Vulnerability Assessment & Penetration Testing (VAPT) Report

Target: testphp.vulnweb.com

1. Executive Summary

For Non-Technical Management

This report summarizes the findings of a vulnerability assessment performed against the target web application, focused on configuration and server components.

Key Finding: The target is running an outdated, End-of-Life (EOL) version of its core web server component (PHP 5.x). This exposure is **Critical**, as the software contains numerous publicly known and easily exploitable vulnerabilities (CVEs).

Overall Risk: High. The documented component disclosure confirms the presence of easily exploitable flaws that could lead to remote code execution (RCE) or information disclosure if targeted by an attacker.

Immediate Recommendation: Patching and component upgrade must be prioritized immediately to remove all known public risks and safeguard the environment.

2. Scope and Authorization

Target: The external HTTP service running on testphp.vulnweb.com. **Authorization:** The target is a designated practice site; permission for non-destructive, lab-based testing is assumed. **Limitations:** The assessment was strictly external and **non-destructive**. No interactive input fields suitable for deep injection validation were found, thus the focus remained on server-side component analysis.

3. VAPT Objectives and Methodology (High-Level)

The assessment followed a methodical, non-intrusive approach to identify configuration weaknesses and component flaws.

Methodology Phase	**Purpose**	**Tools Utilized (Sample)**
Port and Service Scan	Identify open ports and the specific services running.	Nmap

Automated Vulnerability Scan	Scan for common misconfigurations and software versions.	Nikto
Passive Traffic Inspection	Manual review of HTTP headers and server responses.	Burp Suite

4. Key Finding Summary: EOL Component Risk

The most significant threat identified is the active use of **PHP 5.x**. This version is no longer supported by the vendor, meaning security patches for critical flaws are not being released. This creates an enormous window of opportunity for attackers leveraging publicly available exploits.

Risk Implication: The risk is not theoretical; it is based on the existence of known, documented vulnerabilities (CVEs) that affect this specific version.

5. Detailed Findings and Vulnerabilities

ID	Finding/Exposure	Category	Severity	Simple Explanation
V-01	**Outdated PHP Server Component**	Component Disclosure / EOL Software	**CRITICAL**	The server component version is past End-of-Life (EOL), making it vulnerable to numerous public exploits, potentially leading to Remote Code Execution (RCE).

V-02	Missing XSS Protections (Inferred)	Input/Output Handling	**HIGH**	The application's configuration suggests a high likelihood of Cross-Site Scripting (XSS) due to standard framework practices, should suitable user input fields be present.
V-03	Missing HTTP Security Headers	Server Misconfigurati on	Medium	The web server is missing modern security headers (e.g., CSP) necessary to protect users against common browser-base d attacks.

6. Risk Assessment Matrix

We assessed the risk based on the potential Impact (damage caused) and Likelihood (ease of exploitation).

Finding ID	**Likelihood**	**Impact**	**Overall Risk**	**Justification**

V-01 (Outdated PHP)	High	Critical	**CRITICAL**	Easy to exploit because CVEs are public; impact is RCE/system takeover.
V-02 (Missing XSS)	Medium	High	**HIGH**	Common flaw; impact is user session hijacking or data theft.
V-03 (Missing Headers)	Low	Medium	**MEDIUM**	Requires other flaws to be useful, but lowers overall defensive posture.

7. High-Level Remediation Strategy

Priority	**Recommendation**	**Action to Be Taken**
1. CRITICAL	**Patch and Upgrade PHP (V-01)**	Immediately update the PHP component to the latest stable, supported version (7.x or 8.x) and formalize a patch management schedule.
2. HIGH	**Implement Secure Coding Practices (V-02)**	Ensure all user-supplied output is properly encoded before being rendered to the user and implement strict input validation.
3. MEDIUM	**Configure Security Headers (V-03)**	Deploy modern HTTP security headers, including Content Security Policy (CSP) and

		X-Content-Type-Options, to harden the server response.

8. Proposed Remediation Timeline

This is a proposed plan based on the severity of the findings. The CRITICAL vulnerability must be addressed first.

Priority	Finding	Proposed Target Completion	Responsible Team
P-1 (Critical)	V-01: EOL PHP	**Immediately / 1 Week**	Infrastructure / DevOps
P-2 (High)	V-02: XSS Mitigation	3 Weeks	Development Team
P-3 (Medium)	V-03: Security Headers	4 Weeks	Web Server Administration

9. Distribution and Confidentiality

This report contains information regarding the operational components and potential security exposures of the application.

- **Distribution:** Restricted to authorized management and security personnel only.
- **Confidentiality:** This document is classified as **"Strictly Confidential"** and must not be shared externally under any circumstances.

10. Appendix: Technical Component Details

The full technical details, including raw Nmap and Nikto output, specific PHP version disclosures, and the CVE lookups (e.g., CVE-2019-0024), are located in the companion report: **Technical_Report.md** and the uploaded evidence file **Project 2.pdf**.