Student Name:Samuel Adeduntan
University:Olabisi Onabanjo University
Major: Computer Science
Internship Duration:April 10th, 2025 - May 3rd, 2025
Company:Hack Secure
Domain: Cyber Security
Mentor:Mr.Nishant Prajapati
Assistant Mentor: Mr. Aman Pandey
Coordinator: Mr. Shivam Kapoor

Penetration Testing Report

Target: http://testphp.vulnweb.com

Executive Summary

A comprehensive penetration test was conducted on http://testphp.vulnweb.com to assess vulnerabilities across multiple attack vectors. Critical findings include:

- Exposed admin panel with default credentials (test:test).
- SQL Injection (SQLi) in artists.php and login pages.
- Reflected XSS via search parameters.
- Cleartext credential transmission over HTTP.
- Minimal open ports (only port 80), but misconfigured services (nginx 1.19.0, PHP 5.6.40).

Overall Risk: Critical due to data exposure, authentication flaws, and lack of encryption.

Methodology

- Reconnaissance: Nmap scans, directory enumeration (dirb, gobuster).
- Vulnerability Exploitation: SQLi, XSS, credential interception.
- Post-Exploitation: Admin panel access, data extraction.
- Traffic Analysis: Wireshark for HTTP plaintext analysis.

Task-Specific Findings

Task 1: Directory Enumeration & Admin Panel Exposure

Tools: dirb, gobuster

Findings:

- Accessible paths: /admin/, /secured/, /CVS/ (source control).
- Admin panel (http://testphp.vulnweb.com/admin/) accessible with default credentials (test:test).
- Exposed PII: Credit card numbers, emails, addresses.
- Risk: Critical (CVE-2025-XXXX).

Task 2: Port Scanning & Service Enumeration

Tool: Nmap

Findings:

- Only port 80/tcp open (nginx 1.19.0).
- No SSL/TLS (HTTPS missing).
- OS detection inconclusive due to TCP wrappers.
- Risk: Medium (misconfiguration).

Task 3: Reflected XSS Vulnerability

Endpoint: http://testphp.vulnweb.com/search?query=<script>alert('XSS')</script>

Impact:

- Session hijacking, phishing, malware delivery.
- Risk: High (exploitable via malicious links).

Task 4: SQL Injection (SQLi)

Vulnerable Pages:

- artists.php?artist=1 (Payload: ' OR 1=1 --).
- login.php (Brute-force bypass).

- Impact: Full database compromise (e.g., acuart DB).

Risk: Critical.

Task 5: Cleartext Credential Transmission

Tool: Wireshark

Finding:

Login credentials (uname=admin&pass=password1234) sent over HTTP.

Risk: Critical (network sniffing).

Task 6: Incident Response Playbooks (SOC)

Key Actions:

Developed IR playbooks for identification, containment, recovery.

Tools: Splunk, Sysmon, EDR solutions.

Task 7: Splunk Investigation (Exchange Exploits)

Findings:

- Monitored lateral movement, persistence tactics.
- Detected credential dumping attempts.

Risk Assessment Summary

Vulnerability	Severity	Likelihood	Impact
Default Admin Credentials	Critical	High	Data breach
SQL Injection	Critical	High	DB compromise
Reflected XSS	High	Medium	Session hijack
HTTP Cleartext Transmission	Critical	High	Credential theft
Open Port 80 (No HTTPS)	Medium	High	Misconfiguration

Recommendations

1. Authentication:

- Change default credentials; enforce MFA.
- Implement account lockouts for brute-force protection.

2. Input Validation:

- Sanitize user inputs to prevent SQLi/XSS.
- Use prepared statements for SQL queries.

3. Encryption:

- Deploy HTTPS (TLS 1.2+).
- Enable HSTS and disable HTTP.

4. Web Server Hardening:

- Update nginx/PHP (EOL versions).
- Restrict directory listings (/CVS/, /admin/).

5. Monitoring:

- WAF for XSS/SQLi filtering.
- Regular Splunk audits for anomalies.

Conclusion

The target exhibits severe security flaws requiring immediate remediation. Critical risks include data exposure, authentication bypass, and lack of encryption. Patching, hardening, and continuous monitoring are essential to mitigate threats.

Appendices

Raw Data: Nmap scans, Wireshark captures, sqlmap outputs.

Screenshots: Admin panel access, XSS/SQLi proof-of-concept.