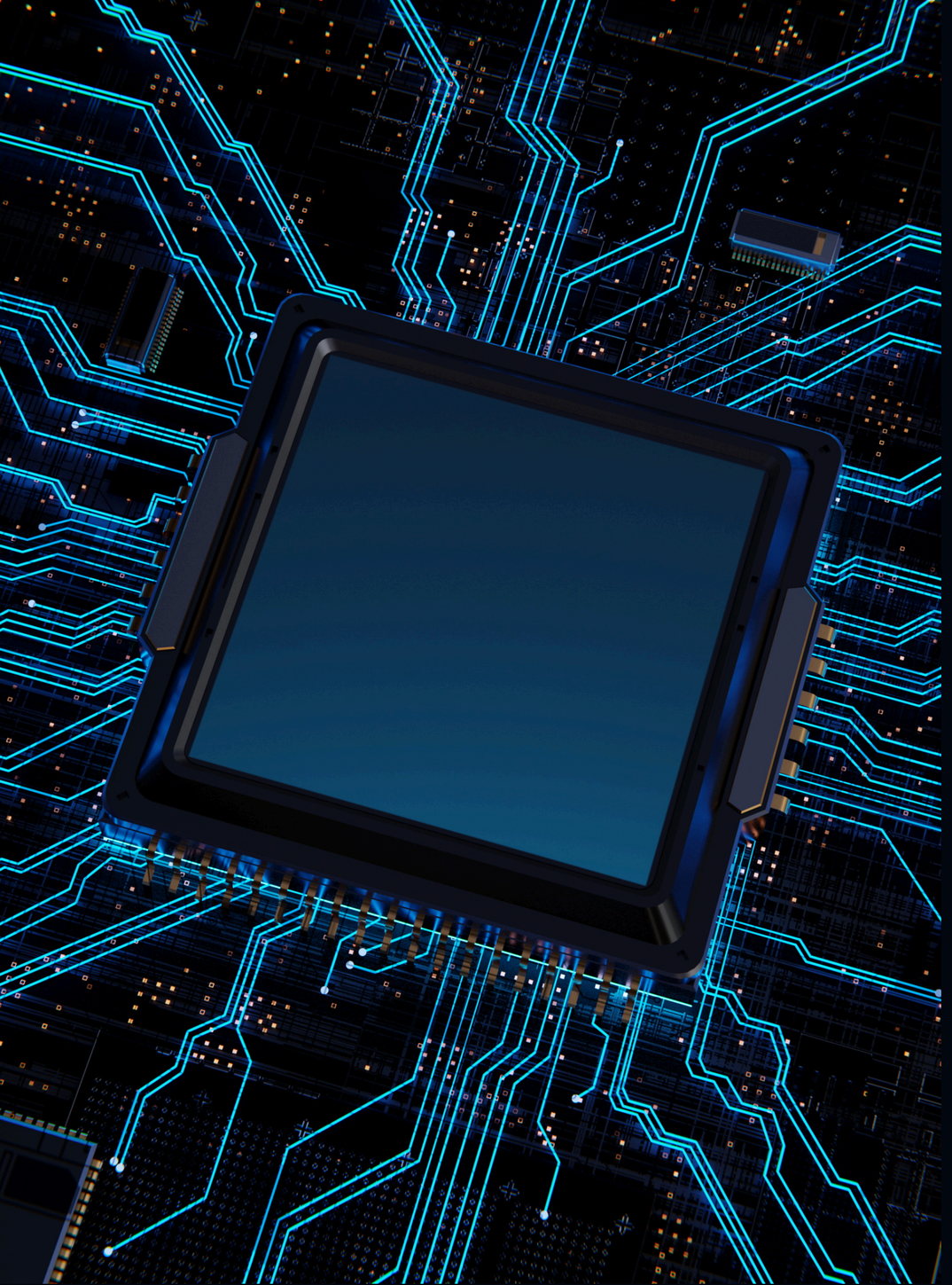
VULNERABILITY ASSESSMENT REPORT

CYBER SECURITY TASK 1 – 2026

FUTURE INTERNS



Website Tested

http://testphp.vulnweb.com

Scope of Assessment

This vulnerability assessment was conducted on a publicly accessible website.

Only passive and read-only techniques were used during the assessment.

No exploitation, authentication bypass, or intrusive testing was performed.

Objective

The objective of this assessment is to identify common security weaknesses, classify associated risks, and provide clear and practical remediation recommendations in a business-friendly manner.

Tools Used

Browser Developer Tools (edge)

SecurityHeaders.com

Identified Vulnerability 1

HTTP Instead of HTTPS

Risk Level: High

Description:

The website is accessible over HTTP, which means data transmitted between the user and the server is not encrypted.

Why This Matters:

Unencrypted communication can be intercepted or modified by attackers, potentially leading to data theft or session hijacking.

