Login functionality for an online banking website must be implemented using PHP because PHP operates on the server side, where sensitive data can be processed securely. JavaScript runs on the client side, meaning its source code is fully visible and accessible through the browser's developer tools. If login verification were handled by JavaScript, a malicious user could easily inspect or modify the code to bypass authentication checks.

Additionally, client-side password validation would expose security logic, allowing attackers to manipulate input values or force the system to return a successful login. Another major risk is that passwords could be intercepted or manipulated before being sent to the server, leading to credential theft.

Server-side processing with PHP ensures that authentication logic, database queries, and password verification remain hidden from users. This fundamental separation between client-side presentation and server-side security is essential for protecting sensitive financial information and maintaining system integrity.