White-Box Command Injection Review

Source-code review and secure remediation

Overview

Reviewed a deliberately vulnerable DNS lookup feature with source-code access. The assessment identified unsafe handling of user input that could reach operating-system command execution.

Approach

- Traced user-controlled input through the application flow.
- Classified the weakness as OS command injection (CWE-78).
- Evaluated the impact and proposed defensive alternatives.

Key findings

- Unvalidated input was passed to shell execution.
- Missing access controls and output encoding increased the potential impact.

Defensive recommendations

- Use native language APIs instead of shell execution.
- Apply strict allowlists, least privilege, output encoding, and logging.

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.