Recommendation:

Install a valid SSL/TLS certificate and enforce HTTPS to ensure secure communication between users and the website

Identified Vulnerability 2

Missing Security Headers

Risk Level: Medium

Missing Headers

Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Evidence: Security header analysis showing missing headers.

Description:

The website is missing important HTTP security headers such as Content-Security-Policy (CSP), X-Frame-Options, and Strict-Transport-Security (HSTS).

Why This Matters:

Missing security headers increase the risk of attacks such as clickjacking and cross-site scripting (XSS).

Recommendation:

Configure appropriate security headers on the web server to enhance protection against common web attacks.

Identified Vulnerability 3

Server Version Disclosure

Risk Level: Medium

Description:

The web server exposes its version information through HTTP response headers.

Observed Evidence:

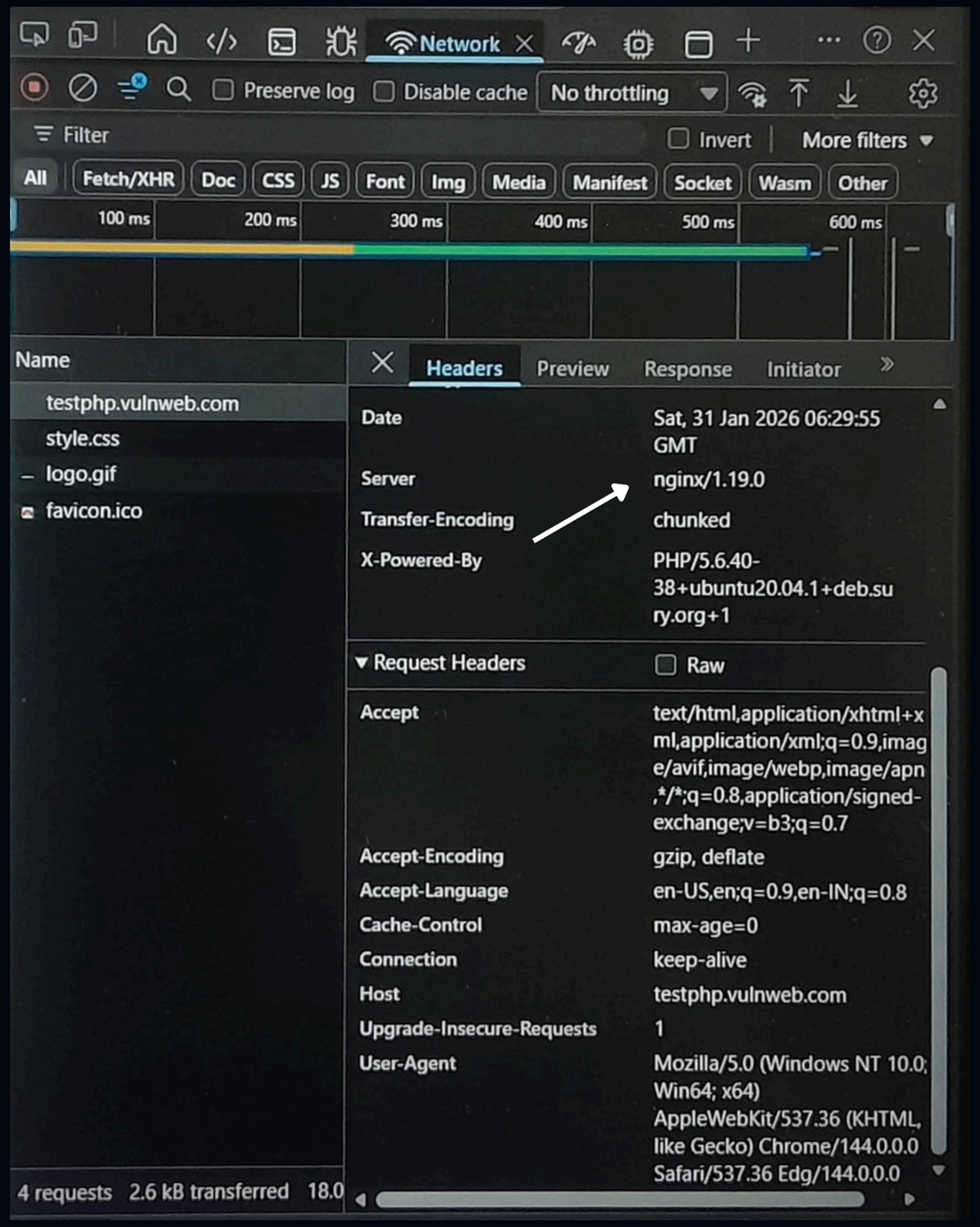
Server: nginx/1.19.0

Why This Matters:

Exposing server type and version helps attackers identify known vulnerabilities associated with that software.

