Vulnerability Assessment and Penetration Testing Report

Client / Website Tested
testphp.vulnweb.com
Assessment Type
Vulnerability Assessment and penetration Testing
Intern Name
Rushikesh Borse Cyber Security Intern – Future Interns (2026)
Assessment Date
February 2026

• **The assessment was carried out using: Tools**
• Browser Developer Tools
• Nmap (basic exposure analysis)
• OWASP ZAP (Passive Scan only)

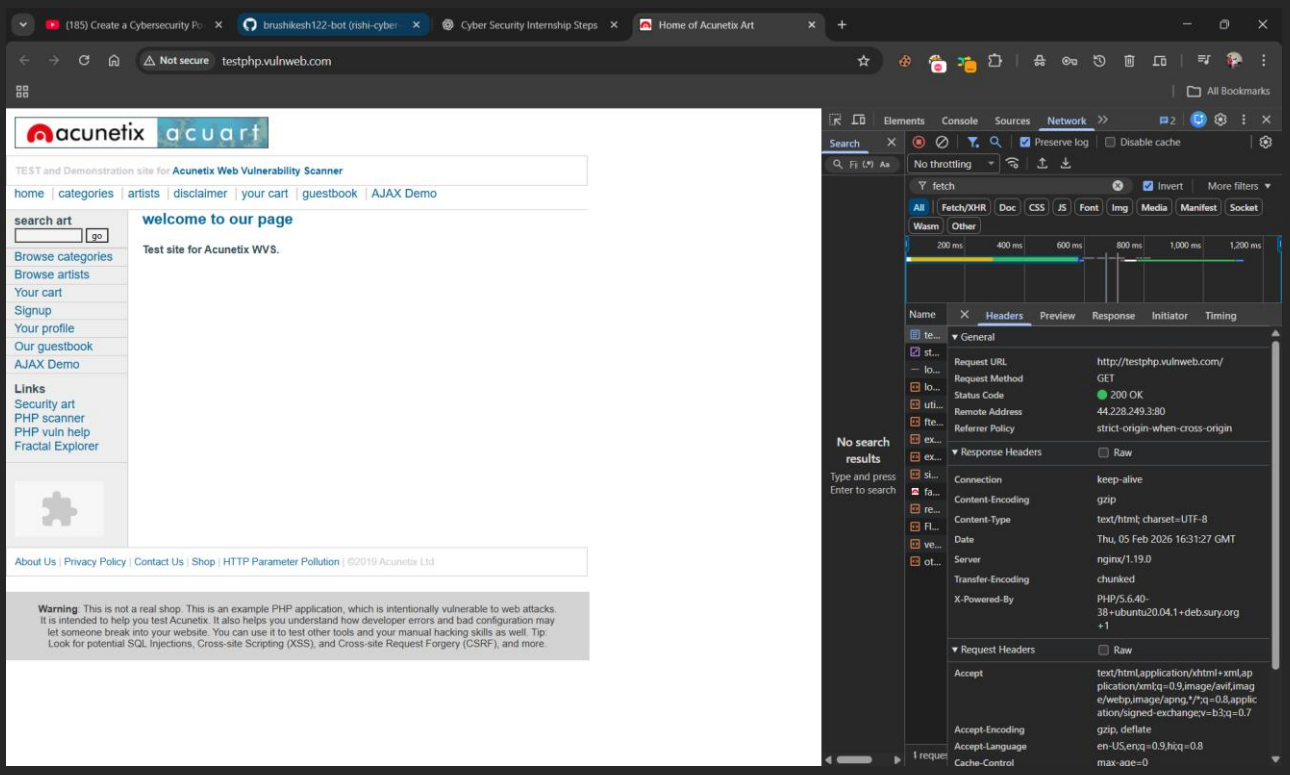
1. No authentication bypass, brute-force attempts, or denial-of-service activities were performed.

