ID: 180917

Course: Web & Mobile Application Development II

Date: March 29, 2019

Class Summary

In the class of the date shown above we were reminded about the importance of hashing passwords before storing them in databases. Choosing appropriate hashing algorithm is important. Using a weaker hashing algorithm (an algorithm with fewer bit length) results in an increased number of collisions whereas choosing a hashing algorithm that is too strong will result in a case where what is lost in efficiency will not be gained in security. For example, using current technology, a 256 bit hash will take an eternity to break, as would 512 bit hash, however a 512 bit hashing algorithm requires more system resources, to execute, therefore a 256 bit hashing algorithm would be the optimal choice.

During the classtime the lecturer explained the logic of a simple student portal flask application and how form data is to be handled on the backend. For the class exercise we were required to modify a flask application that allows a user to log in and view posts made by administrators. What I have managed to accomplish in the time is to incorporate a mysql database instead of the former sqlite database and allowed registering users to submit a profile picture to the database. The format used for the pictures is base64 encoding where the encoded data would be stored in a longtext mysql database column in the Users Table. When a user signs in the picture is rendered into the index template, which displays their profile picture once the page has loaded.