Lab 07: XSS

Goals

- Identify vulnerabilities of a specified type in an application
- Remediate identified vulnerabilities using specified method

Notes

The lab is available in the Learn org of Dakota State University's Information Assurance Lab within the vApp <username>_CSC234_Zwach_Base. It is accessible at https://ialab.dsu.edu. You can start the vApp by double clicking on it and then clicking Actions and Start in the HTML5 client.

The application we are assessing, and remediating is running in a docker container. The container required for the app is already running and available via the links at http://localhost:8000 within your vApp. If you need to revert all code changes system wide you can use the `revertall` command .

The code that comprises the entire application is available within the /home/student/course_files/_assignments/xsscsrf/app directory. Make your changes there using a text editor of your choosing.

The username is **student** and the password is **Password1!**.

Discovery

This app is vulnerable to cross site scripting. Respond to the following prompts:

1. Review the source code for the application of interest (/home/student/course_files/_assignments/xsscsrf/app).
    a. Provide a screenshot of the vulnerable line of code.
    b. Explain the issue in your own words.
2. Access the application in the browser within the Kali VM.
    a. Provide a screenshot demonstrating exploitation of the vulnerability using the application

Remediation

After confirming the vulnerability, use your knowledge and available resources to secure the vulnerable portion of the application as you see fit.

3. Edit the source code from within the /home/student/course_files/_assignments/xsscsrf/app directory. Changes will be reflected immediately within the docker container. Resolve the issue you identified. Provide a screenshot of the adapted code here.
4. Explain, in detail, why your defense prevents the issues at hand.
5. Test your changes
    a. Are your attempts at entering further malicious input successful? Explain why.
    b. Provide a screenshot that shows both safe output and the GET request passed along with your name.

Scoring

The rubric will be published at scoring time. Each portion of the assignment has the following points assigned.

Section	Points
1	5
2	2
3	2
4	5
5	3
Total	**17**