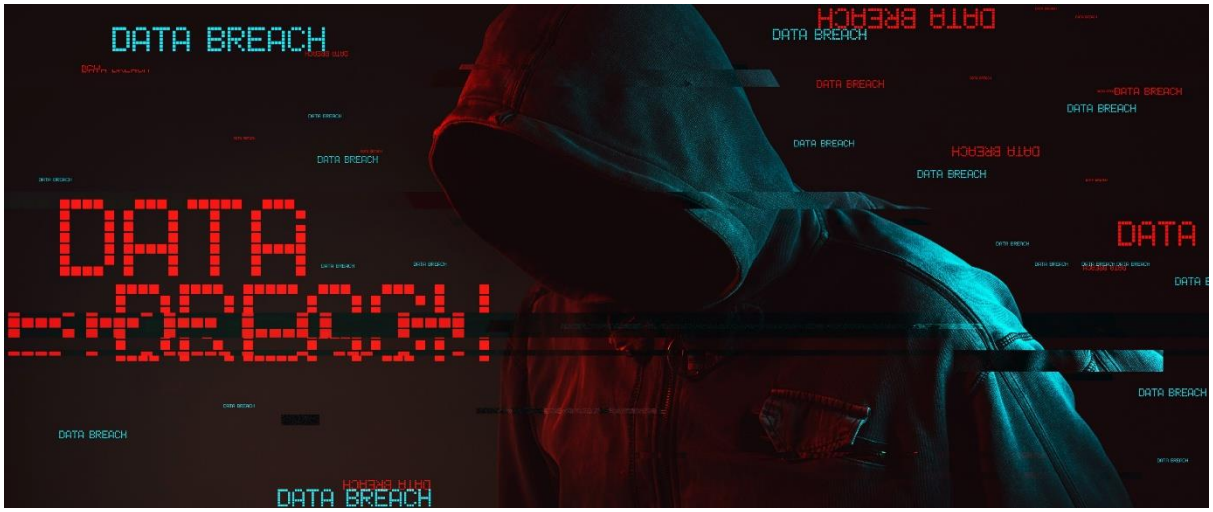
Vulnerability Assessment Report

Cyber Security Internship – **Task 1**

Organization: Future Interns



Prepared by: Harshit Shrivastav

Date: Feb 1st, 2026

Executive Summary

This report presents a vulnerability assessment conducted on a test website using passive scanning techniques.

The objective of this assessment is to identify common security vulnerabilities and recommend improvements to enhance the website’s security posture.

Scope & Methodology

Target Website: *testphp.vulnweb.com*

Testing Type: Passive Vulnerability

Assessment

Tools Used: Nmap, OWASP ZAP

Testing Approach: Observation and analysis only.

No active exploitation or attacks were performed.

Vulnerability Findings

Finding 1

Vulnerability Name:

Open HTTP Service with Version Disclosure

Risk Level: Low

Description:

An open HTTP service was detected running on port 80. The service is using nginx version 1.19.0, which reveals version information to potential attackers. This information disclosure may assist attackers in targeting known vulnerabilities.

Technical Details:

- Open Port: 80/tcp

- State: Open

- Service Name: HTTP

- Version: nginx 1.19.0

Recommendation:

Disable unnecessary service banners and hide server version information to reduce information disclosure.

Finding 2

Vulnerability Name:

Missing Security Headers

Risk Level: Medium

Description:

Important security headers are not implemented, which may expose the application to attacks such as clickjacking and content injection.

Recommendation:

Implement security headers such as X-Frame-Options, Content-Security-Policy, and X Content - Type-Options.

Finding 3

Vulnerability Name:

Cookie Without Secure Flag

Risk Level: Low

Description:

Cookies are transmitted without secure attributes, increasing the risk of interception over unsecured connections.

Recommendation:

Enable Secure and Http Only flags for all sensitive cookies to improve session security.

Conclusion

The assessment highlights the importance of basic security configurations.

Addressing these vulnerabilities will improve the overall security of the application.

Disclaimer

This report is created strictly for educational purposes as part of a Cyber Security internship.

No unauthorized access or exploitation was performed.