1. Executive Summary
This Vulnerability Assessment was conducted to identify common security weaknesses present on a publicly accessible website using non-intrusive and ethical methods.
The objective of this assessment is not to exploit or attack the website, but to provide clarity to a business owner about potential security risks and recommend practical remediation steps.

Finding 1: Missing Security Headers

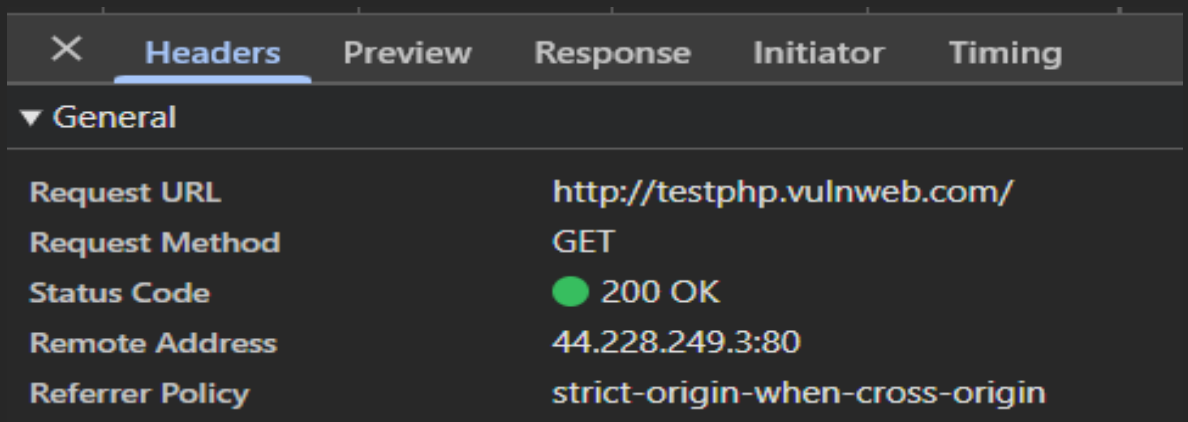
Tool Used: Browser DevTools

What is the issue?
The website is accessible over HTTP, which means data is transmitted without encryption.



Why does it matter?
Without encryption, sensitive information such as login details or user data can be intercepted by attackers. This reduces user trust and may lead to data exposure.
Risk Level :- High
Suggested Remediation (Business-Friendly Fix)
• Enable HTTPS using an SSL/TLS certificate • Redirect all HTTP traffic to HTTPS

•



observed Missing Headers:

- **Content-Security-Policy (CSP)**
- **X-Frame-Options**
- **X-Content-Type-Options**

Why This Matters:

Missing headers increase the risk of:

- **Clickjacking**
- **Cross-Site Scripting (XSS)**
- **Content injection attacks**

Risk Level: Medium

Recommended Remediation:

