VULNERABILITY ASSESSMENT REPORT

CYBER SECURITY TASK-1 : 2026

FUTURE INTERNS

Website Tested

http://testaspnet.vulnweb.com

Scope of Assessment

The testing focused only on analysing the target website using safe and read only methods. No harmful or intrusive attacks were performed during the assessment.

Objective

The aim of this assessment is to identify vulnerabilities, understand their impact, and suggest ways to enhance website's security.

Tools used

Security Hearder.com
Browser Developers Tool

RISK:HIGH

Description

The website is accessible over HTTP, the communication between the user's browser and the web server is not encrypted. This means that sensitive information such personal data is transmitted in plain text and can be intercepted by attackers.

Why it matters

Without the use of HTTPS it can lead to Data sniffing, Session hijacking,Data tampering, and Loss of user trust.

Recommended Fixes

Enable HTTPS using SSL/TLS certificate
Redirect all HTTP traffic to HTTPS
Enable HSTS (HTTP Strict Transport Security)

Identified Vulnerability:1

HTTP instead of HTTPS

Identified Vulnerability:2

Server Version Disclosure

RISK:MEDIUM

Description

The application reveals server and framework version information through HTTP response headers, including Microsoft-IIS/8.5 and ASP.NET version details.

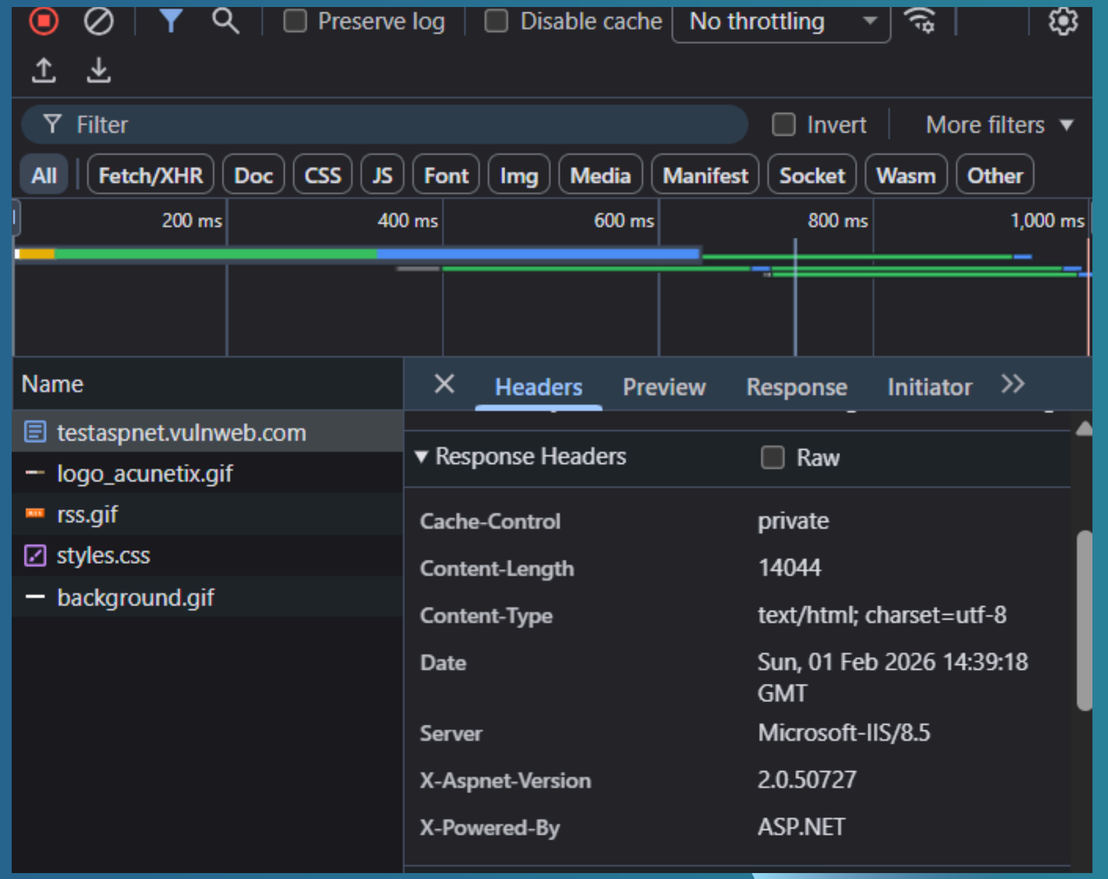
Evidence:Microsoft-IIS/8.8

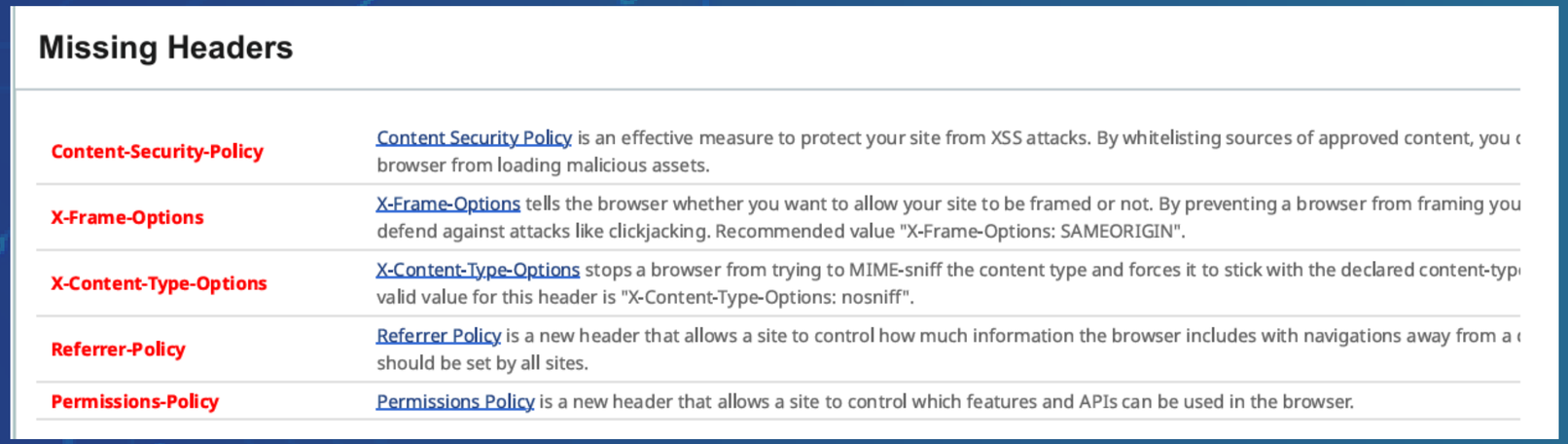
Why it Matters

Exposing version information helps attackers:Identify server technology, Search known vulnerabilities (CVEs), Use ready-made exploits, Perform targeted attacks.

Recommended Fixes

Remove or suppress server version headers and ensure the server software is regularly updated.





