Vulnerability Assessment Report

Conducted By: **Rajat Kumar**

Cyber Security Internship Program
Future Interns

February 2026

1 . Introduction

This report presents the findings of a vulnerability assessment conducted on the web application http://testphp.vulnweb.com. The objective of this assessment was to identify potential security weaknesses, open ports, and misconfigurations using automated security tools such as Nmap and OWASP ZAP.

2. Scope of Assessment

The scope of this assessment was limited to publicly accessible services of the target web application. The testing included port scanning, service detection, and automated vulnerability scanning using Nmap and OWASP ZAP. No exploitation or denial-of-service attacks were performed during this assessment.

3. Tools Used

• **Nmap** – Used for port scanning and service detection.

• **OWASP ZAP** – Used for automated vulnerability scanning of the web application.

4. Nmap Scan Results

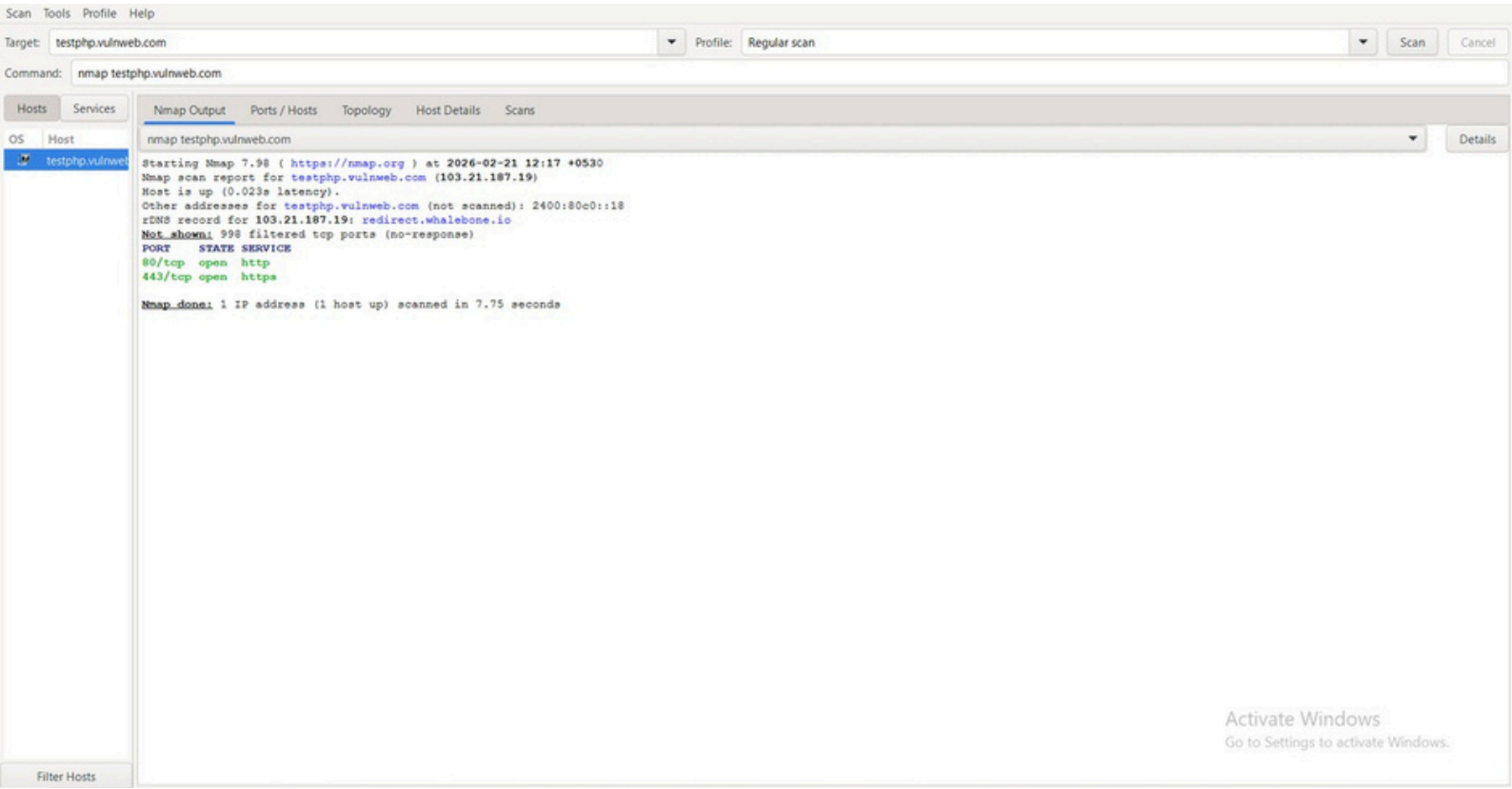
The Nmap scan was performed to identify open ports and running services on the target web application (testphp.vulnweb.com).

