface, text, application, email

Description automatically generated

Just <script>alert(‘helloworld’)</script>

**\*\*You are strongly encouraged to attempt the questions and document the steps on how you solve the challenges.**

**Your Tutor may require you to submit as part of your progress monitoring or General Performance**.