Recommendation:

Configure the server to hide or obfuscate server version information in HTTP response headers.



Evidence: HTTP response headers observed using browser developer tools.

Identified Vulnerability 4

X-Powered-By Header Disclosure

Risk Level: Medium

Description:

The application exposes backend technology details through the X-Powered-By HTTP response header.

Observed Evidence:

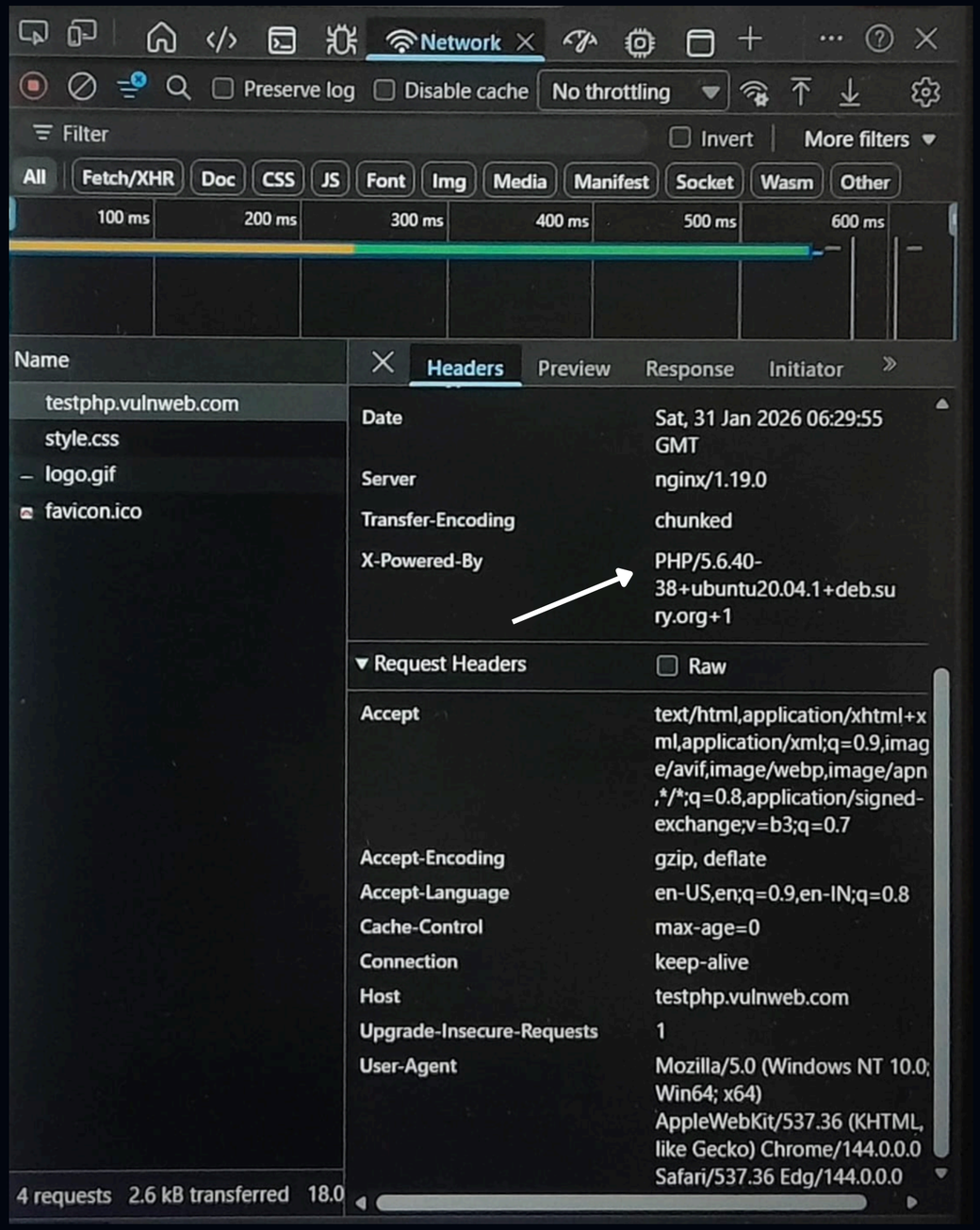
X-Powered-By: PHP/5.6.40

Why This Matters:

Revealing backend technologies and software versions can help attackers target known vulnerabilities.

Recommendation:

Disable the X-Powered-By header and ensure backend components are updated to supported and secure versions.



Evidence: HTTP response headers observed using browser developer tools.

Conclusion:

This vulnerability assessment identified multiple security weaknesses, including the absence of HTTPS, missing security headers, and unnecessary information disclosure through HTTP response headers.

Addressing these issues will significantly improve the website's security posture and reduce exposure to common web-based attacks.