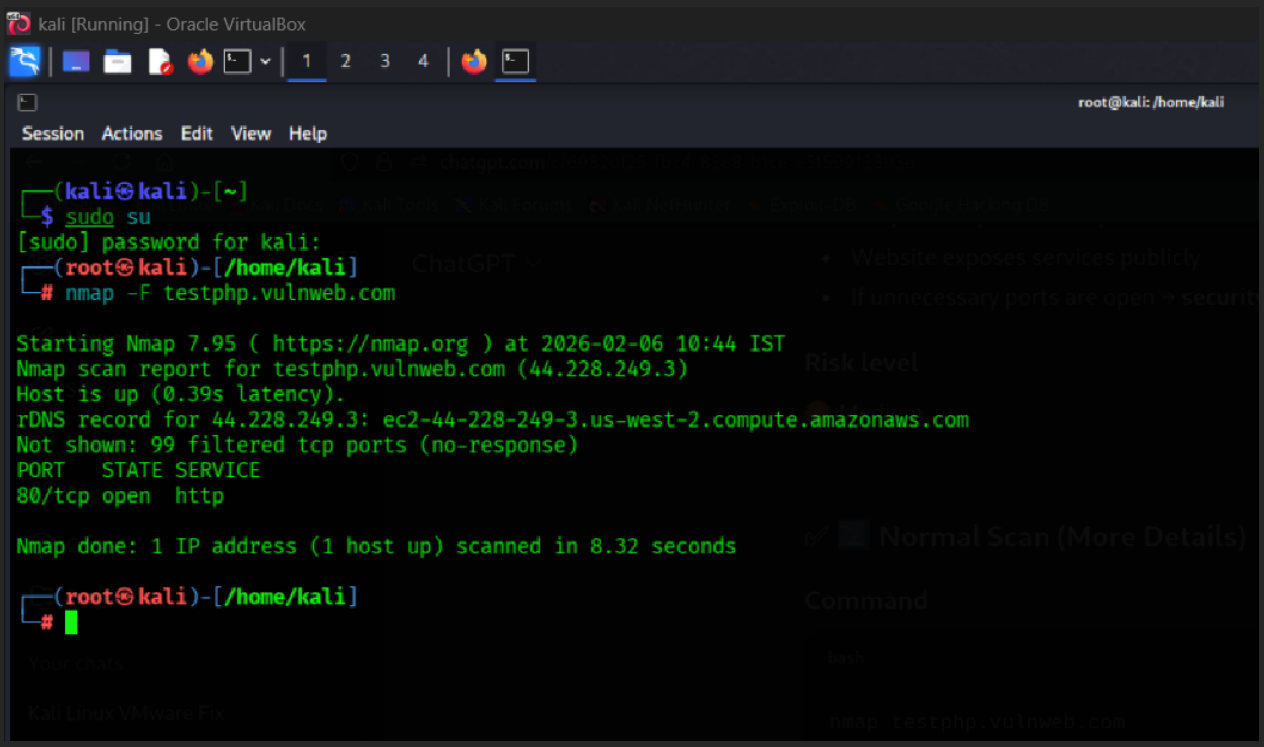
- **Implement standard security headers at the server level**

Finding 2

Nmap 1 : Open HTTP Port (Port 80)

Tool Used: Nmap

Command Example: Nmap -F testphp.vulnweb.com



What was checked?

- Scanned the most commonly used ports to quickly identify exposed services.

Identified Issue: - Common web service ports are open and reachable

Why does it matter? - Open ports increase the attack surface if not properly secured

