Secure Software System Development

Project Requirements

Registration Process:

Full Name: The user must provide their full name during registration.
Username:

- Must be unique across the system.
- Should be longer than 3 characters.
- Can only include alphanumeric characters (letters and numbers), no special characters or spaces are allowed.
- Validate against a list of “reserved” names (prevent **admin** etc..)

Password:

- Must not be a commonly used password.
- Integration with the external database Have I Been Pwned to check password strength and uniqueness.
- Should be at least 8 characters long.

Email Address:

- Needs to follow a valid email format (example@domain.com).
- Validate the domain extension from https://data.iana.org/TLD/tlds-alpha-by-domain.txt
- Validate the domain name by checking MX records to ensure it's a legitimate and active domain.

Phone Number:

- Must be unique.
- Must be a mobile number
- Validate the format using the Google phone library.

Email Confirmation: After registration, send a confirmation email to the user with a link to verify their email address.

Login Process:

Username/Email: Validate whether the entered username or email exists in the database.
Password: Check if the entered password matches the one stored in the database.
Account Security:

- Implement Captcha after 3 failed login attempts and log these attempts.
    - Log failed attempts
- Introduce a second authentication step (2FA) which include:
    - SMS verification.
    - Time-based one-time passwords (TOTP) using an authenticator app like Google Authenticator, Microsoft Authenticator, etc.
    - Email-based verification code.
    - (Optional) Support for security keys like Yubico.
    - Provide recovery codes for 2FA as a backup method.

Forgot Password:

Email Verification: The user must provide their email to initiate a password reset.
Attempt Limit: Limit password recovery attempts to 2, after which a captcha is displayed.
Reset Link: Send an email with a password change link that:

- Expires in 5 minutes.
- Can only be used once.
- Limit the number of tries to 2 in the last 10 minutes.

Password Reset: Allow the user to set a new password.
Confirmation Email: Send an email confirming that the password has been changed.

Welcome Area (Post-Login):

Personalized Greeting: Display a welcome message with the user's name.
Security Settings: Allow users to update their 2FA settings.
Password Change: Provide an option to change the password.
Logout: Enable users to log out of their accounts.

Suggested flow

Follow the registration and login flow on GitHub.

Technical Stack and Implementation Details:

- Backend: Use PHP with MySQL/MariaDB for the database.
- Framework: Utilize FlightPHP for building the API.
- API Documentation: Use OpenAPI (Swagger) to document all API endpoints.

- API-Centric: All functionalities should be exposed as REST API endpoints, ensuring all validations are handled on the API side.
- Frontend: Note that the frontend will not be graded, the focus should be on the backend API.

Regular commits

Fridays by 12:00 (for all groups)