



WEB APPLICATION

Vulnerability Assessment Report

Web Application Security Assessment

Prepared by:

NAGULAPALLI SRIVIDYA NARASIMHA

Cybersecurity Task 1

INTRODUCTION

Web applications are frequently targeted by attackers due to misconfigurations and security vulnerabilities. This report documents the security assessment performed on a public demo web application using automated and manual testing tools.

The objective of this assessment is to identify potential security weakness and recommend improvements.

Objective

- To identify common web security vulnerabilities
- To analyze security misconfigurations using passive techniques
- To understand real-world web application security risks
- To document findings in a professional security report

Tools Used

Security Tools & Environment:

- Kali Linux (Testing environment)
- Nmap (Port and service identification)
- OWASP ZAP (Automated Web Application Vulnerability scanning)
- Browser Developer Tools (Header & cookie inspection)

Nmap Scan Results

Command Used: nmap -sT testphp.vulnweb.com

Nmap Scan Summary:

- TCP port scan performed using safe scan techniques
- Open ports identified:
 - Port 80 (HTTP)
 - Port 443 (HTTPS)
- Web services found running on the target system

Nmap Scan Results

```
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
# nmap -ST testphp.vulnweb.com
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-30 22:42 -0500
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.035s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 7.65 seconds

(root㉿kali)-[/home/kali]
```

MEDIUM RISK VULNERABILITY

Vulnerability Name: Content Security Policy (CSP) Header Not Set

- Risk Level: Medium
- CWE ID: 693

Description: The website does not implement a Content Security Policy header, increasing the risk of client-side attacks such as Cross-Site Scripting (XSS).

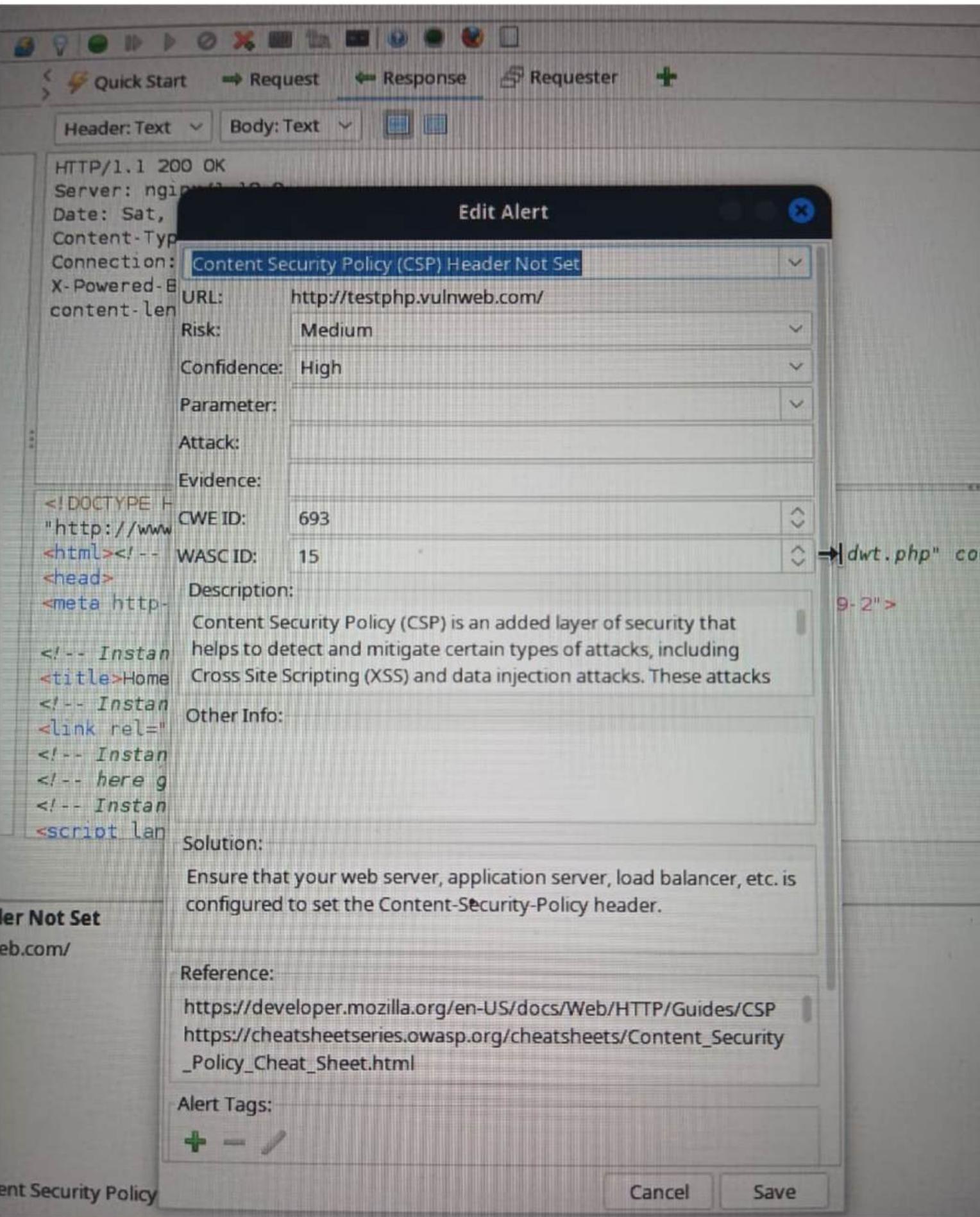
Impact:

