Caden Weiner

Cyber Security, Cpts 427

Investigating Password Security Techniques combined with Two Factor Authentication to Create a More Secure Login Experience: Milestone 1

In this project I have so far created the framework for a basic website using the flask framework for python. There exists login functionality and a basic sqlite database to store usernames and passwords. I also implemented my own hashing and salt system as well as using an existing framework. I have implemented basic unit tests for passwords and need to look into enabling multi factor authentication and researching the feasibility of cracking a users password.

Status of the Project

- Website created and database initialized using the Flask Framework for python.
- Login set up using the flask_login library
- Login limitations set in place (Failed Attempt Timeout, password requirements)
- Testing login functionality with unit tests.
- Creating my own hash+salt function and finding existing libraries as well.

Milestone 2, expected by 7/17/2021

Implementing sms messages for multi factor authentication. Investigating other ways to implement multifactor authentication using a secondary device. Improving salt and hash functions to try and be able to create unique salt and hash functions for each user.

Final Project: expected by 7/31/2021

Wrapping up any improvements needed for Milestones 1 and 2 as well as implementing different tests to see if it is possible to crack different passwords that are less secure if they are salted and hashed vs not salted and hashed. Look into different methodologies for choosing passwords and ways to enforce more secure passwords. Would creating a new library specifically for passwords using symbols like emojis be effective?