Risk Level :- Medium

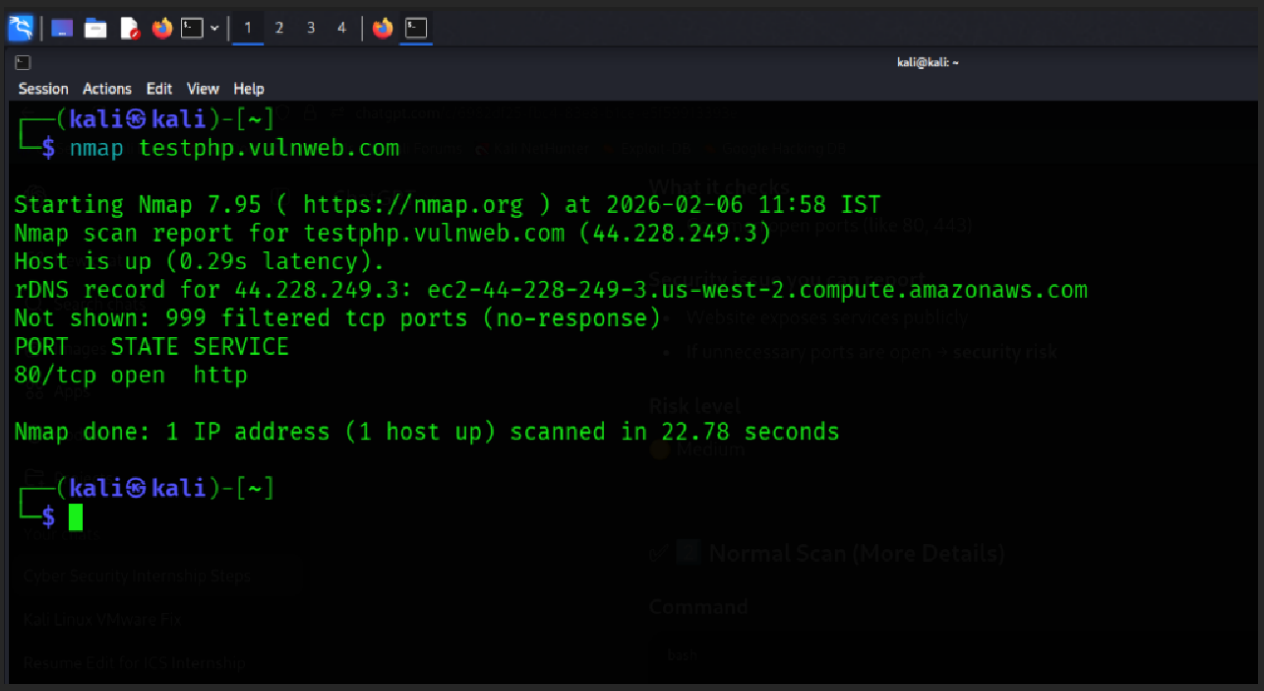
Clear Remediation Steps

- Close unused ports
- Restrict access using firewall rules

Nmap 2: Default Nmap Scan

Tool Used: Nmap

Command Example: nmap testphp.vulnweb.com



What was checked?

- A standard scan to identify **open ports** and **basic service exposure** on the target server.

- **Why does it matter?**
- Port 80 (HTTP) is open and publicly accessible

  Web service is exposed without enforced encryption

Identified Issue

- Port 80 (HTTP) is open and publicly accessible
- Web service is exposed without enforced encryption

