VULNERABILITY ASSESSMENT REPORT

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

Prepared By: Kusumba Radha Kishna

Date:20-01-2026

Assessment Type: Read- Only Vulnerability Assessment

1.Introduction

In today's digital environment, websites are exposed to various security risks due to misconfigurations, outdated software, and weak security controls. This vulnerability assessment was conducted to identify common security weaknesses in a publicly accessible website using ethical and non-intrusive methods.

The objective of this assessment is to help understand potential risks, explain them in a clear and business-friendly manner, and provide practical recommendations to improve the security posture of the application.

2. Scope of Assessment

The scope of this assessment was strictly limited to read-only and passive testing of publicly accessible resources.

Included in Scope:

- Public web pages
- HTTP/HTTPS headers
- Passive vulnerability scanning
- Basic network exposure analysis

Excluded from Scope:

- Login bypass attempts
- Exploitation of vulnerabilities
- Brute-force attacks
- Denial-of-Service (DoS)
- Any activity that could disrupt the service

This assessment was performed in an ethical manner following responsible security testing guidelines.

3. Tools Used

The following tools were used during the assessment:

- Ping – To verify reachability
- Nmap – To identify open ports and services
- Curl – To analyse HTTP response headers
- Web Browser (Firefox) – For manual exploration
- OWASP ZAP – For passive vulnerability scanning

4. Methodology

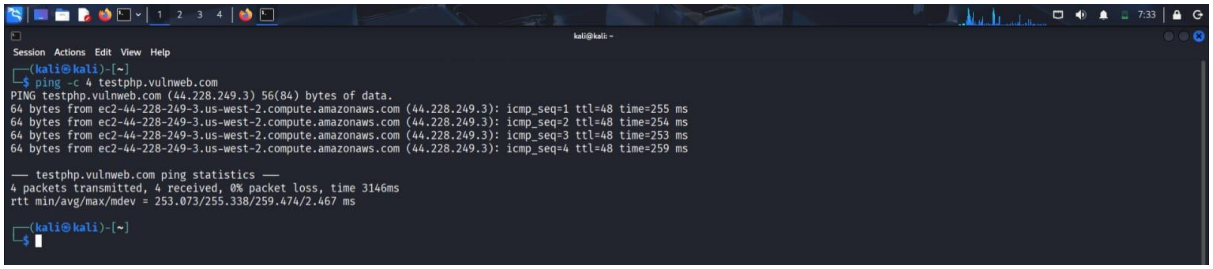
The assessment followed a structured approach:

1. Connectivity verification
2. Network and port analysis
3. HTTP header inspection
4. Manual application exploration
5. Passive vulnerability detection
6. Documentation of findings
7. Recommendation of remediation steps

5. Reconnaissance & Information Gathering

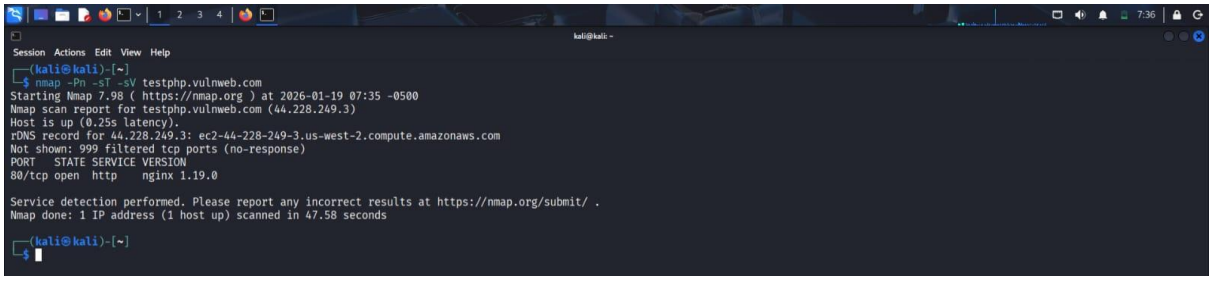
5.1 Ping Test

A ping test was conducted to confirm that the target website was reachable and responding to network requests.



