Lab 10: CSRF

Turn in a Word or PDF document to D2L

Notes

The lab is available in the Learn org of Dakota State University's Information Assurance Lab within the vApp **<username>_CSC234_Zwach_CSRFLab**. It is accessible at https://ialab.dsu.edu. You can start the vApp by clicking Actions and Start.

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

The username of the Kali VM is `student` and the password is `Password1!`

The application should be running at http://localhost:8006, which is also linked from the homepage of Firefox in your vApp (http://localhost:8000).

The following PHP documentation will be useful:

- https://www.php.net/manual/en/reserved.variables.session.php
- https://www.php.net/manual/en/function.random-bytes
- https://www.php.net/manual/en/function.bin2hex

Discovery

This program has one or more flaws. Identify changes you will make and why.

1. *(6 points)* Review the source code for the application of interest (/home/student/course_files/_assignments/csrf/app/index.php).
    a. **Provide screenshots** of vulnerable or otherwise flawed code segments. Be specific.
    b. Explain each issue in your own words.
2. *(2 points)* Run the application
    a. **Provide screenshots** demonstrating each of the vulnerabilities using a method of your choice.

Remediation

After confirming the vulnerabilities, use your knowledge and available resources to modify the source to follow best practices and remediate any vulnerabilities.

1. *(6 points)* Modify the source code to remediate the flaw(s).
    a. Document your resulting source code with **a screenshot of each** of the flaws you remediated.
    b. Explain how each of your changes fixes the flaw(s)
2. *(2 points)* Test your changes
    a. **Provide screenshots** documenting the proper operation of the application without vulnerabilities.

© Shawn Zwach 2020 – Reproduction or sharing of this material without permission is prohibited.