Vulnerability Assessment Report

- Future Interns – Cyber Security Task 1
- Read-Only Website Security Review
- Prepared by: Jeremiah Olatubosun
- Tools: Nmap | OWASP ZAP | Browser DevTools

Executive Summary

- A passive vulnerability assessment was conducted on a public website.
- No exploitation or harmful testing was performed.
- Several configuration weaknesses and exposed services were identified.
- Findings include missing security headers and publicly accessible services.

Scope & Ethics

- Allowed: Passive scanning, public pages, header checks, configuration review
- Not Allowed: Exploitation, brute force, login bypass, DoS
- Assessment performed strictly within read-only boundaries

Methodology

- 1. Nmap – Discover open ports and services
- 2. OWASP ZAP – Passive vulnerability scan
- 3. Browser DevTools – Manual header inspection
- 4. Findings documented and risk classified

Tools Used

- · Nmap – Port & service exposure analysis
- · OWASP ZAP – Passive vulnerability detection
- · Browser DevTools – HTTP header inspection
- · Canva – Professional report design

Service Exposure Findings (Nmap)

- • Port 80 – HTTP service publicly accessible
- • Port 587 – SMTP mail submission service publicly accessible
- • Multiple exposed services increase attack surface

- Risk Level: Low
- Recommendation: Restrict unnecessary ports and apply firewall rules

Medium Risk Findings (OWASP ZAP)

- · Absence of Anti-CSRF Tokens
- · Content Security Policy (CSP) header not set
- · Missing Anti-Clickjacking protection (X-Frame-Options)
- Impact: Higher likelihood of session hijacking or clickjacking attacks

Low Risk Findings (OWASP ZAP)

- · X-Powered-By header exposes technology stack
- · Server version disclosure via Server header
- · Missing X-Content-Type-Options header

- Impact: Information disclosure useful for reconnaissance

Browser DevTools Header Analysis

- Observed headers:
- · Server: nginx/1.19.0
- · X-Powered-By: PHP/5.6.40

- Missing security headers:
- · Content-Security-Policy
- · X-Frame-Options
- · X-Content-Type-Options

- Risk Level: Medium–Low

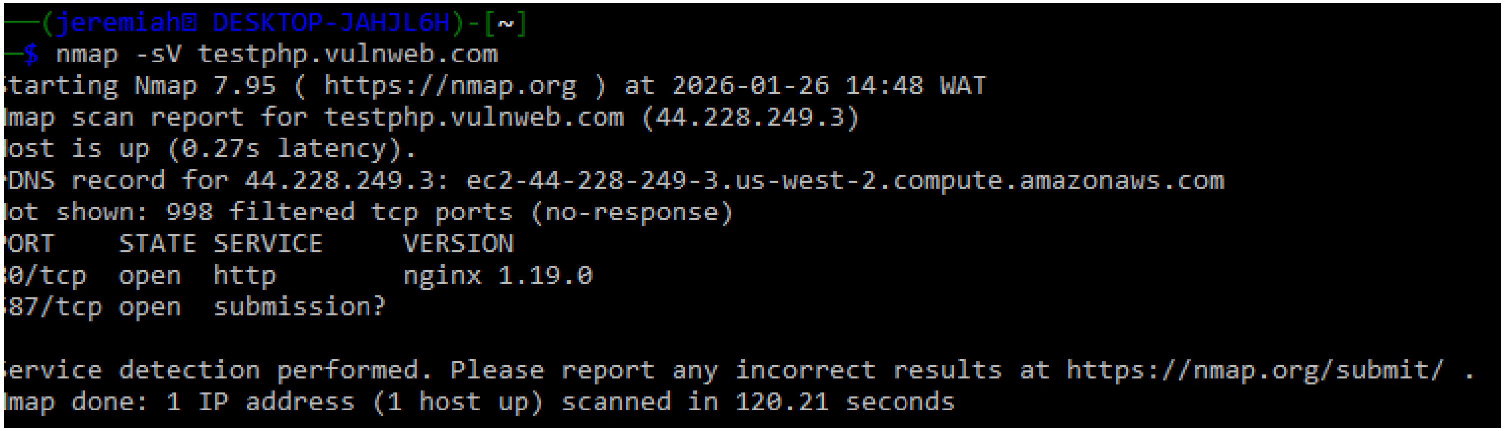
Risk Summary

- Medium Risks: 3
- Low Risks: 3+
- Informational/Exposure: Open services (80, 587)

- Overall Risk: Moderate
- Security hardening recommended

Evidence Collected

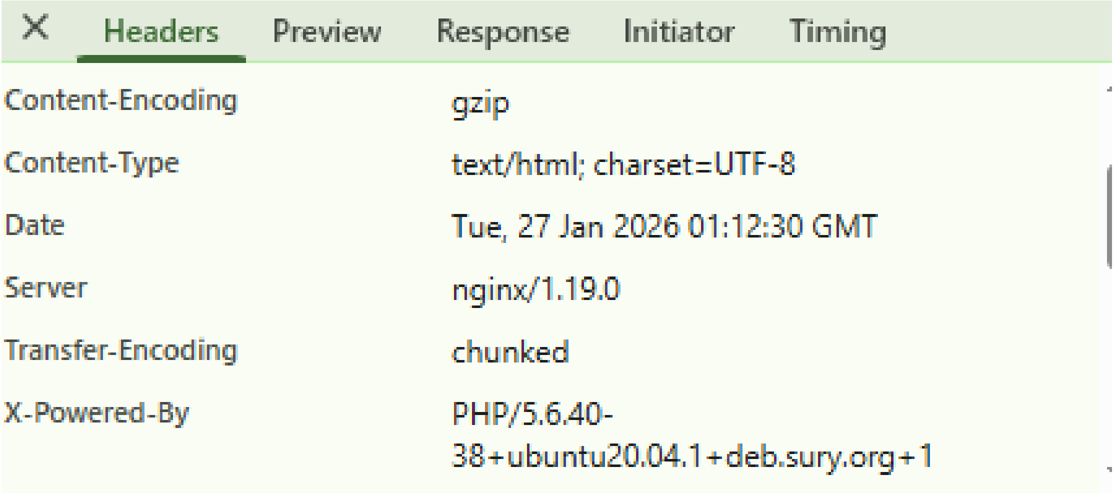
- · zap_report.html (full scan report)
- · nmap_scan(port scan output screenshot)



```
──(jeremiah⊠ DESKTOP-JAHJL6H)-[~]
─$ nmap -sV testphp.vulnweb.com
tarting Nmap 7.95 ( https://nmap.org ) at 2026-01-26 14:48 WAT
map scan report for testphp.vulnweb.com (44.228.249.3)
ost is up (0.27s latency).
DNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
ot shown: 998 filtered tcp ports (no-response)
ORT     STATE SERVICE     VERSION
0/tcp   open  http        nginx 1.19.0
87/tcp  open  submission?

ervice detection performed. Please report any incorrect results at https://nmap.org/submit/ .
map done: 1 IP address (1 host up) scanned in 120.21 seconds
```

- · browser_headers.png (DevTools screenshot



Content-Encoding	gzip
Content-Type	text/html; charset=UTF-8
Date	Tue, 27 Jan 2026 01:12:30 GMT
Server	nginx/1.19.0
Transfer-Encoding	chunked
X-Powered-By	PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

All evidence stored in GitHub repository

Remediation Recommendations

- • Implement Content Security Policy (CSP)
- • Add CSRF protection to forms
- • Enable X-Frame-Options and X-Content-Type-Options
- • Remove or hide server/version headers
- • Restrict unnecessary open ports using firewall rules

Conclusion

- The website is functional but lacks basic security hardening.
- Addressing identified issues will reduce attack surface and improve resilience.
- Passive testing confirms several quick-fix improvements are possible.