WAPH-Web Application Programming and Hacking

Instructor: Dr. Phu Phung

Bridget May

Name: Bridget May

Email: mailto:mayb05@udayton.edu

Short-bio: Hi! My name is Bridget May! I am a senior at the University of Dayton studying computer science and graphic design.

Figure 1: My headshot

Repository Information

Respository's URL: https://github.com/mayb05/waph-mayb05.git

This is a private repository for Bridget May to store all code from the course. The organization of this repository is as follows.

Project 2 Overview

Project link: https://github.com/mayb05/waph-mayb05/tree/main/labs/lab1
Video link: https://youtu.be/MaWZH1VHObg

In this project, I created a website for users to create an account, view their information, edit it, and change passwords securely. Using the security principles

used in class, I secured my website from SQL injection, XSS attacks, and session hijacking.

Objectives:

Security My application is deployed over https and the passwords are hashed using MD5 (even when you change passwords, the pass is hashed again.) I also used a seperate account in MySQL to avoid further issues. My login, display data, and change password all use prepared statements.

Input Validation Passwords and other fields are sanitized to prevent issues to the database. The password is required to be certain criteria before being accepted.

Database Design My database is used by doing prepared statements whenever being queried and preventing code from being injected to it. I used a seperate account from the root to prevent full access to my database incase of data breach.

Front-End My website uses a Bootstrap/CSS theme and HTML to create a sleek look. The primary colors are light blue and and pink which makes a cotton candy feel. Inputs are required to have criteria before being accepted to promote security.

Session Management The important forms like changing passwords and editing names are protected by the session_auth.php file which checks the user's browser and cookie information to prevent session hijacking.