Risk Level :- Medium

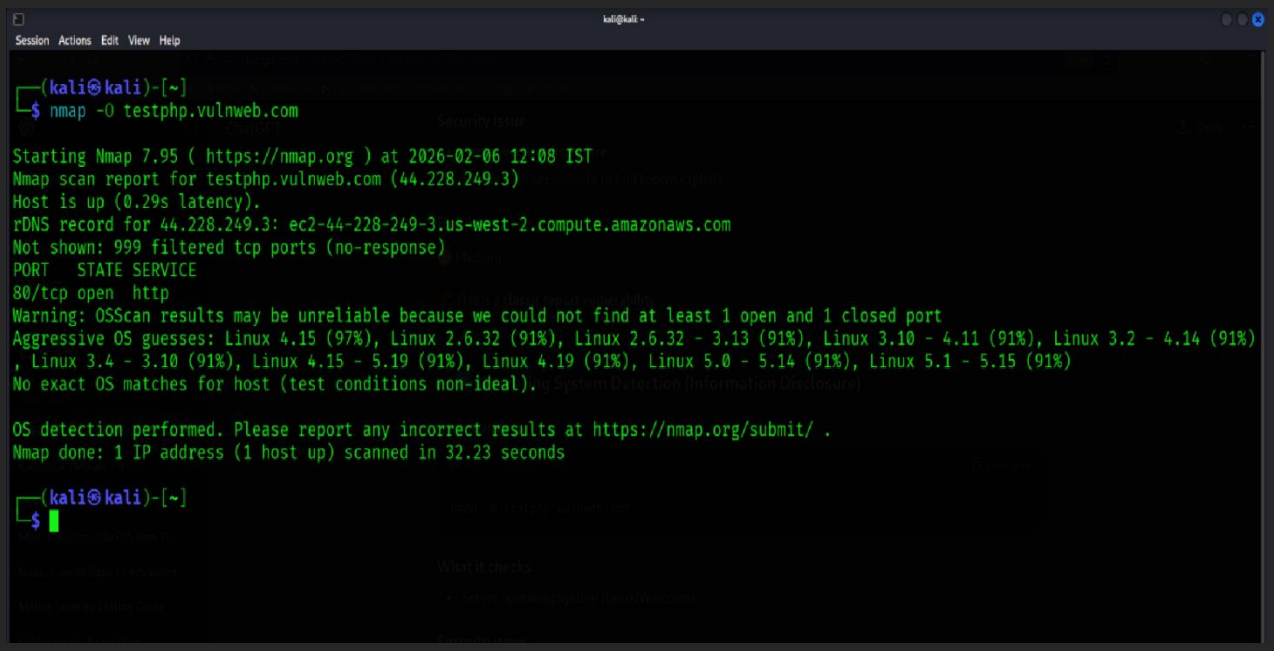
Clear Remediation Steps

- Redirect all HTTP traffic to HTTPS

Nmap 2 : Operating System Detection

Tool Used: Nmap

Command Example: Nmap -O testphp.vulnweb.com



What was checked?

- **Attempted to identify the operating system of the server.**
- **Why does it matter?**

  OS fingerprinting information may be inferred

Identified Issue :-

- **Knowing the operating system helps attackers craft targeted attacks.**

Risk Level :- Low

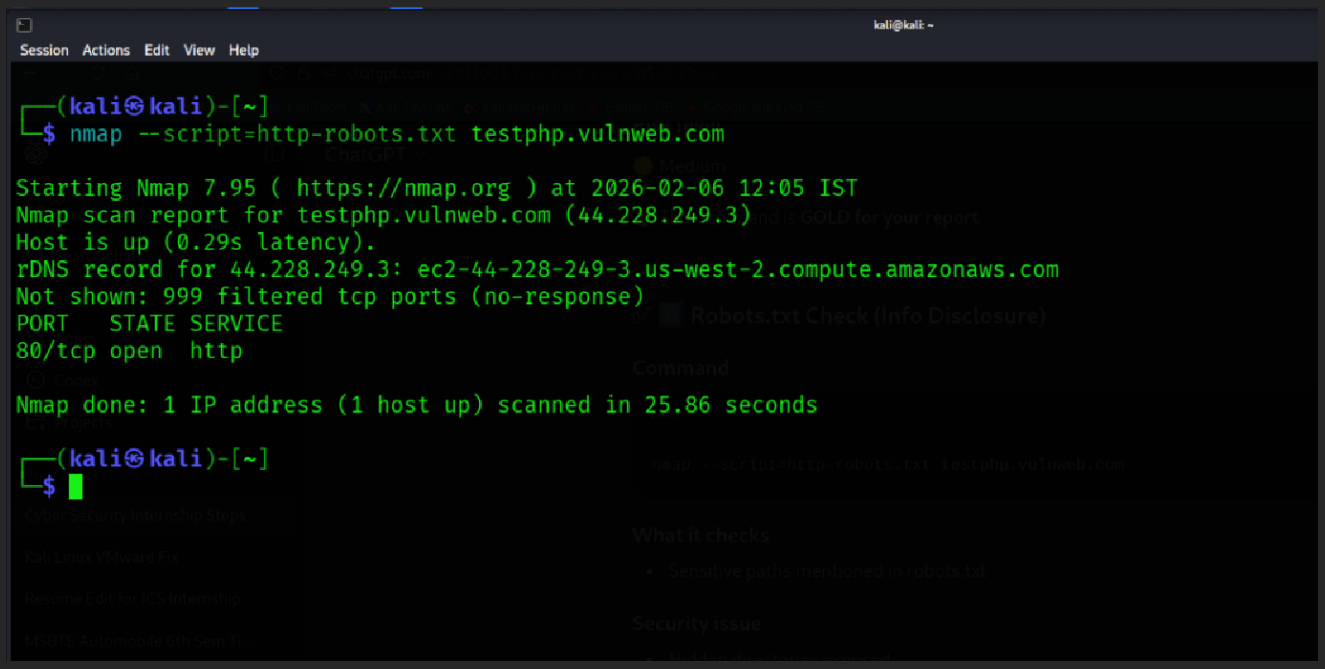
Clear Remediation Steps

- Implement firewall and intrusion prevention rules
- Apply OS hardening measures

Nmap 3 : robots.txt Information Disclosure

Tool Used: Nmap

Command Example: nmap --script=http-robots.txt testphp.vulnweb.com



What was checked?

