VULNERABILITY ASSESSMENT REPORT

Target Website: http://testphp.vulnweb.com

Prepared by: Anjali Rakshale
Cyber Security Intern – Future Interns
Date: 13 Jan 2026

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report presents the findings of a passive vulnerability assessment conducted on the publicly accessible website http://testphp.vulnweb.com.

The objective of the assessment was to identify common security weaknesses using ethical, non-intrusive techniques without performing any exploitation or active attacks.

The assessment focused on publicly visible configurations, HTTP security headers, cookies, and exposed services using industry-standard tools.

Based on the analysis, several low to medium risk issues were identified. Addressing these findings will help improve the overall security posture of the website and reduce potential attack vectors.

INTRODUCTION

In today’s digital environment, websites play a critical role in business operations and user engagement. However, many websites are deployed with security misconfigurations that can expose them to potential risks if not regularly reviewed.

This report presents a **passive vulnerability assessment** of a publicly accessible website, conducted using ethical techniques without performing exploitation or active attacks. The assessment focuses on externally visible security weaknesses using industry-standard tools such as **Nmap** and **OWASP ZAP (Passive Scan)**.

The objective of this assessment is to identify common security issues and present the findings in a clear and easy-to-understand manner to support basic security improvements.

Scope of Assessment

The scope of this vulnerability assessment was limited to the publicly accessible website http://testphp.vulnweb.com.

The assessment focused solely on passive analysis techniques, including observation of HTTP requests, security headers, cookies, server responses, and exposed network services.

No authentication testing, exploitation, brute-force attacks, fuzzing, or denial-of-service (DoS) activities were performed as part of this assessment.

Methodology of Assessment

1.Target Website Selection

The publicly accessible website http://testphp.vulnweb.com was selected for assessment.

2.Passive Reconnaissance

The website was manually explored using OWASP ZAP to observe HTTP requests and responses without performing active attacks.

3.Security Header and Cookie Analysis

HTTP security headers and cookie attributes were analyzed to identify common security misconfigurations.

4.Network Exposure Analysis

A basic Nmap scan was performed to identify exposed network services using non-aggressive scanning techniques.

5.Vulnerability Identification

Observed security issues were identified based on passive scan results and tool observations.

6.Reporting and Documentation

All findings were documented, and supporting evidence was collected in the form of screenshots and scan outputs.

Findings Summary

ID	FINDING	Risk Level	Brief Description	Remediation
01	Missing Security Headers	Medium	Recommended HTTP security headers were not present in server responses.	Configure recommended HTTP security headers such as Content-Security-Policy, X-Frame-Options, and X-Content-Type-Options on the server.
02	Insecure Cookie Attributes	Medium	Cookies were observed without important security flags such as HttpOnly and Secure.	Set secure cookie attributes including HttpOnly, Secure, and SameSite to protect user sessions from misuse.
03	Information Disclosure via HTTP Headers	Low	Server and application details were exposed through HTTP response headers.	Remove or restrict unnecessary server and application information from HTTP response headers.

Finding 01: Missing Security Headers

Risk Level: Medium

Issue:
The website does not include several recommended HTTP security headers in its responses.

Why it matters:
Security headers help protect users from common attacks such as clickjacking, content injection, and cross-site scripting.

Impact:
The absence of these headers increases the attack surface and reduces the baseline security of the application.

Evidence:
Identified through **OWASP ZAP passive scan**, which detected missing headers in HTTP responses.

Recommendation:
Implement standard HTTP security headers including **Content-Security-Policy**, **X-Frame-Options**, and **X-Content-Type-Options**.

Finding 02: Insecure Cookie Attributes

Risk Level: Medium

Issue:
Cookies were observed without recommended security attributes such as **HttpOnly** and **Secure**.

Why it matters:
Without these attributes, cookies can be accessed by client-side scripts or transmitted over insecure connections, increasing the risk of session hijacking.

Impact:
An attacker may be able to steal or misuse user session information, which can lead to unauthorized access.

Evidence:
Identified through **OWASP ZAP passive scan**, which flagged cookies missing security attributes.

Recommendation:
Configure cookies with **HttpOnly**, **Secure**, and **SameSite** attributes to protect session data and reduce the risk of misuse.

Finding 03: Information Disclosure via HTTP Headers

Risk Level: Low

Issue:
The website exposes server and application information through HTTP response headers.

Why it matters:
Exposed information can help attackers understand the underlying technology and plan targeted attacks.

Impact:
While this issue does not directly compromise the system, it increases the risk of reconnaissance and targeted exploitation.

Evidence:
Identified through **OWASP ZAP passive scan**, which detected informative headers in server responses.

Recommendation:
Remove or limit unnecessary server and application details from HTTP response headers to reduce information exposure.

CONCLUSION

This vulnerability assessment identified several common security weaknesses in the assessed website, including missing security headers, insecure cookie attributes, and information disclosure through HTTP headers. While no critical vulnerabilities were observed, the identified issues may increase the risk of client-side attacks if left unaddressed.

All findings were identified using passive and ethical assessment techniques on publicly accessible components of the website. Implementing the recommended remediation measures will help improve the website’s overall security posture and reduce potential attack surfaces. Regular security reviews and adherence to security best practices are advised to maintain a secure web environment.