Supporting Evidence

Screenshot 1:

Nmap – Basic Scan

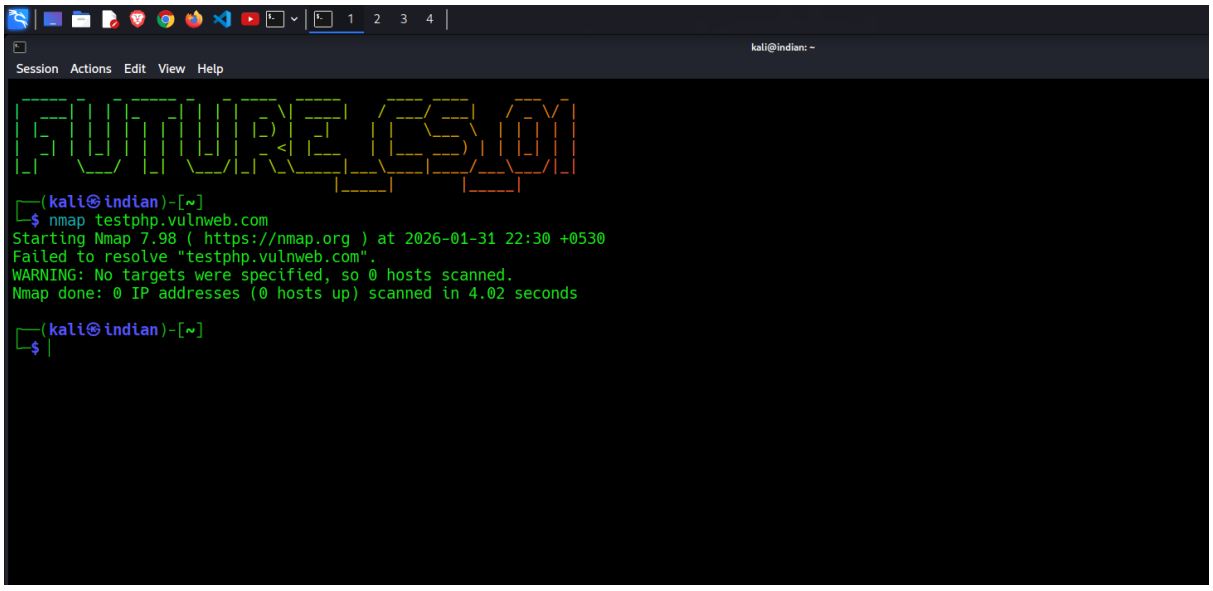


Figure 1: *Nmap basic scan showing open ports on the target website.*

Screenshot 2:

Nmap– Service Version Scan

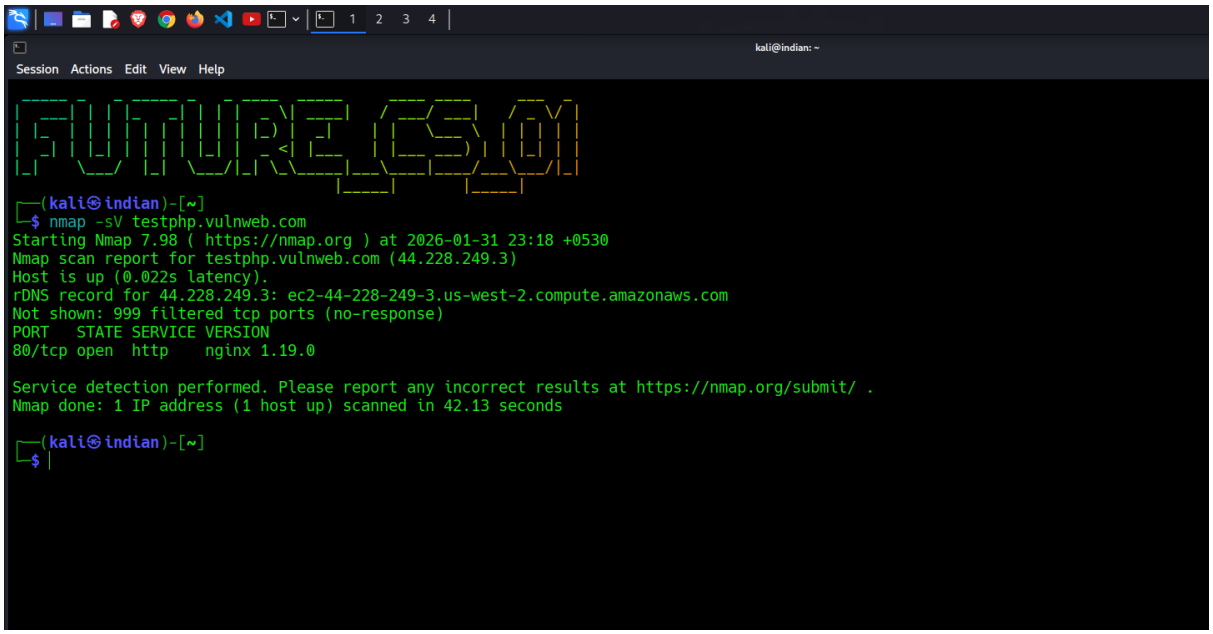


Figure 2: *Nmap service version scan displaying detected services and versions.*

Screenshot 3:

OWASP ZAP – Alerts Overview

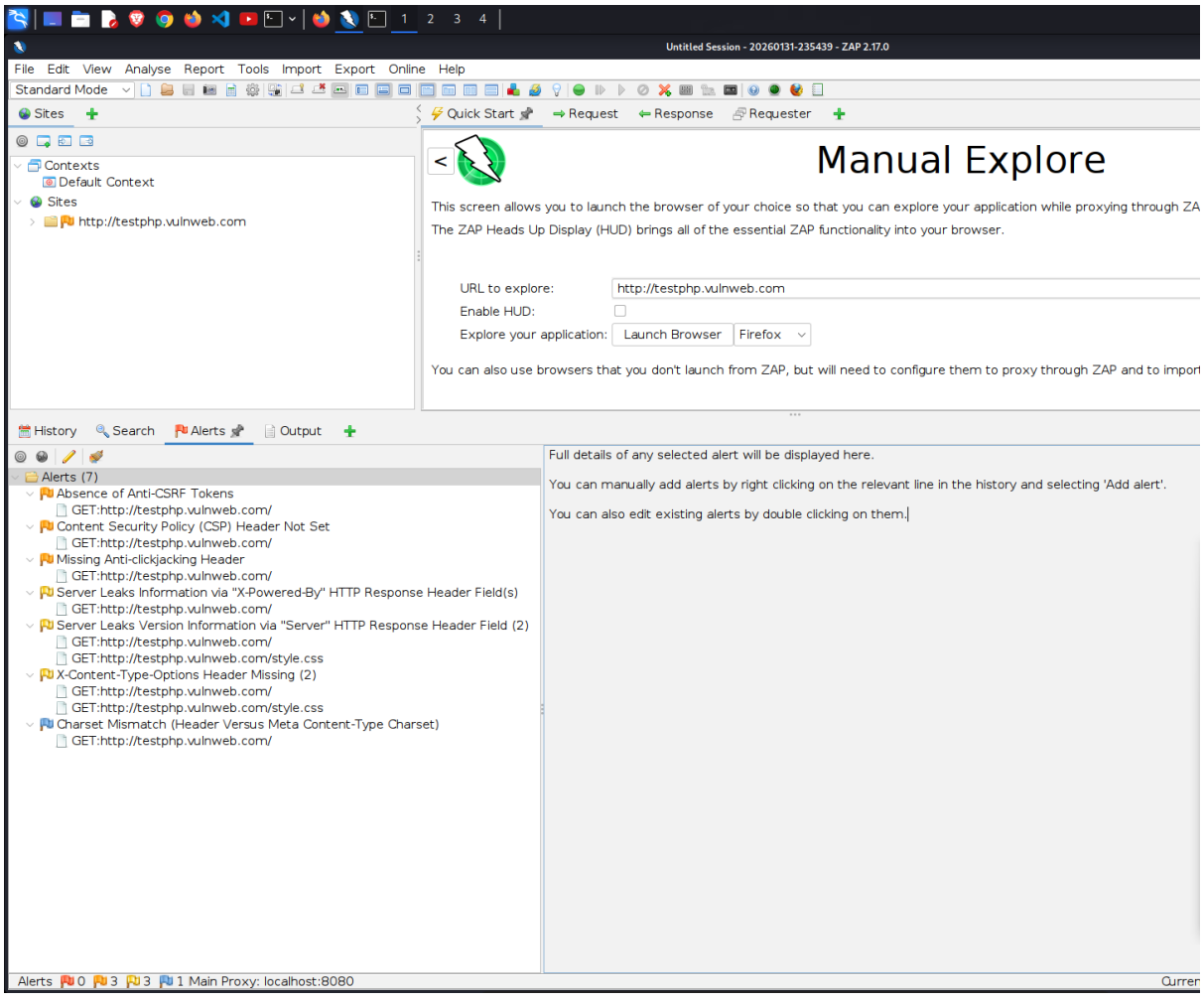


Figure 3: *OWASP ZAP passive scan alerts highlighting identified security issues.*

Screenshot 4:

OWASP ZAP – Vulnerability Details

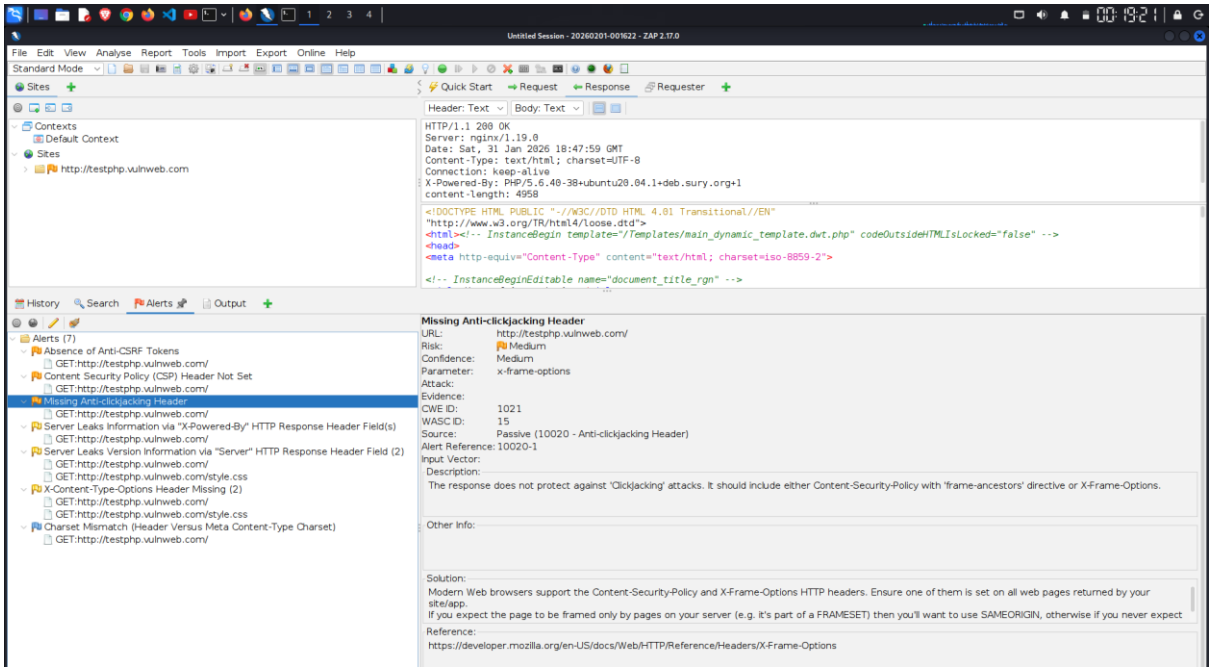


Figure 4: *Detailed view of a vulnerability detected during OWASP ZAP analysis.*

Author Details

Name: Harshit Shrivastav

Role: Cyber Security Intern

LinkedIn: *https://www.linkedin.com/in/harshit-shrivastav-14790338b*

GitHub: *https://github.com/harshshrii-2000*

Skills Used:

- Nmap
- OWASP ZAP
- Vulnerability Assessment
- Report Writing