- **Reviewed the robots.txt file for exposed paths.**
- **Why does it matter?**

  robots.txt file is publicly accessible and reveals internal paths

Identified Issue

- **Attackers canuse these paths to locate hidden or sensitive sections of the website.**

Risk Level :- Low

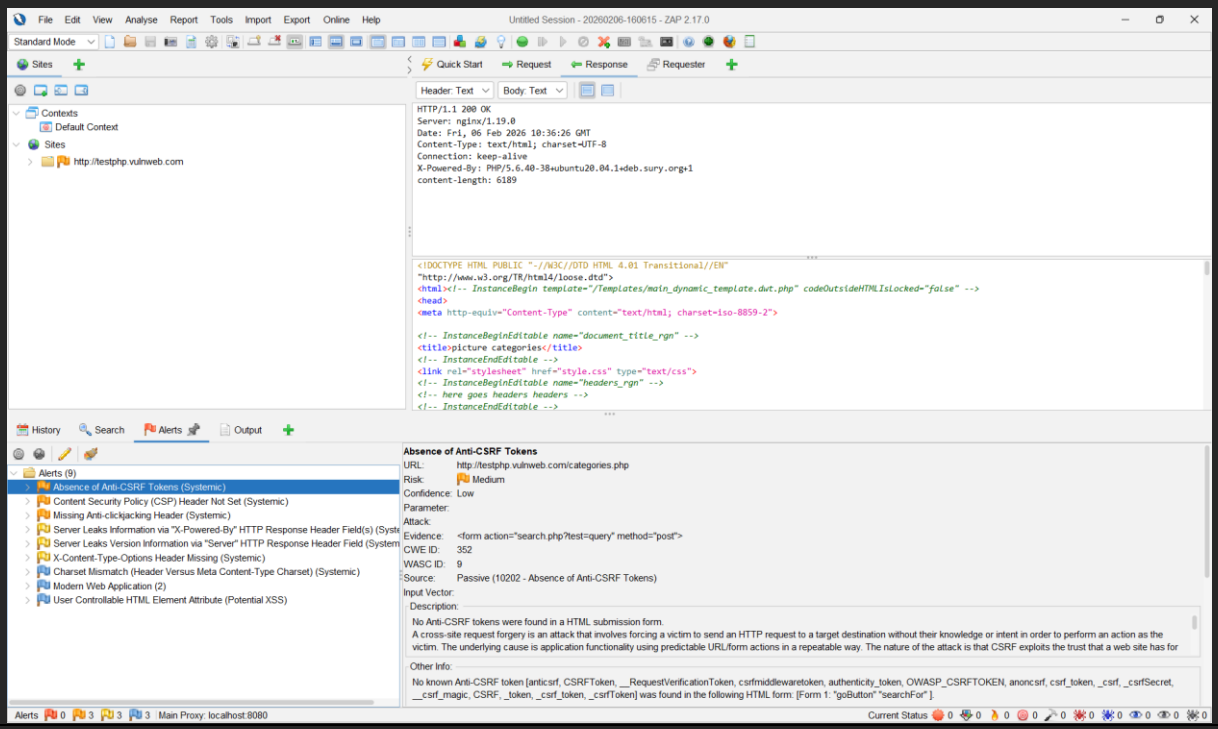
Clear Remediation Steps

- Avoid listing sensitive directories in robots.txt
- Use authentication and access control instead