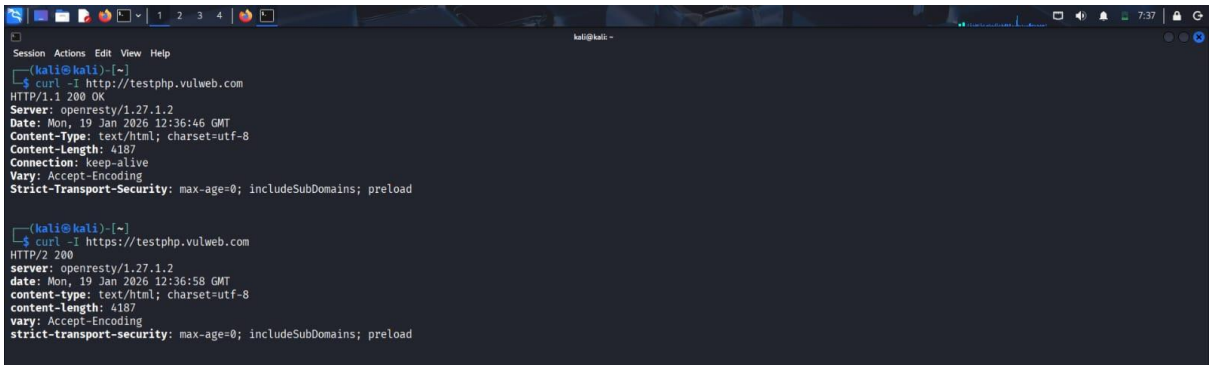
5.2 Port Scanning (Nmap)

An Nmap scan was performed to identify open ports and services running on the target server. The scan revealed that port 80 (HTTP) was open and accessible.



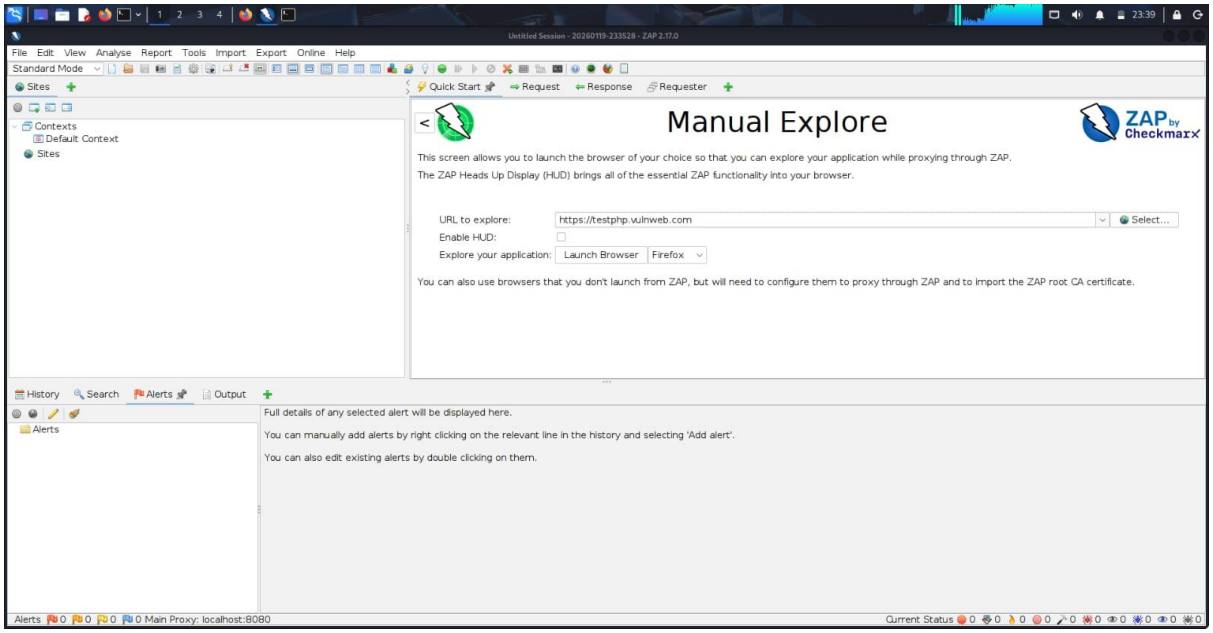
5.3 HTTP Header Analysis (Curl)

HTTP response headers were analyzed using the curl command. This helped identify server information and the presence or absence of security-related headers.



6. Manual Application Exploration

The web application was manually explored using a browser to understand its structure, navigation, and publicly accessible features. The site is a deliberately vulnerable demo application provided for testing purposes.



