Performance & Security Testing Report

Website: testphp.vulnweb.com

1. Functional Testing

Functional testing ensures that different features of the site work as expected.

Tested Pages:

- /login.php - User authentication page.
- /search.php - Search functionality.
- /admin.php - Admin panel access.
- /cart.php - Shopping cart page.

Key Findings:

- SQL Injection (SQLi) vulnerability in /login.php.
- Cross-Site Scripting (XSS) in /search.php.
- Admin panel lacks proper access control.
- Shopping cart is vulnerable to parameter tampering.

2. Performance Testing

Performance testing evaluates the system's response under different load conditions.

Load Testing Results:

- 100 Virtual Users: Avg Response Time 470ms [PASS]
- Peak Response Time: 1100ms [FAIL] (High Latency)
- Failure Rate: 5.8% [FAIL] (Above 1% threshold)

Stress Testing Results:

- Site starts degrading at 200 users, fails at 400 users.
- High response time and errors indicate database overload.

Optimization Needed:

- Optimize database queries & implement caching.
- Improve session management to handle user load.

3. Security Testing Findings

Vulnerabilities Identified:

- SQL Injection (SQLi) allows bypassing authentication [FAIL]
- Cross-Site Scripting (XSS) allows script execution [FAIL]
- Weak session management [FAIL]
- Parameter tampering in cart [FAIL]

Recommendations:

- Sanitize inputs to prevent SQLi & XSS.
- Restrict access to /admin.php.
- Implement session expiration & token-based authentication.
- Validate and sanitize URL parameters.

4. Conclusion

[PASS] Key Takeaways:

- Severe security vulnerabilities (SQLi, XSS, parameter tampering) detected.
- Performance stable up to 100 users, fails beyond 200 users.
- Stress testing indicates system failure at 400 users.

[NOTE] Next Steps:

1. Fix security vulnerabilities (SQLi, XSS, and session management).
2. Optimize database queries & caching for better performance.
3. Re-test after implementing security and performance enhancements.