DVWA Cross-Site Scripting Assessment

Client-side security and session protection

Overview

Tested reflected and stored cross-site scripting behavior in a deliberately vulnerable training application. The assessment examined how unencoded browser output can affect users and sessions.

Approach

- Validated reflected and stored client-side injection in a controlled training environment.
- Reviewed session-cookie protections and the potential impact of script execution.
- Documented defensive controls appropriate to the application context.

Key findings

- Unencoded user-controlled content could execute in a visitor's browser.
- XSS can put client-side data and authenticated sessions at risk.

Defensive recommendations

- Apply context-aware output encoding and a Content Security Policy.
- Use Secure and HttpOnly cookies, session rotation, and sensible session timeouts.

Publication note: This is a sanitized portfolio summary. All testing was performed in intentionally vulnerable, isolated training environments. Target identifiers, credentials, payloads, screenshots, and step-by-step exploitation instructions have been omitted.