7. Identified Vulnerability

7.1 Content Security Policy (CSP) Header Not Set

Risk Level: Medium

Confidence: High

Affected URL: http://testphp.vulnweb.com

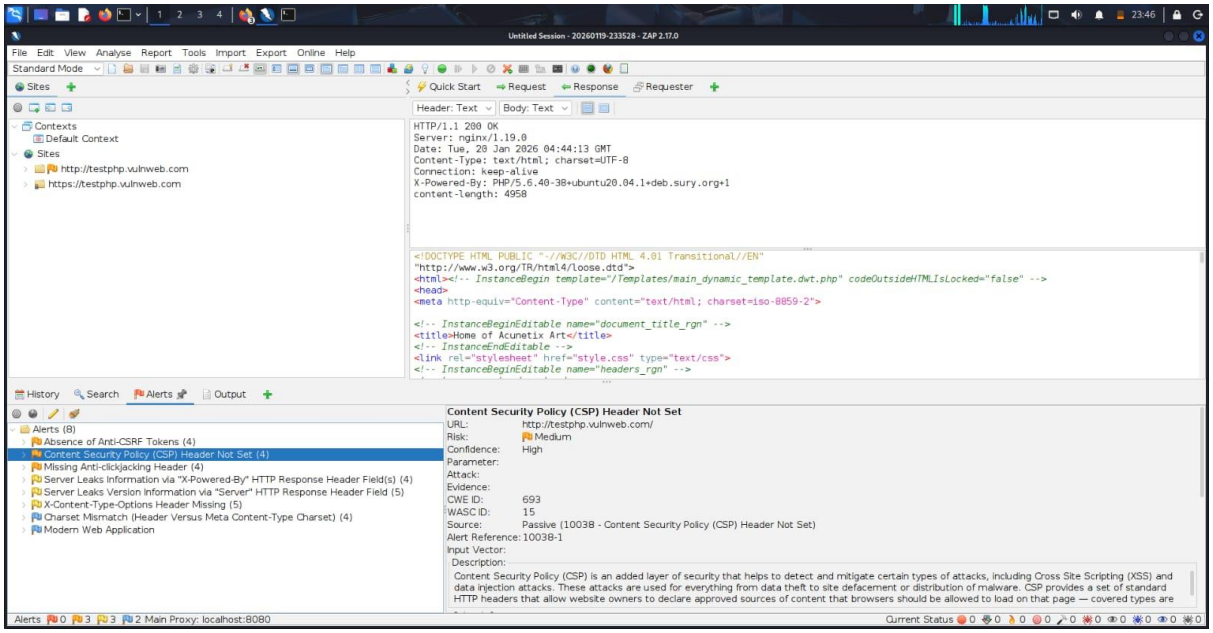
Description:
Content Security Policy (CSP) is an important security mechanism that helps prevent common web attacks such as Cross-Site Scripting (XSS) and data injection attacks. During the assessment, it was observed that the target application does not implement a CSP header in its HTTP responses.

Without a defined CSP, the browser does not restrict the sources from which content can be loaded, increasing the attack surface of the application.

Impact:
An attacker may exploit this weakness to inject malicious scripts into the application, potentially leading to:

- Data theft
- Session hijacking
- Website defacement
- Malicious content execution in the user's browser

Evidence:
The absence of the Content Security Policy header was identified using OWASP ZAP during passive scanning.



Recommendation:
It is strongly recommended to implement a **Content Security Policy (CSP)** header to restrict the sources from which content can be loaded by the browser. CSP acts as an additional layer of defense against client-side attacks such as Cross-Site Scripting (XSS) and data injection attacks.

A basic example of a CSP header is shown below:

```
Content-Security-Policy: default-src 'self';
```

This policy should be customized according to the application's functional requirements. Implementing a properly configured CSP will significantly reduce the risk of malicious script execution and improve overall browser-side security.

8. Risk Summary

Vulnerability	Risk Level
Content Security Policy Header Not Set	Medium

9. Conclusion

The vulnerability assessment conducted on the target application identified the absence of a Content Security Policy header, which presents a medium-level security risk. While no critical vulnerabilities were observed, implementing proper security headers such as CSP will greatly strengthen the application's resistance to common client-side attacks.

This assessment demonstrates the importance of secure configuration and regular security testing. It also reflects the ability to perform ethical, read-only security analysis and present findings in a structured and professional security report format.

10. Disclaimer

This assessment was conducted using non-intrusive, read-only techniques on a publicly available test website. No exploitation or destructive actions were performed. The findings are intended strictly for educational and learning purposes.