Class: CS499 Computer Science Capstone

Professor: Ramsey Kraya, PhD

Student: Anna Fisher

Date: 2/16/2025

1. **Briefly describe the artifact. What is it? When was it created?**

I included my original artifact the Project Two Dashboard, which was created approximately a year ago. I also included my new revised artifact Revised Dashboard With Authentication CS340, which I created this week. In my original project, we hard coded a username and password to utilize in the Python script, in real life it is much more secure to include user authentication within the script.

1. **Justify the inclusion of the artifact in your ePortfolio. Why did you select this item? What specific components of the artifact showcase your skills and abilities in software development? How was the artifact improved?**

I selected this item to demonstrate my security mindset and how I anticipate adversarial exploits. Protection of data is not only important from an internal perspective to ensure integrity and access to data, there are legal implications as well. This artifact is a great representation of my ability to think about security of data and my ability to implement software solutions within my code to appropriately provide security. The artifact was improved in several ways. First, I implemented a login, user authentication process. When the user lands on the initial page, they will be prompted to login with their registered username and password. This is an important improvement over my initial artifact which only included a hardcoded username and password to access the MongoDB records. In real life, an employer would expect implementation of a login screen with user authentication to protect the business data. This authentication process includes thoughtful messages to inform the user what they need to do – for example, “Please Login Here to Begin”. I also chose to utilize red color label styles to make the login process more obvious to the user. Another important improvement I made was password hashing available with the hashlib module. The purpose of password hashing is to securely store the user passwords by transforming it into a scrambled unreadable string of characters (known as hash) which cannot be easily reversed to get the original password back. If a cyber criminal gains access to our database, they would not be able to read the original passwords. I added the hashlib module with SHA\_256 hash algorithm to take the user entered password, transform the entry into a scrambled unreadable string of characters and store as a hashed password. When the user attempts to log in, the password they enter on the page is hashed and compared to the stored password hash for authentication. This showcases my ability to provide a very secure method for user authentication and login functionality.

1. **Did you meet the course outcomes you planned to meet with this enhancement in Module One? Do you have any updates to your outcome-coverage plans?**

I believe I met the course outcome I planned to complete with this enhancement, because I was able to modify my dashboard to include user authentication for a database. I demonstrated my ability to think with a security mindset, providing protection of data through user authentication. I was able to build a login page and add the hashlib module with SHA256 hash algorithm for secure password storage and authentication. I was able to effectively and professionally articulate the purpose of my code utilizing in line comments. This demonstrates my ability to work and communicate within a team of developers. Realistically, I would like to include a more comprehensive login functionality, including a registration process for a brand-new user and the ability to retrieve a forgotten username or password. I did not include that functionality for this artifact, but I do think that is important to include and I believe most users would expect it for login functionality.

1. **Reflect on the process of enhancing and modifying the artifact. What did you learn as you were creating and improving it? What challenges did you face?**

It was challenging not having the original data file from MongoDB to be able to unit test the login process while trying out my new code for user authentication. In real life, I would unit test various scenarios to ensure new users can set up a login, existing users can login, and when a login fails the user receives notification and cannot access the system. For this activity I had to rely solely on my research of the hashlib module, plotly, app callbacks, and hashing to implement user authentication on the dashboard. To research user authentication, I referenced the following Python documentation: <https://docs.python.org/3/library/hashlib.html> and <https://dash.plotly.com/basic-callbacks> and <https://dash.plotly.com/dash-html-components/output>