Assignment 8

Security Testing – XSS & CSRF Attacks

Due Date: March 19, 2020

Yasaman Amannejad, 2020

1 INTRODUCTION

In this assignment, we will continue with security testing. We will do some practices on Cross-site scripting (XSS), and Cross-site request forgery (CSRF). This assignment needs to be done as a **group work**. It is recommended that all team members communicate and exchange the ideas to find the solutions.

Students must complete:

- Complete tasks 1-8, and also 12 of XSS activities in WebGoat. Answer the question from step 4 of the instruction (XSS prevention) in your report.
- Complete tasks 1-5 of cross-site request forgeries in WebGoat.
- XSS reflected and stored tasks in DVWA with security level = low. Answer the question from step 11 of the instruction (XSS prevention) in your report.
- CSRF attack in DVWA, and write answers to questions in steps 14-15 of the instructions.

Submission – Each team must submit one report file that contains their solution for the given tasks and also the given questions in the instructions (steps: 4, 11, 14, 15).
For WebGoat, you have the option of demoing your results or including your solution in your report.

2 INSTRUCTION

❖ **Complete the following tasks on WebGoat**

Cross-site scripting (XSS)

1. Open WebGoat
2. Go to Cross-site scripting (XSS) page.
3. Complete tasks 1-8, and 12 (The rest of the tasks are *optional*).
4. How can we prevent XSS attacks? Discuss your answer from an end-user point of view, and also a system developer?

Request Forgery

5. Open WebGoat
6. Go to Request forgeries – Cross-site request forgeries.
7. Complete tasks 1 – 5 (The rest of the tasks are *optional*).

❖ **Complete the following tasks on DVWA**

Cross-site scripting (XSS)

8. Open DWVA. Set the security level to low.
9. Go to XSS reflected page and check if it is vulnerable, if it is, use this field to make a modification of your choice in the current page (e.g., add a field, or text to the HTML file).
10. Repeat the same with the XSS stored page.
11. What is the difference between XSS stored and reflected?

Request Forgery

12. Open DWVA. Set the security level to low.
13. Go to the CSRF page. It is the password change page. You can change your password from this page.
14. Describe how this page (source code with security level low) is vulnerable to CSRF attack. How can an attacker utilize this vulnerability?

15. How can we prevent CSRF attacks?

3 SUBMISSION

3.1 DELIVERABLES

- Each team must submit one report file that contains their solution for the given tasks and also the given questions in the instructions (steps: 4, 11, 14, 15).

- For WebGoat, you have the option of demoing your results or including your solution in your report.

3.2 MARKING SCHEME

	Item	**Grade**
WebGoat	XSS (tasks 1-8, and also 12)	25%
	XSS prevention (from step 4)	10%
	CSRF (tasks 1 – 5)	20%
DVWA	XSS 1. Solution for XSS reflected 2. Solution for XSS stored 3. What is the difference between XSS stored and reflected?	25%
	CSRF 1. Describe how this page (source code with security level low) is vulnerable to CSRF attack. How can an attacker utilize this page? 2. How can we prevent CSRF attacks? Discuss your answer from an end-user point of view, and also a system developer?	20%