UNIVERSITY OF MARYLAND
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

ENEE 457
Computer Systems Security
Instructor: Dana Dachman-Soled

Programming Project 2: Cross Site Request Forgery and Cross Site Scripting

Out: 09/18/19 Due: 10/02/19 10:59am

Instructions

1. Strictly adhere to the University of Maryland Code of Academic Integrity.
2. Submit the .html files for Part I as a .zip file, as well as a detailed writeup including screenshots and any other documentation explaining what you did as a pdf document at Canvas. Include your full name in the writeup. Name the .zip file as x-project2.zip and the .pdf file as x-project2.pdf where x is your first and last name. For example, if your name is "Jane Doe," you should be handing in files named "JaneDoe-project2.zip" and "JaneDoe-project2.pdf."

Labs are sourced from SEED labs `https://seedsecuritylabs.org/`

1 Overview

In this lab, students will interact with the Elgg website–a generic social media site–and experiment with two types of attacks: Cross-Site Request Forgery (CSRF) attacks and Cross-Site Scripting (XSS) attacks. The Cross-Site Request Forger attacks are fairly straightforward. The Cross-Site Scripting attacks are more challenging, with the final one culminating in an attack similar to Samy's worm, which was an attack on MySpace discussed in class.

2 Lab Tasks

2.1 Setting Up the Virtual Machines

Most of our labs are taken from the SEED website: `https://seedsecuritylabs.org/Labs_16.04/`. Before you can start doing the labs, you must install Virtual Box and must load the pre-built `Ubuntu` virtual machine (SEEDUbuntu16.04.zip). In order to do this, see instructions here: `https://seedsecuritylabs.org/lab_env.html`. Please make sure to carefully read the documentation here `https://seedsecuritylabs.org/Labs_16.04/Documents/SEEDVM_VirtualBoxManual.pdf` which explains how to configure and run the machine.

Important: Note that the websites used in Part I and Part II below are different, although both use the Elgg application. Your attacks will not transfer from one to the other, so make sure you are using the correct website for each part.

2.2 Part I

Follow the instructions for the SEED Cross Site Request Forgery lab, which can be found here: `https://seedsecuritylabs.org/Labs_16.04/PDF/Web_CSRF_Elgg.pdf`.

2.3 Part II

Follow the instructions for the SEED Cross Site Scripting Lab, which can be found here: `https://seedsecuritylabs.org/Labs_16.04/PDF/Web_XSS_Elgg.pdf`.

Important:

- You do not need to do Task 3 (See Section 3.4) of the XSS lab.
- You must add a variable declaration "var sendurl" and set its value correctly for the script provided in Task 5 (See Section 3.6) to work.

3 Submission

Students need to submit .html code for Part I as a .zip file, as well as a writeup explaining what you did for both Part I and Part II as a pdf document at Canvas. Some questions in the labs are open-ended and there is not necessarily a right or wrong answer. Be sure to include screenshots and document your step-by-step process to receive full credit. Include your full name in the writeup. Name the .zip file as x-project2.zip and the writeup as x-project2.pdf, where x is your first and last name. For example, if your name is "Jane Doe," you should be handing in a single file named "JaneDoe-project2.pdf."