CS 1122 Project 2: Sprint 3

This is the final portion of project 2. In Sprint 1 and 2, you were asked to investigate, identify, and exploit vulnerabilities in a python web application. Fixing problems is just as important as finding problems. That's why Sprint 3 will focus on fixing these vulnerabilities.

Task 1: Identify the root of the issue

Using the provided source code (located in the Project 2 section of the Resources repo) of the application, you must find the lines of codes that cause each of the vulnerabilities you identified in Sprints 1 and 2. If it is not possible to identify code that causes the vulnerability, you will need to explain what the root cause is.

Task 2: Fix the issue

Modify the code you have identified to resolve the security vulnerability. **Do not** delete the original line of code! Comment it out. Additionally, add a brief comment in the code above the new code you write describing the vulnerability you are patching and how the new code fixes it. Do not write more than a sentence.

If one of your vulnerabilities cannot be fixed by modifying the source code, provide detailed instructions on how to fix the vulnerability.

Task 3: Justify your fix

Explain how your modifications in the source code (or otherwise) prevent the vulnerability. Is there a possible scenario where an attacker can bypass the fix you implemented?

What to turn in

Your final submission for Project 2 will be a report summarizing your findings, as well as the modified source code.. Your report may either be in markdown, uploaded as README.md, or in PDF format. The report must be in the master branch of your project 2 repo by the deadline (Sunday, April 15th 11:55 PM).

The report must follow the specified format:

- Cover page with the following information
    - Group Number
    - Full names and net IDs of each group member
- 1 paragraph summary of vulnerabilities discovered
- For each vulnerability you must
    - Identify the type of vulnerability (ex; XSS, CSRF, etc.)
    - Explain how the vulnerability works. What is the impact/severity? Be specific.
    - Explain where this vulnerability exists in the application. Be specific. Include code snippets with line numbers and file name (if applicable).
    - Explain how you exploited this vulnerability step by step. Be specific. Include any code you wrote.
    - Explain how you fixed the vulnerability. (All the tasks from above)
- 1 paragraph describing distribution of work throughout the project
- EXTRA CREDIT: What did you enjoy about this project? What was easiest and what was most difficult? What would you change about this project?