Vulnerability Assessment Report

Target website: testphp.vulnweb.com

Assessment type: Read only/passive

Prepared By: Harish Saud

Role: Cybersecurity Intern

Date:

1. Executive Summary

This Vulnerability Assessment was conducted to evaluate the security posture of the publicly accessible website **testphp.vulnweb.com** using **passive and non-intrusive testing techniques**. The objective of the assessment was to identify common configuration weaknesses, assess their potential business impact, and provide clear remediation guidance in a manner suitable for non-technical stakeholders.

The assessment was performed strictly within a **read-only scope**, focusing only on public-facing components of the application. No exploitation, authentication bypass, brute-force attempts, or denial-of-service activities were conducted during the engagement. The analysis relied on passive traffic inspection, configuration review, and service exposure analysis using industry-recognized tools.

During the assessment, a total of **seven security findings** were identified. These findings primarily relate to **missing security headers, absence of protective controls, and information disclosure through server configuration**. No **high-risk or critical vulnerabilities** were observed as part of this assessment; however, several **medium-risk issues** were identified that could increase the application's exposure to common web-based attacks if left unaddressed.

The most notable issues include the absence of a **Content Security Policy (CSP)**, missing **anti-clickjacking protections**, lack of **anti-CSRF mechanisms**, and disclosure of server software and version information. While these issues do not represent an immediate compromise of the system, they weaken the overall security posture and may assist attackers in executing client-side attacks or conducting targeted reconnaissance.

From a business perspective, these weaknesses may lead to **reduced user trust, increased attack surface, and higher risk of browser-based attacks**, such as clickjacking or malicious script execution. The identified issues are largely **configuration-level weaknesses** and can be mitigated through well-established security best practices with minimal operational impact.

It is strongly recommended that the organization prioritize the implementation of missing security headers, reduce unnecessary information disclosure, and periodically review server configurations to align with modern web security standards. Addressing these findings will significantly enhance the website's resilience against common threats and demonstrate a proactive approach to cybersecurity risk management.

2. Scope of Assessment

The scope of this assessment was limited to the **publicly accessible components** of the website **testphp.vulnweb.com**. The assessment was conducted under a **read-only scope**, ensuring no impact on system availability, integrity, or confidentiality.

In Scope

- Public-facing web pages
- HTTP response headers and configurations
- Client-side behavior observable via passive analysis
- Service exposure and basic network visibility

Out of Scope

- Authentication and authorization testing
- Login bypass or credential-based attacks
- Exploitation of vulnerabilities
- Brute-force attacks, fuzzing, or DoS testing
- Access to administrative or restricted resources

3. Methodology & Tools Used

Methodology

The assessment followed a structured approach:

1. Target identification and scope definition
2. Passive vulnerability detection
3. Security header and configuration analysis
4. Service exposure analysis
5. Risk classification and reporting

Tools Used

- **OWASP ZAP (Passive Scan)** – Identification of web configuration issues
- **Nmap** – Basic service exposure and version detection
- **Browser Developer Tools** – Manual inspection of headers and cookies

4. Risk Rating Criteria

Risk Level	Description
High	Issues that may directly lead to data compromise or system abuse
Medium	Security weaknesses that increase attack surface
Low	Information disclosure or best-practice gaps
Informational	Observations with no direct security impact

5. Summary of Findings

Vulnerability	Risk Level
Absence of Anti-CSRF Tokens	Medium
Content Security Policy (CSP) Not Set	Medium
Missing Anti-Clickjacking Header	Medium
Server Version Disclosure	Low
X-Content-Type-Options Header Missing	Low
X-Powered-By Header Disclosure	Low
Charset Mismatch	Low

6. Detailed Findings

Finding 1: Absence of Anti-CSRF Tokens

Risk Level: Medium
Source: OWASP ZAP

Description:
The application does not implement anti-CSRF tokens to protect against unauthorized requests initiated from external websites.

Business Impact:
An attacker could trick authenticated users into performing unintended actions, potentially affecting user trust and application integrity.

Evidence:
[Screenshot Required – OWASP ZAP alert showing Absence of Anti-CSRF Tokens]

Recommendation:
Implement anti-CSRF tokens for all state-changing requests to ensure requests originate from trusted sources.

Finding 2: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Source: OWASP ZAP

Description:
The website does not define a Content Security Policy to control permitted content sources.

Business Impact:
Increases exposure to browser-based attacks such as malicious script injection.

Evidence:
[Screenshot Required – ZAP alert showing CSP header missing]

Recommendation:
Define and enforce a strict Content Security Policy aligned with application requirements.

Finding 3: Missing Anti-Clickjacking Header

Risk Level: Medium
Source: OWASP ZAP

Description:
The application does not restrict framing by external websites.

Business Impact:
Users may be exposed to clickjacking attacks, potentially leading to unintended actions.

Evidence:
[Screenshot Required – Missing X-Frame-Options alert]

Recommendation:
Implement X-Frame-Options or CSP frame-ancestors directive.

Finding 4: Server Version Disclosure

Risk Level: Low
Source: Nmap & OWASP ZAP

Description:
The server discloses its software type and version (nginx 1.19.0).

Business Impact:
Provides attackers with reconnaissance information that may assist in targeted attacks.

Evidence:
[Screenshot Required – Nmap scan output showing nginx version]

Recommendation:
Suppress server version information in HTTP headers and server configuration.

Finding 5: X-Content-Type-Options Header Missing

Risk Level: Low
Source: OWASP ZAP

Description:
The application does not prevent browsers from MIME-type sniffing.

Business Impact:
May allow unintended execution of certain content types.

Evidence:
[Screenshot Required – Missing X-Content-Type-Options alert]

Recommendation:
Set X-Content-Type-Options: nosniff.

Finding 6: X-Powered-By Header Disclosure

Risk Level: Low
Source: OWASP ZAP

Description:
The server exposes backend technology details via HTTP headers.

Business Impact:
Assists attackers during reconnaissance.

Evidence:
[Screenshot Required – X-Powered-By disclosure]

Recommendation:
Disable or obfuscate technology disclosure headers.

Finding 7: Charset Mismatch

Risk Level: Low
Source: OWASP ZAP

Description:
Mismatch observed between HTTP response charset and HTML meta charset.

Business Impact:
May cause rendering inconsistencies and minor security concerns.

Evidence:
[Screenshot Required – Charset mismatch alert]

Recommendation:
Ensure consistent charset configuration across headers and HTML.

7. Network Exposure Analysis (Nmap)

Open Ports Identified:

- Port 80 (HTTP)

Service Detected:

- nginx 1.19.0

Risk Level: Low

Evidence:
[Screenshot Required – Nmap command and output]

8. Overall Recommendations

- Implement missing security headers
- Reduce unnecessary information disclosure
- Align server configuration with web security best practices
- Perform periodic security assessments

9. Conclusion

The assessment identified several configuration-level weaknesses that can be addressed with minimal effort. While no critical vulnerabilities were discovered, implementing the recommended controls will significantly improve the website’s security posture and reduce exposure to common web threats.

10. Appendix (Evidence)

- OWASP ZAP Alerts Summary – [Screenshot Required]
- Individual ZAP Findings – [Screenshots Required]
- Nmap Scan Output – [Screenshot Required]