User Account Creation & Deletion

These were supposed to be done by Steven and Nathan and we were unable to finish them.

User Account Recovery

Success Outcomes

- Account Recovery Submission: The user provides a valid username and OTP, which is validated by the system and the user is allowed back in.
- MFA Recovery Submission: User successfully answers their security question and is allowed access into their account.

Failure Outcomes

- Account Recovery Submission: The user provides an invalid username or OTP. Message displays “Invalid username or OTP provided. Retry again or contact system administrator”
- Account Recovery Submission: The user’s OTP expires after 2 minutes have passed.
- Account Recovery Submission: The user provides correct credentials, but the request is not completed successfully.
- MFA Recovery Submission: The system is unable to fetch the user’s security question.
- MFA Recovery Submission: The user provides an invalid or incorrect answer to their security question. Message displays “Invalid or incorrect answer submitted. Retry again or contact system administrator”
- MFA Recovery Submission: The user provides the correct answer, but the request is not completed successfully.
- Account/MFA Recovery Submission: System does not complete execution of a step within 3 seconds of invocation.
- Account/MFA Recovery Submission: System Message does not display within 3 seconds of invocation.

Classes/Interface

Public Class UserRecovery

- Attributes:
    - Username: Username of the user attempting account recovery.
    - OTP: One-time password given to the user.
    - securityCode: holds inputted security code, only used for MFA recovery.
    - otpTimestamp: Time the OTP was created.
    - Timestamp: Time of initial recovery request.
    - failedAttempts: total number of failed attempts.
    - lastFailedAttempt: time of last failed recovery attempt.
    - validCred: true if username + otp are valid, false otherwise.
    - securityQuestion: user’s security question, pulled from database.
    - securityAnswer: user inputted answer to their question.

Public Class Recovery

- Methods:
    - Result recoverDisabledAccount(string username)
        - Takes a given, already validated username, and creates a user recovery object.
        - Sends a new OTP to users registered email/phone number.
        - Then has the user input the OTP before creating a recovery request to be stored in the system.
    - Result recoverMultiFactor(string username)
        - Takes user’s username, then pulls the associated security question from the database Both are stored in a new user recovery object.
        - User then inputs an answer, which is hashed and compared to the stored hashed answer in the database.
        - If they match, the user is allowed back in.

        - The user gets 5 attempts before being locked out.
    - bool isValidUsername(string username)
        - Checks if the given username follows the core requirements.
        - Can just call this from auth
    - bool isValidOTP(string otp)
        - First it checks if the OTP was created less than two minutes ago.
        - Checks if the inputted OTP follows the core requirements.
        - Can just call this from auth
    - bool validateCred(string username, string hashedOTP, string hashedSecurityAnswer)
        - If OTP is null, compares hashed security answer with database, and vice versa.
        - OTP and SecurityAnswer should be hashed before comparing it with the database.
        - Returns true if the OTP or answer hashes match.
    - Result approveRecovery(string username)
        - Only executes if either of the recovery methods results in a success.
        - Updates database to set user's isDisabled value to false, and failedAttempts to 0.

User Stories

- For all users:
    - As a user of the system, I want to securely regain access to my account if it has become unavailable or disabled.
    - As a user of the system, I want to securely regain access to my account if I have lost access to my phone number or email I use for multi-factor authentication.