Lab 08: Password Issues

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_Base. It's 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/password_problems 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`!

To start the application, open a terminal and type `flask run`. You then can browse to the application using a web browser at http://127.0.0.1:5000 in the Kali VM. The application should update automatically as you save your changes. If you run the code on your own machine, you will need to export FLASK_DEBUG=1

Valid usernames in the application are **alice**, **bob**, and **charlie**

To modify how user passwords are stored and formatted, use the *update_password.py* script in the /home/student/ course_files/_assignments/password_problems directory. The script takes a username and plaintext password as input and will update the password for the user in the database. You need to modify this script.

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/password_problems/app.py). You may focus your attention to the login function that begins on line 34.
   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.
      i. If you can read or otherwise convert passwords to plaintext, demonstrate that with screenshots.

Remediation

After confirming the vulnerabilities, use your knowledge and available resources to modify the source to follow best practices and remediate any vulnerabilities. The easiest way to restart the application is to kill it with **CTRL-C** and restarting it with `flask run` (but it should update automatically as you save changes)

1. *(6 points)* Modify the source code to remediate the flaws.

    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

2. *(2 points)* Test your changes
    a. **Provide screenshots** documenting the proper operation of the application without vulnerabilities.