Aaron Hanks

CS4460-001

Assignment 3

Assignment Analysis Report

1. I consider my password requirements to be strong. I require passwords to be at least 12 characters long, containing at least one of: lowercase letters, uppercase letters, numbers, and special characters. The permitted special characters are characters on the number keys. This provides 72 possibilities per character of the password, so at least 12^{27} possible passwords. On average, at 1 billion passwords per second, these passwords will take about $8 \cdot 10^{60}$ years to crack.
2. I store my passwords in the server/data/passwd.txt file the data entries in this file contain the user_id, username, and password hash generated by the bcrypt hashpw function, each delimited by commas. For example:

   ```
   user_id,username,password_hash

   67d041da-5707-499d-be0f-751e0fca90e3,admin,$2b$12$rUWoxB1KSsP245TZUsPP5.PQN4RCiArztCtsVhIHklGyBvshhA//6
   ```

3. Role based access controls were implemented using the server/data/access.txt file. Each entry is a role, followed by the actions that can be performed by that role, delimited by commas. When an action needs to be performed, the system first gets the user's role, and retrieves the actions available to that role. If the action that is being attempted is in the list of actions available to that role, the action is allowed, otherwise, the action is denied.
4. The events being logged are:
   a. Login
   b. Change of password
   c. Change of user data
   d. Calculation
   e. Retrieving calculations performed
   f. Retrieving all users
   g. Add user
   h. Remove user

   Each event is logged with the timestamp, the user that performed the action, the action itself, and whether it succeeded or failed.

The link to my demo video:
https://drive.google.com/file/d/17sNHsyBoCLDixulobIatnyjbiynjhoxB/view?usp=share_link