Finding: - 3

OWASP ZAP Vulnerability Assessment (Passive Scan)

- **Tool Used:** OWASP ZAP (Zed Attack Proxy)



- **Scan Type:** Passive Scan (Read-Only)
- **Target Website:** testphp.vulnweb.com
- **Testing Approach:** Non-intrusive, ethical security analysis

Methodology

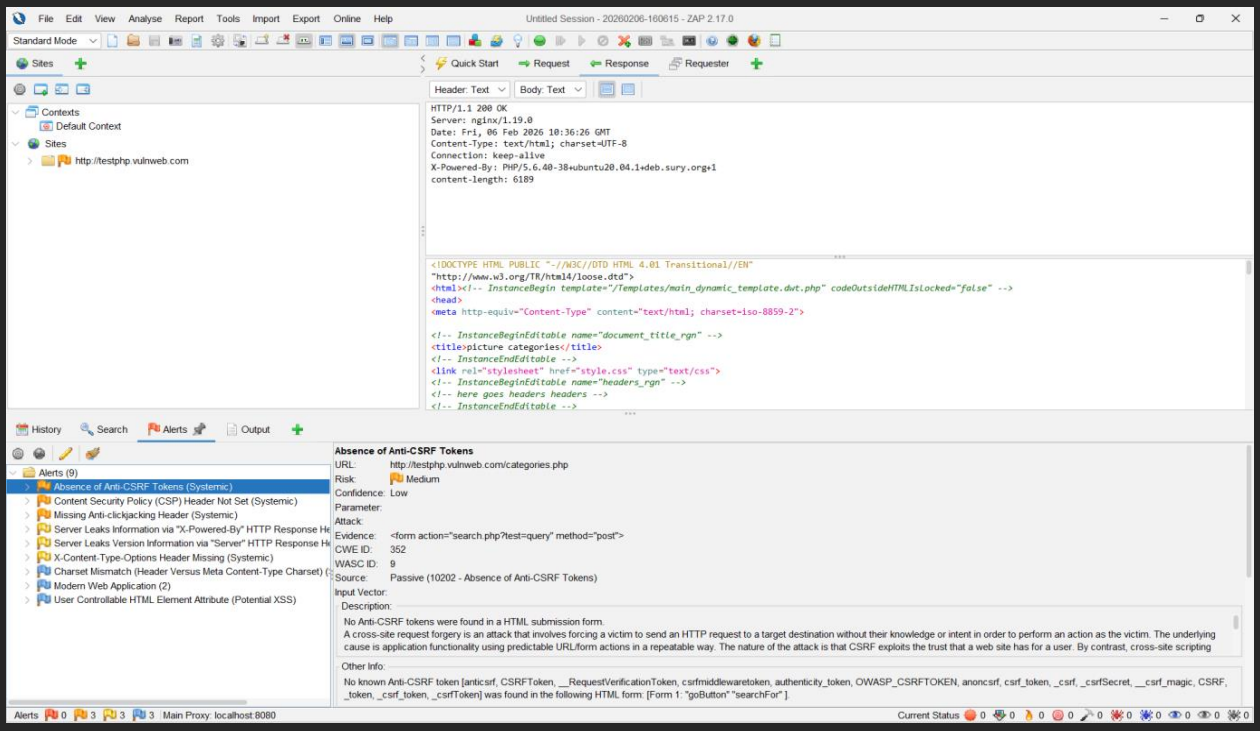
OWASP ZAP was used as a **passive security analysis tool** to monitor traffic between the browser and the website.

The tool identified common web security misconfigurations and weaknesses **without sending malicious requests**.

Owasp zap 1 : Missing Content Security Policy (CSP)

Tool Used: Owasp zap

Command Example: nmap --script=http-robots.txt testphp.vulnweb.com



What was checked?

- **The website does not implement a Content Security Policy (CSP) header.**
- **Why does it matter?**

  Without CSP, attackers may inject malicious scripts into the website, potentially leading to data theft or page manipulation.

