Assignment 1: Two-Factor Authentication

Amma Annorbea Offei - Larbi, David Abeiku Saah

Ashesi University

IS451: Information Security Systems

Dr. Godvinha Yeluripati

October 8, 2024

System Architecture Overview

Demo video: https://youtu.be/P5b_0dOqOW0

Workflow of the system

1. **User Registration**:
    - **Process**: The user registration system collects the following information: username, password, and email for OTP delivery.
    - **Password Security**: The password is hashed using bcrypt before being stored in the database to enhance security, ensuring that plaintext passwords are never saved.
    - **Client validation:** Validation via pattern matching on the client is done to ensure the right information is sent by the user.
    - **Server validation:** Validation on the server to prevent duplicate email and/or username sign ups.
    - **Database Storage**: The registration information is stored on the database.
    - **Error handling:** In the case of errors, they are sent to the user from the server without crashing the software.
2. **Login Process**:
    - **Login Flow**: Users enter their username and password into a login form. The entered password is hashed and checked against the stored hash in the database.
    - **Validation**: If the hashed password matches the stored hash for the given username, the login proceeds to the OTP generation stage. Also, if the

username or password is incorrect, a message is sent to the user from the server.

- **Error Handling**: A generic error message is displayed for incorrect usernames or passwords without specifying which part of the credentials was incorrect. This helps prevent information disclosure to potential attackers.

3. **OTP Generation and Verification**:
   - **OTP Generation**: Upon successful password validation, a one-time password (OTP) is generated using a random number generator to ensure uniqueness and unpredictability.
   - **OTP Delivery**: The OTP is sent to the user via email using PHP's mailer function.
   - **Expiration**: The OTP is configured to expire after 3 minutes and can only be used once, minimising the risk of replay attacks.
   - **OTP Verification**: The user is prompted to enter the received OTP. The system checks if the entered OTP matches the generated one and is not expired.
   - **Access Granting**: The user can access the system if the OTP is correct and has not expired. Otherwise, a message indicating a wrong or expired OTP is displayed, prompting the user to retry.
4. **Error Handling**:
   - **Invalid Credentials**: A user-friendly error message appears if the username or password entered is incorrect.
   - **OTP Errors**: An error message is shown if the OTP is incorrect or expired, allowing users to request a new OTP by logging in.

Security Controls

1. **Password Security**:
    - **Hashing Algorithm**: Passwords are securely stored using a hashing algorithm (brcypt), preventing plaintext passwords from being exposed in case of a data breach.
2. **OTP Expiration**:
    - **Timed Expiry**: The OTP expires after 3 minutes, reducing the time window in which an attacker could intercept or use it.
    - **One-Time Use**: Each OTP can only be used once. Upon successful login, the OTP is marked as used, and any further attempts with the same OTP are invalid.
3. **Validation Checks**:
    - **Input Validation**: Registration and login input are sanitised to avoid SQL injection attacks.
    - **Error Feedback**: Error messages are generalised to prevent attackers from deducing specific information about the account credentials.

Potential Security Attacks and Countermeasures

1. **Brute Force Attacks**:
    - **Complex Password Requirements**: Users are encouraged to use complex passwords to prevent brute-force attacks from succeeding quickly. The pattern is: the password must be at least 8 characters long, must include a letter (upper and lower case), a number and a special symbol

2. **Replay Attacks**:
    - **OTP Expiration**: By enforcing a strict expiration time for OTPs, replay attacks are mitigated, as intercepted OTPs will likely be invalid when used.
    - **One-Time Use**: OTPs can only be used once per session, reducing the replay risk.