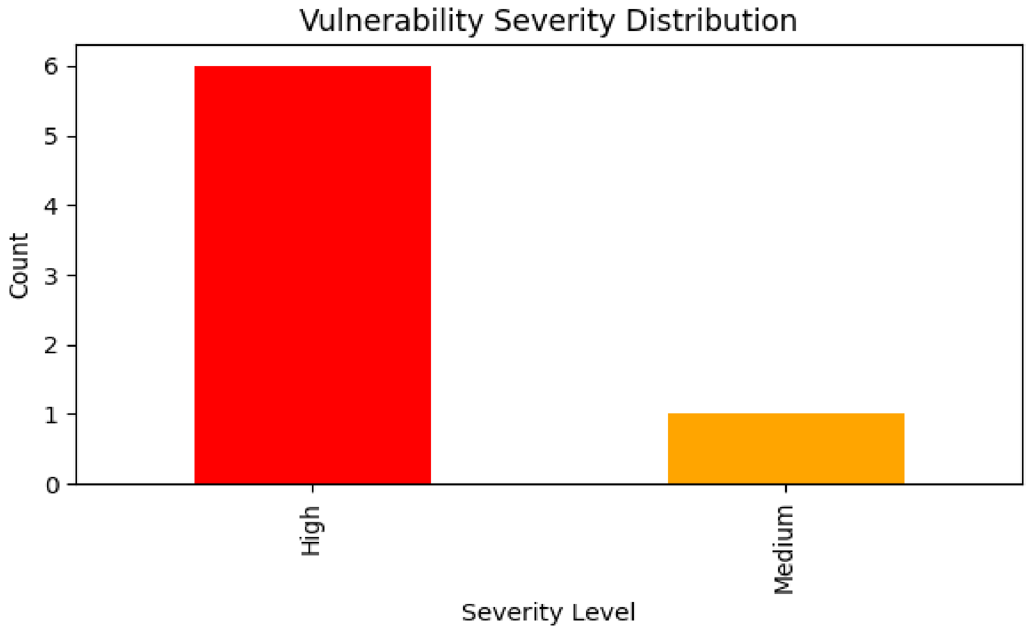
Web Application Security Testing Report

Total Vulnerabilities Found: 7



XSS (Stored): http://localhost/vulnerabilities/xss_s/ (High)
Evidence: Stored payload visible
Mitigation: Store clean input only, use output encoding and server-side filtering.

XSS (Reflected): http://localhost/vulnerabilities/xss_r/?name=alert(1)&Submit;=Submit (High)
Evidence: Payload reflected in response
Mitigation: Sanitize user input, implement HTML encoding and enable Content Security Policy (CSP).

XSS (DOM): http://localhost/vulnerabilities/xss_d/ (Medium)
Evidence: Dangerous DOM sink detected
Mitigation: Avoid writing raw user input to DOM, use safe JavaScript methods.

auth: /login.php (High)
Evidence: Weak/default credentials allowed
Mitigation: Enforce strong password policy, lockout mechanism and 2FA.

IDOR-Horizontal: http://localhost/vulnerabilities/xss_s/?id=1 (High)
Evidence: User data accessed without permission
Mitigation: Implement access control checks before serving user-specific data.

IDOR-Horizontal: http://localhost/vulnerabilities/xss_s/?id=2 (High)
Evidence: User data accessed without permission
Mitigation: Implement access control checks before serving user-specific data.

IDOR-Horizontal: http://localhost/vulnerabilities/xss_s/?id=3 (High)
Evidence: User data accessed without permission
Mitigation: Implement access control checks before serving user-specific data.