Identified Issue

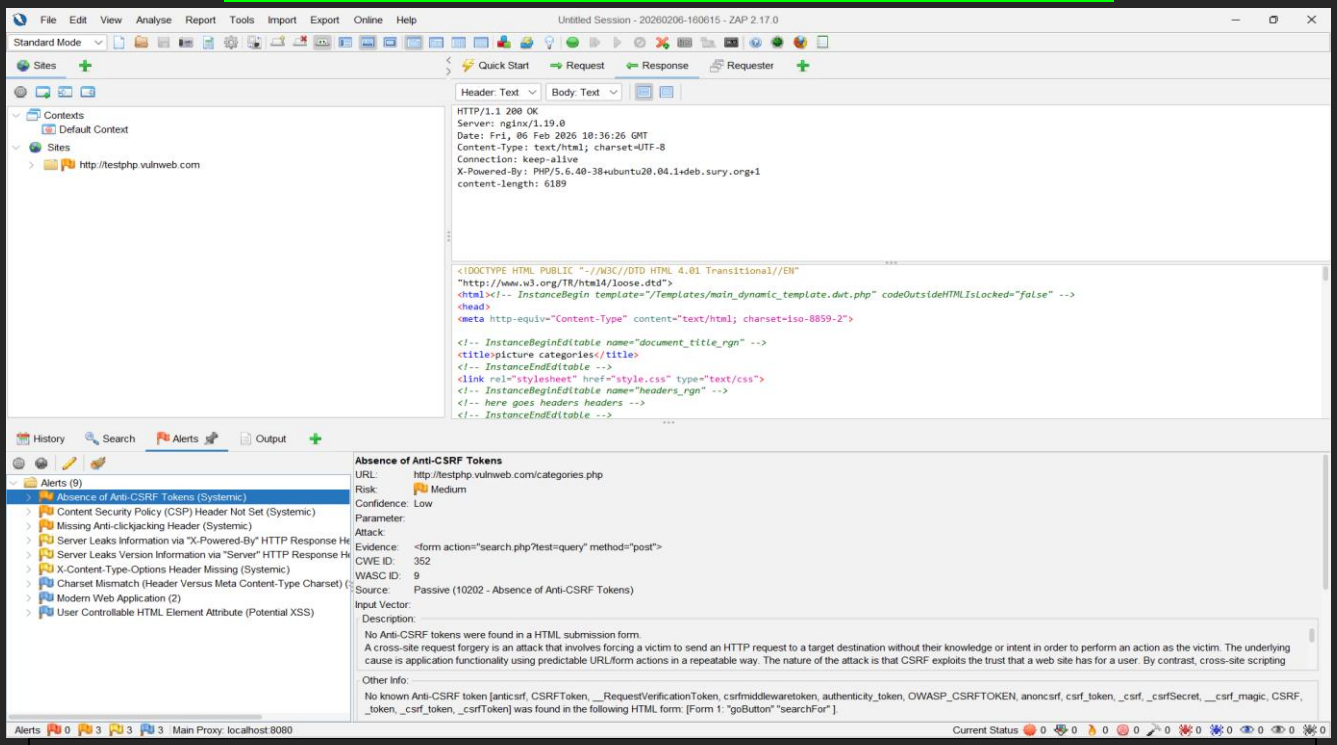
- **Attackers can use these paths to locate hidden or sensitive sections of the**

Risk Level: - medium

Clear Remediation Steps

 Review and update CSP rules during application changes

Finding 2: Missing X-Frame-Options Header



What is the issue?

The website does not include the **X-Frame-Options** header.

Why does it matter?

This can allow attackers to embed the website inside a malicious page, leading to **clickjacking attacks**.

Risk Level: - Medium

Suggested Remediation

- Set X-Frame-Options to DENY or SAMEORIGIN
- Prevent unauthorized framing of the website