Black-Box Web Security Assessment

Reconnaissance, validation, and remediation

Overview

Performed an authorized black-box assessment in an isolated lab. The work moved from service and web-surface discovery to controlled validation of an input-handling weakness.

Approach

- Performed high-level service discovery and web-content enumeration.
- Tested application input handling in the defined lab scope.
- Recorded impact evidence without exposing target-specific access details.

Key findings

- An unauthenticated web feature accepted unsafe input.
- Legacy services and weak permission practices increased the attack surface.

Defensive recommendations

- Remove shell-dependent application behavior.
- Reduce exposed services, enforce least privilege, and monitor suspicious input.

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.