CompSci 657/790 Topics: Introduction to Cybersecurity
HW #5 (50 points)
2024 Spring

Due: April 19, 2024 8:30pm

1 Overview

This homework is to practice the cross-site scripting (XSS) attack. The XSS vulnerability allows an attacker to inject code (typically HTML or JavaScript) into the contents of a website not under the attacker's control. When a victim views such a page, the injected code executes in the victim's browser. Therefore, the victim's private information associated with the website can be stolen by attackers.

1.1 Hands-on Lab Environment Setup in your local computer

We will use the online environment Gruyere for the hands-on practice on cross-site scripting (XSS) attacks. The website URL is: `https://google-gruyere.appspot.com/part2#2__cross_site_scripting`

2 Task 1: Complete the metacognition questions for HW5

On Canvas >Assignment >Homework >HW5-Metacognition Questions (6 points, due on April 16)

3 Task 2: Complete the Cross-Site Scripting (XSS) challenges

We will use the JavaScript function **alert()** to conduct the XSS attacks. The **alert()** function creates a pop-up box with whatever string you pass as an argument.

In this homework, we use this simple function to demonstrate the process of injecting scripts, which can be transferred to inject other malicious scripts. Your challenge is to find XSS vulnerabilities in Gruyere.

The XSS vulnerabilities usually involve applications not properly handling untrusted user data. In this homework, you will observe how a random input text in the input fields could be rendered in the response page HTML source.

Please use your LASTNAME as the footprint message for the attack tasks, where if the attack is successful, you can see such footprint. Make screen prints for the step-by-step process to show how you did the assignment and also how that attack got triggered, for example, an explanation along with screenshots.

What you need to do:

Challenge 1. File Upload XSS

Challenge 2. Reflected XSS

Challenge 3. Stored XSS

Challenge 4. Stored XSS via HTML Attributes

Bonus Tasks:

Challenge 5. Stored XSS via AJAX

Challenge 6. Reflected XSS via AJAX

4 Submission

Submit the following item on Canvas:

- HW5-Metacognition Questions
- report.pdf