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 c 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 you 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-typ 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 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.

Identified Vulnerability:3

Missing Security Headers

RISK:MEDIUM

Description

The application reveals server and framework version information through HTTP response headers, including Microsoft-IIS/8.5 and ASP.NET version details.

Why it matters

Attackers can identify the underlying technology and exploit known vulnerabilities specific to these versions.

Recommended fixes

Remove or suppress server version headers and ensure the server software is regularly updated.

Identified Vulnerability:4

X-Powered-By header disclosure

RISK:LOW

Description

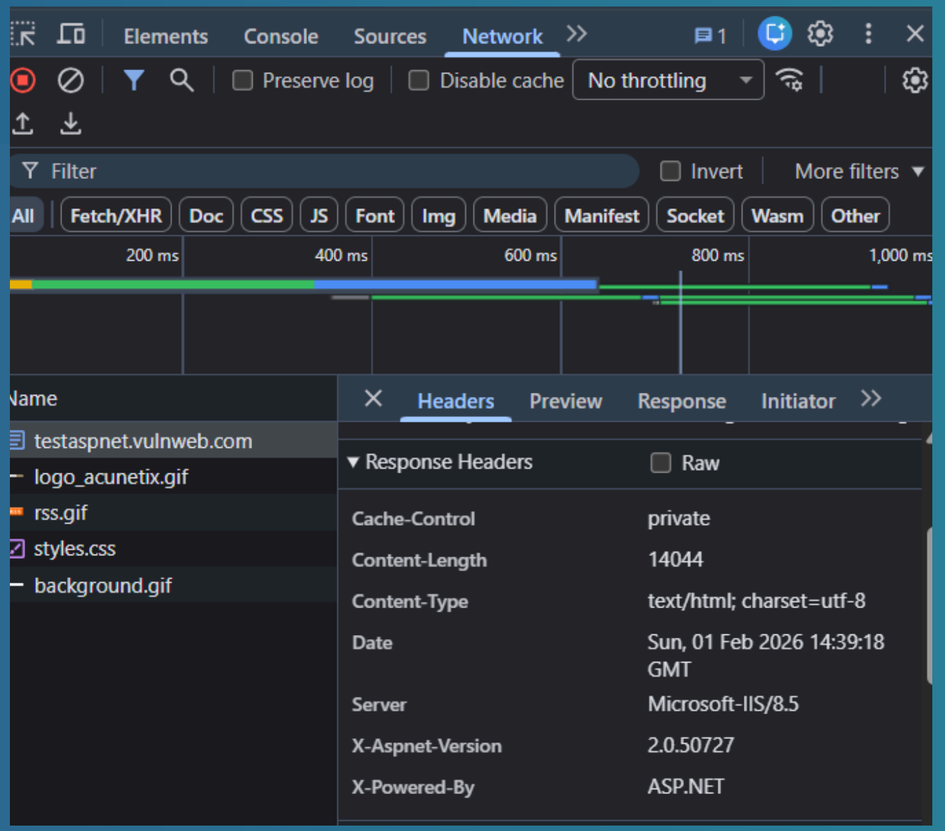
The server exposes backend framework details through the “X-Powered-By” HTTP header, revealing that the application is running on ASP.NET.

Why it Matters

Attackers can identify the underlying technology and target known vulnerabilities.

Recommended Fixes

Remove or disable the X-Powered-By header to prevent information disclosure.



More Vulnerabilities which can be found:

- Server / Configuration Issues
- Authentication Issues-Brute Force
- Cookie & Session Issues
- Input & Web Attacks: SQL injection
- Information Disclosure

Conclusion

The assessment revealed several vulnerabilities that could affect the security of the web application. Issues such as insecure headers, information disclosure, and weak configurations were identified. Fixing these vulnerabilities will help protect user data and improve system reliability. Regular testing and updates are recommended to ensure continued security.