- Malicious scripts can be injected
- Reduced browser protection

Solution:

- Implement a strong Content-Security-Policy header on the server.

MEDIUM RISK VULNERABILITY



MEDIUM RISK VULNERABILITY

Vulnerability Name: Absence of Anti-CSRF Tokens

- Risk Level: Medium
- CWE ID: 352

Description: HTML forms do not contain Anti-CSRF tokens, making the application vulnerable to Cross-Site Request Forgery attacks.

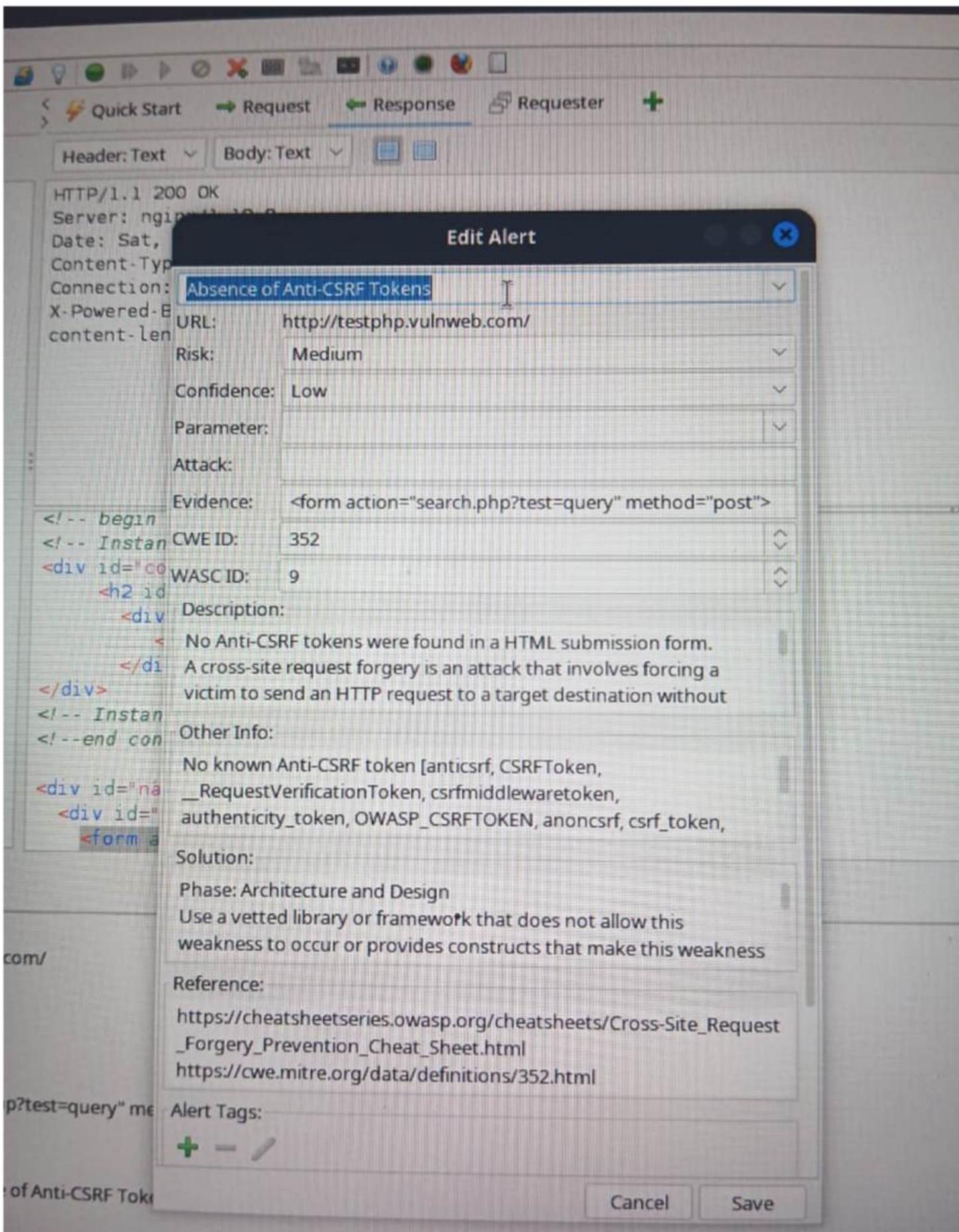
Impact:

- Unauthorized actions may be performed.
- User sessions can be misused.

Solution:

- Implement Anti-CSRF tokens in all sensitive forms.

MEDIUM RISK VULNERABILITY



LOW RISK VULNERABILITY

Vulnerability Name: Information Disclosure via X-Powered-By Header

- Risk Level: Low
- CWE ID: 497

Description: The server exposes backend technology details through HTTP response headers.

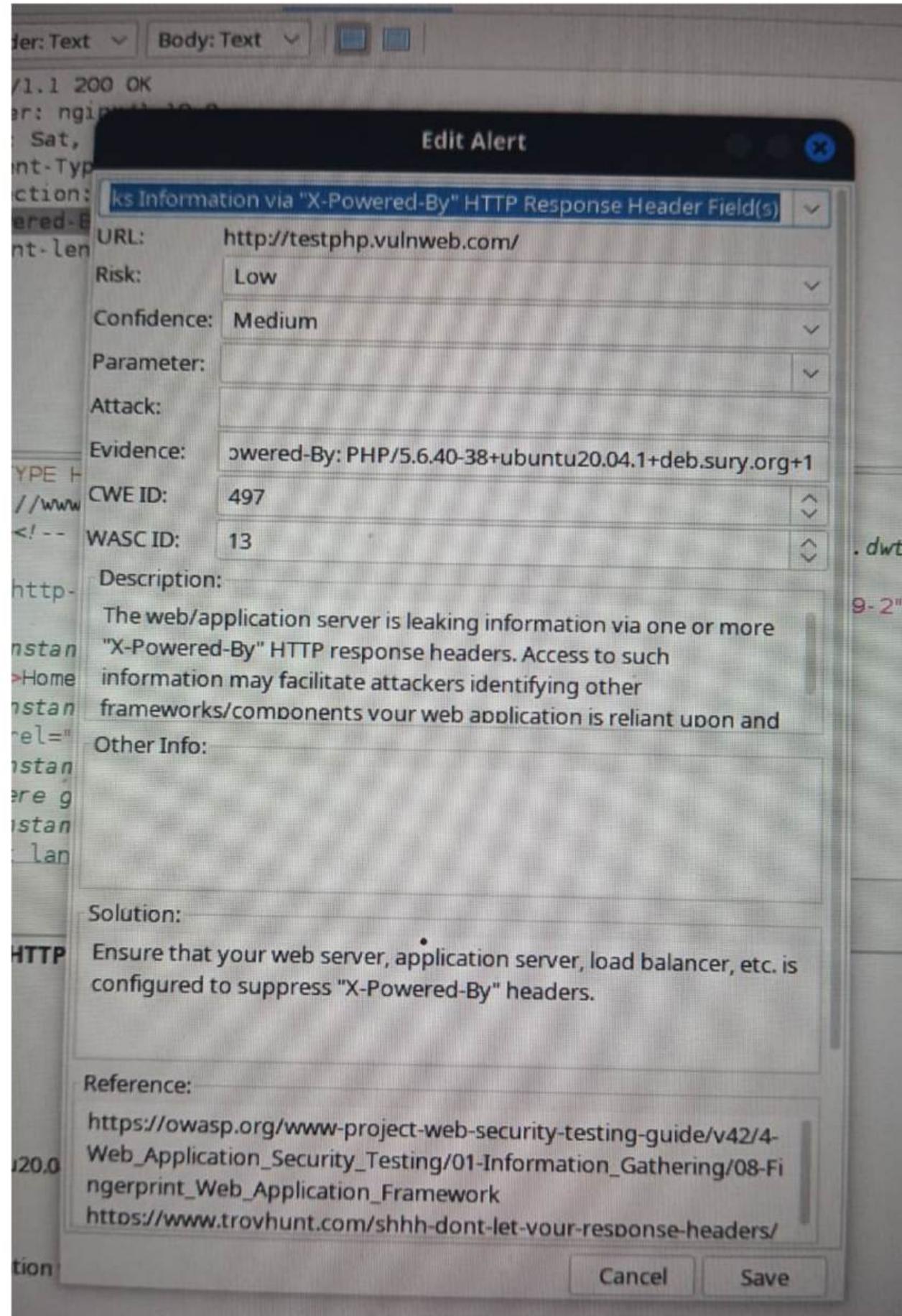
Impact:

- Attackers can identify server technologies
- Easier exploitation of known vulnerabilities

Solution:

- Disable or remove the X-Powered-By header from server configuration.

LOW RISK VULNERABILITY



INFORMATION FINDINGS

Timestamp Disclosure - Unix

Timestamp values were observed in server responses. This may expose timing information but does not directly impact security.

Cache-Control Header Review

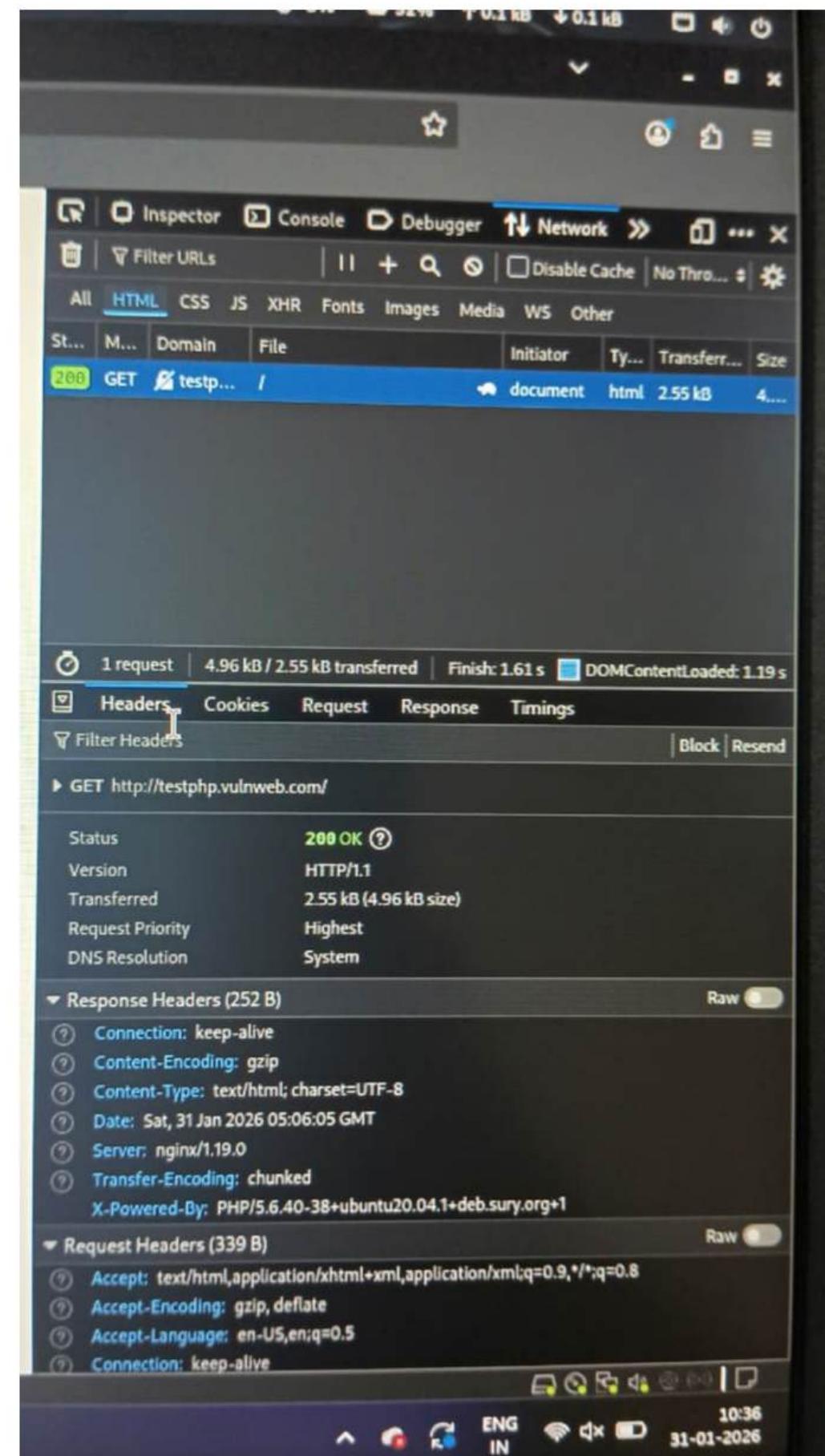
Cache-control directives were observed and require review to ensure sensitive content is not cached.

