

**Lab8: *XSS Game* (3%)**

**Overview:**

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy

**Objective:**

In this training program, you will learn to find and exploit XSS bugs. You'll use this knowledge to confuse and infuriate your adversaries by preventing such bugs from happening in your applications.

**The Lab Activities**

**XSS Attack**

In this lab you get to play a cyber security game using <https://xss-game.appspot.com/>

It provides an enjoyable introduction to cyber-attacks.

Through the lab you’ll receive a basic introduction to XSS. Your goal will be to complete 3 levels of this Lab.

1. Navigate to the website: ‘<https://xss-game.appspot.com/>
2. Click on ‘LET ME’
3. Successfully complete three (3) levels of challenges.
4. Take screen shots showing each challenge is complete and save it in your report.

**Make sure in all screenshots part of your customized background time/date is visible.**

**Lab Assignment Write-up**

Use this file as your Lab report template, enter your screenshots into the report.

**Deliverable**

Submit your Lab report as a “.docx” or “pdf” format through the course’s web site with the following name: