WEB APPLICATION Vulnerabiltiy Assessment Report

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

Assessment Type:
Legal and public Web Security Testing

Tools Used:

Nmap,OWASP ZAP ,Browser Developrer Tools

Prepared by:
LakshmiCharanya

Internship Task:
Task 1 – Vulnerability Assessment

OBJECTIVE AND SCOPE

Objective

The objective of this assessment is to identify common web security
misconfigurations using ethical, legal, and non-intrusive testing methods and to provide appropriate remediation recommendations.

Scope

- The assessment was limited to a publicly accessible demo website.
- Only passive and non-intrusive testing techniques were used.
- No authentication, login, or private areas were tested.
- No exploitation or data modification was performed.

METHODOLOGY

Methodology Used

- Network scanning using Nmap
- Automated vulnerability scanning using OWASP ZAP
- Manual HTTP header verification using Browser Developer Tools

NMAP SCAN RESULT

Tool Used: Nmap

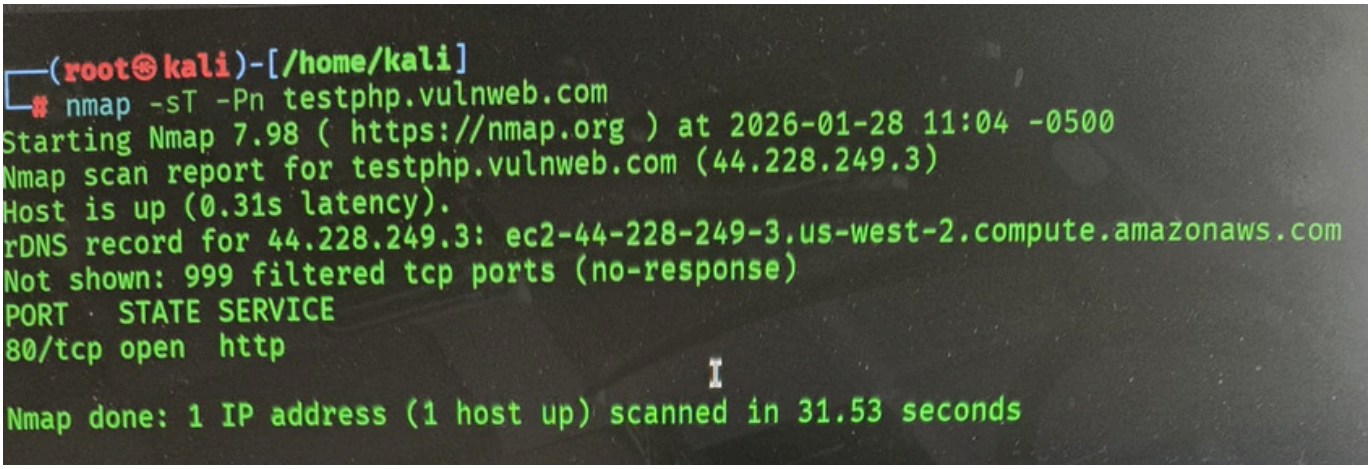
Command Executed:

nmap -sT -Pn testphp.vulnweb.com

Result:

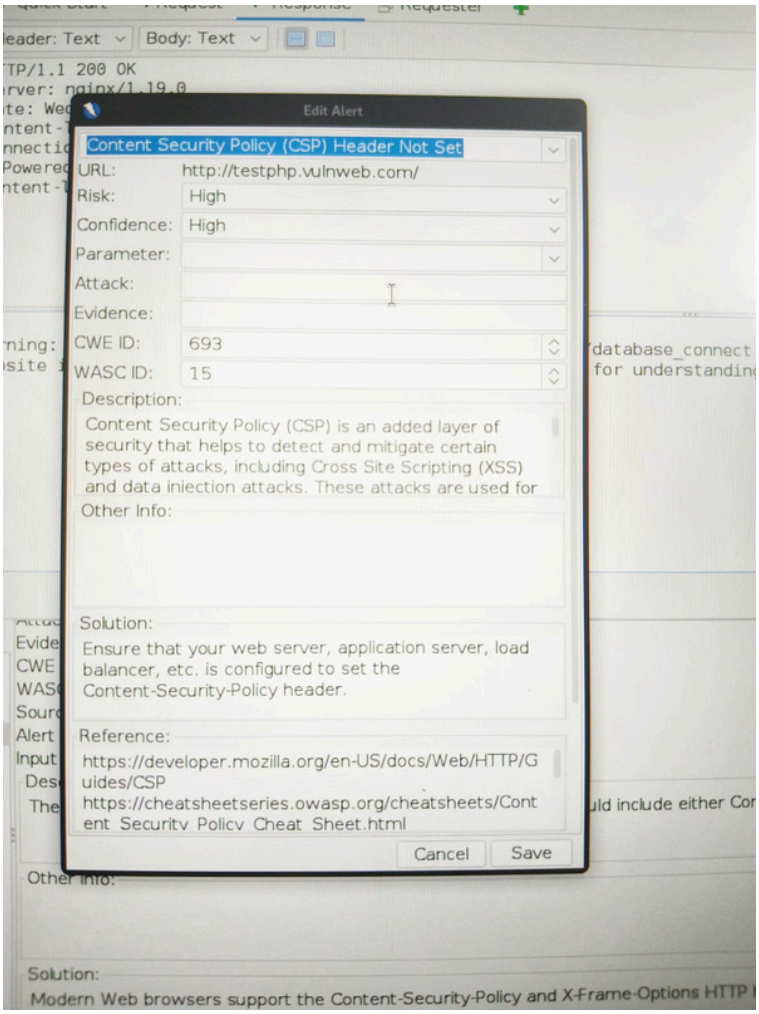
- Host is active
- Port 80/tcp (HTTP) is open
- The scan was limited to basic connectivity and port discovery only.

- **Impact:**
- The web application is publicly accessible and should be secured against web-based attacks.



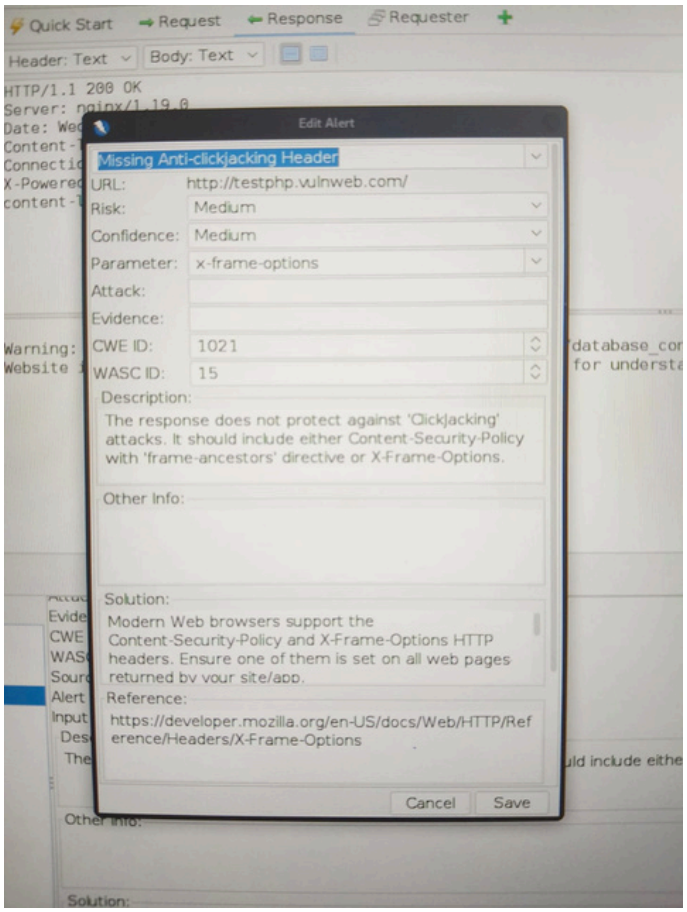
HIGH RISK VULNERABILTY

Vulnerability:
Content Security Policy (CSP) Header Not Set
Risk: High
Confidence: High
CWE ID: 693
Description
The application does not implement a Content Security Policy (CSP) header, which increases the risk of Cross-Site Scripting (XSS) and data injection attacks.
Recommendation
Configure the web server to include a strict Content-Security-Policy header.



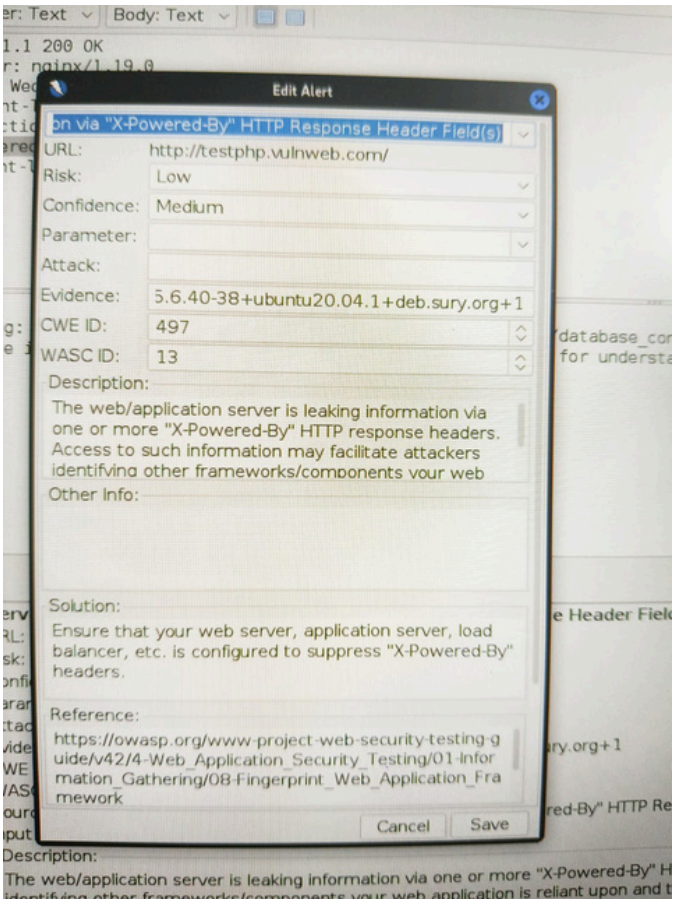
MEDIUM RISK VULNERABILITY

Vulnerability:
Missing Anti-Clickjacking Header
Risk: Medium
Confidence: Medium
Parameter: X-Frame-Options
CWE ID: 1021
Description
The application does not protect against clickjacking attacks
Impact
This may affect user trust and application integrity.
Recommendation
Implement X-Frame-Options or frame-ancestors directive.



LOW RISK VULNERABILITY

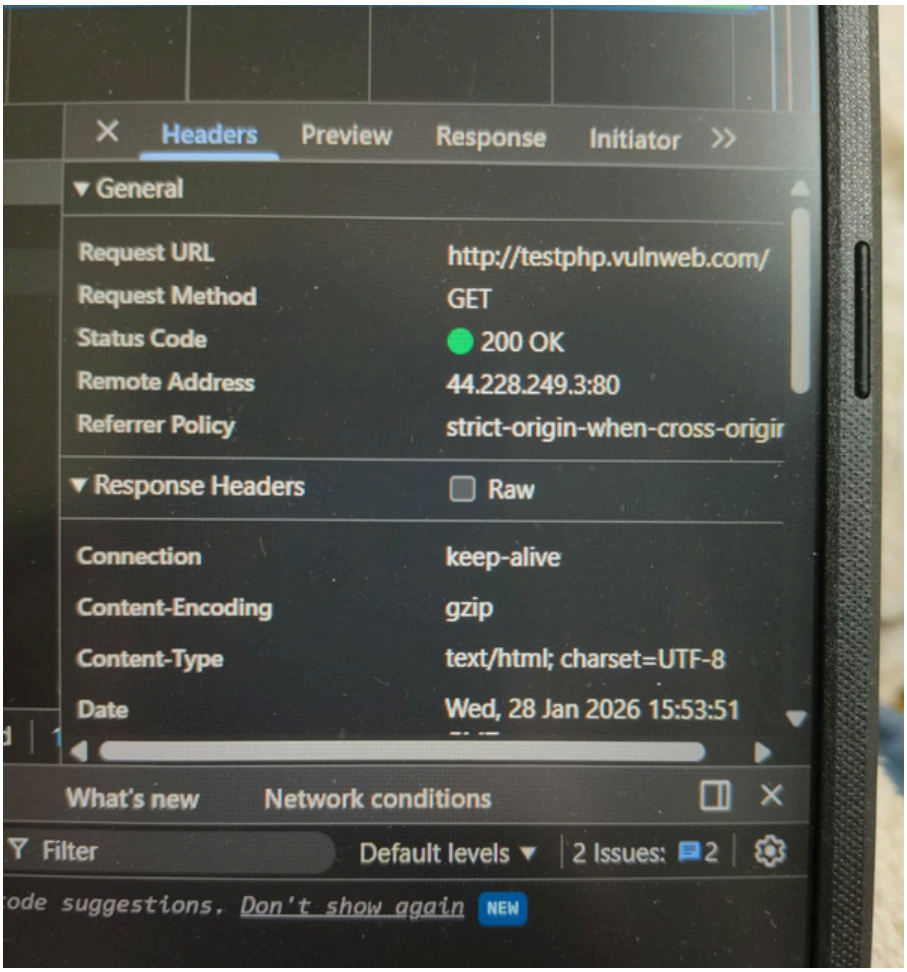
Vulnerability:
X-Powered-By Header Information Disclosure
Risk: Low
Confidence: Medium
CWE ID: 497
Description
The server reveals backend technology information through HTTP headers.
Recommendation
Suppress the X-Powered-By header at the server level.



BROWSER DEV TOOLS VERIFICATION

Description

Browser Developer Tools were used to manually verify the absence of security headers.



CONCLUSION

The security assessment identified multiple vulnerabilities related to missing HTTP security headers and information disclosure. Although no exploitation was performed, these issues may increase the attack surface of the application.

All findings were identified using passive and non-intrusive testing techniques on a publicly accessible demo website.

REFERENCES

https://developer mozilla.org
https://owasp.org
https://cheatsheetseries.owasp.org