INFORMATION FINDINGS

BROWSER DEVELOPER TOOLS VERIFICATION

Browser developer tools were used to manually verify HTTP response headers and confirm missing security protections identified by OWASP ZAP.

BROWSER DEVELOPER TOOLS VERIFICATION



CONCLUSION

The assessment identified medium and low-risk security misconfigurations related to missing HTTP security headers. No high-risk vulnerabilities were observed. Implementing recommended security headers will enhance the overall security posture of the application.

DISCLAIMER

This vulnerability assessment report was prepared by solely for educational and internship evaluation purposes . The security testing was conducted on a publicly accessible demo website using passive and non-intrusive techniques.

No exploitation, unauthorized access, data modification, or denial-of-service activites were performed during the assessment. The findings documented in this report are based on the tools and methods used at the time of testing and may not represent all possible security vulnerabilities. The author shall not be held responsible for any misuse of information contained in this report. This report is intended strictly for academic learning and skill demonstration and must not be used for malicious activites.

REFERENCES

- [1] OWASP Foundation, OWASP Top 10 - Security Misconfiguration (A05:2021), 2021.
Available: https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
- [2] OWASP Foundation, OWASP Top 10 - Sensitive Data Exposure (A03:2017), 2017.
Available: https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html
- [3] OWASP ZAP Project, Timestamp Disclosure - Alert Documentation, OWASP.
Available: <https://www.zaproxy.org/docs/alerts/10096/>
- [4] OWASP ZAP Project, Missing Anti-clickjacking Header, OWASP.
Available: <https://www.zaproxy.org/docs/alerts/10020/>
- [5] OWASP ZAP Project, Content Security Policy (CSP) Header Not Set, OWASAP
- [6] OWASP ZAP Project, X-Content-Type-Options Header Missing, OWASP.
Available: <https://www.zaproxy.org/docs/alerts/10021/>
- [7] OWASP ZAP Project, Re-examine Cache-Control Directives, OWASP.
Available: <https://www.zaproxy.org/docs/alerts/10015/>
- [8] MITRE Corporation, CWE-1021: Improper Restriction of Rendered UI Layers or Frames.
Available: <https://cwe.mitre.org/data/definitions/1021.html>
- [9] MITRE Corporation, CWE-693: Protection Mechanism Failure.
Available: <https://cwe.mitre.org/data/definitions/693.html>
- [10] Mozilla Developer Network (MDN), HTTP Header - X-Frame-Options.
Available: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>
- [11] Mozilla Developer Network (MDN), Content Security Policy (CSP).
Available: <https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>
- [12] Mozilla Developer Network (MDN), Cache-Control HTTP Header.
Available: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control>
- [13] Nmap Project, Nmap Service and Version Detection.
Available: <https://nmap.org/book/man-version-detection.html>