SECURITY OF INPUT FIELDS

The registration form you provided incorporates several security measures to enhance the overall security of the user registration process. Here's an explanation of these security measures:

Password Policy Validation:

The validatePassword function enforces a password policy, ensuring that passwords meet specific criteria:

Minimum length of 8 characters.

At least one uppercase letter.

At least one lowercase letter.

At least one digit (number).

At least one special character.

Input Validation and Sanitization:

The htmlspecialchars function is used to sanitize user input, preventing potential Cross-Site Scripting (XSS) attacks. It converts special characters to their HTML entities, ensuring that user input is safely rendered in the HTML output.

Password Hashing:

The user's password is hashed using the password\_hash function before being stored in the database. Password hashing is a crucial security measure to protect user passwords. It ensures that even if the database is compromised, the actual passwords remain secure.

Prepared Statements:

Prepared statements are used in the database queries. This protects against SQL injection attacks by separating SQL code from user input. The use of placeholders and binding parameters helps prevent malicious SQL code execution.

Error Handling:

The code includes try-catch blocks to handle exceptions, particularly PDOException for database-related errors. This prevents sensitive information from being exposed in error messages. Different error messages are displayed based on the type of error, improving user experience and security.

Unique Constraint Violation Handling:

The code checks for unique constraint violations (e.g., duplicate email or code) and provides a user-friendly error message. This prevents attackers from exploiting such constraints to enumerate valid user accounts.

Limited Error Disclosure:

The code avoids providing detailed error messages to users. Instead, it offers generic error messages to prevent potential attackers from gaining insights into the system's internal workings.

Conditional Execution:

The registerUser function only proceeds with user registration if the password passes validation and there are no other error messages. This ensures that the registration process is halted upon detecting security issues.

Server-Side Validation:

While client-side validation is common for improving user experience, server-side validation (in PHP) is crucial for security. Client-side validation can be bypassed, and server-side validation acts as a safety net to catch any potential manipulation or bypass attempts.

By incorporating these security measures, the registration form aims to mitigate common security risks associated with user input, password storage, and database interactions.