Scan Findings:

- Total ports scanned: 1000
- Open ports identified: 2
- Port 80 (HTTP) – Open
- Port 443 (HTTPS) – Open

The results indicate that the web server is accessible over both HTTP and HTTPS protocols. No other open ports were detected during the scan.

Screenshot of Nmap scan output is provided below.



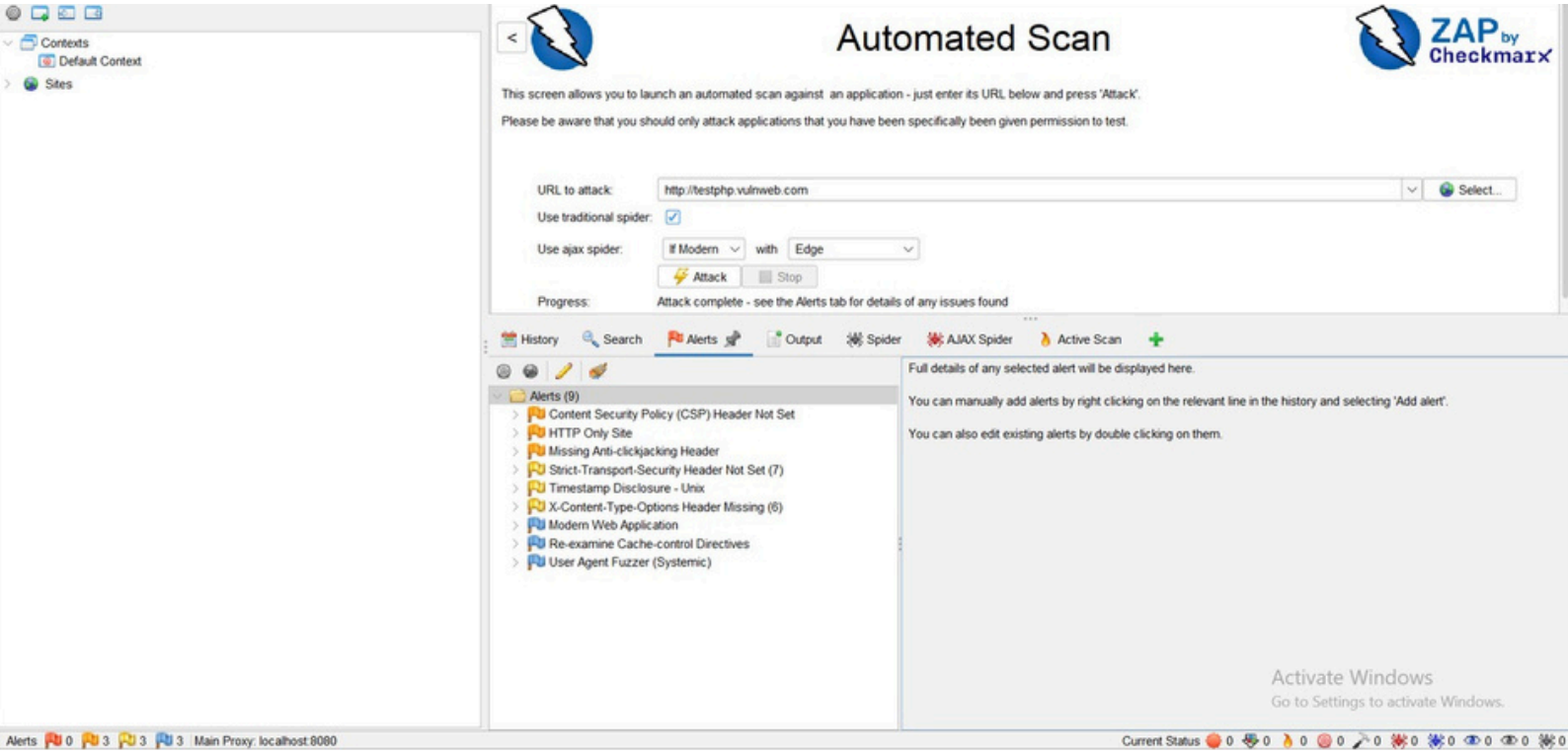
tput | Ports / Hosts | Topology | Host Details | Scans

Protocol	State	Service	Version
tcp	open	http	
tcp	open	https	

5. OWASP ZAP Scan Results

An automated vulnerability scan was conducted using OWASP ZAP against the target web application (http://testphp.vulnweb.com). The scan identified multiple security misconfigurations and missing HTTP security headers.

5.1 Alert Summary



The OWASP ZAP automated scan identified a total of 9 alerts, including medium, low, and informational level vulnerabilities. No high-risk vulnerabilities were detected during this assessment. The findings primarily relate to missing security headers and security misconfigurations.

5.2 Detailed Findings

5.2.1 ContentSecurityPolicy(CSP)HeaderNot Set

Risk Level: Medium

The scan detected that the Content Security Policy (CSP) header is not configured on the web application. CSP helps prevent Cross-Site Scripting (XSS) and other code injection attacks by restricting the sources from which content can be loaded.

Impact:

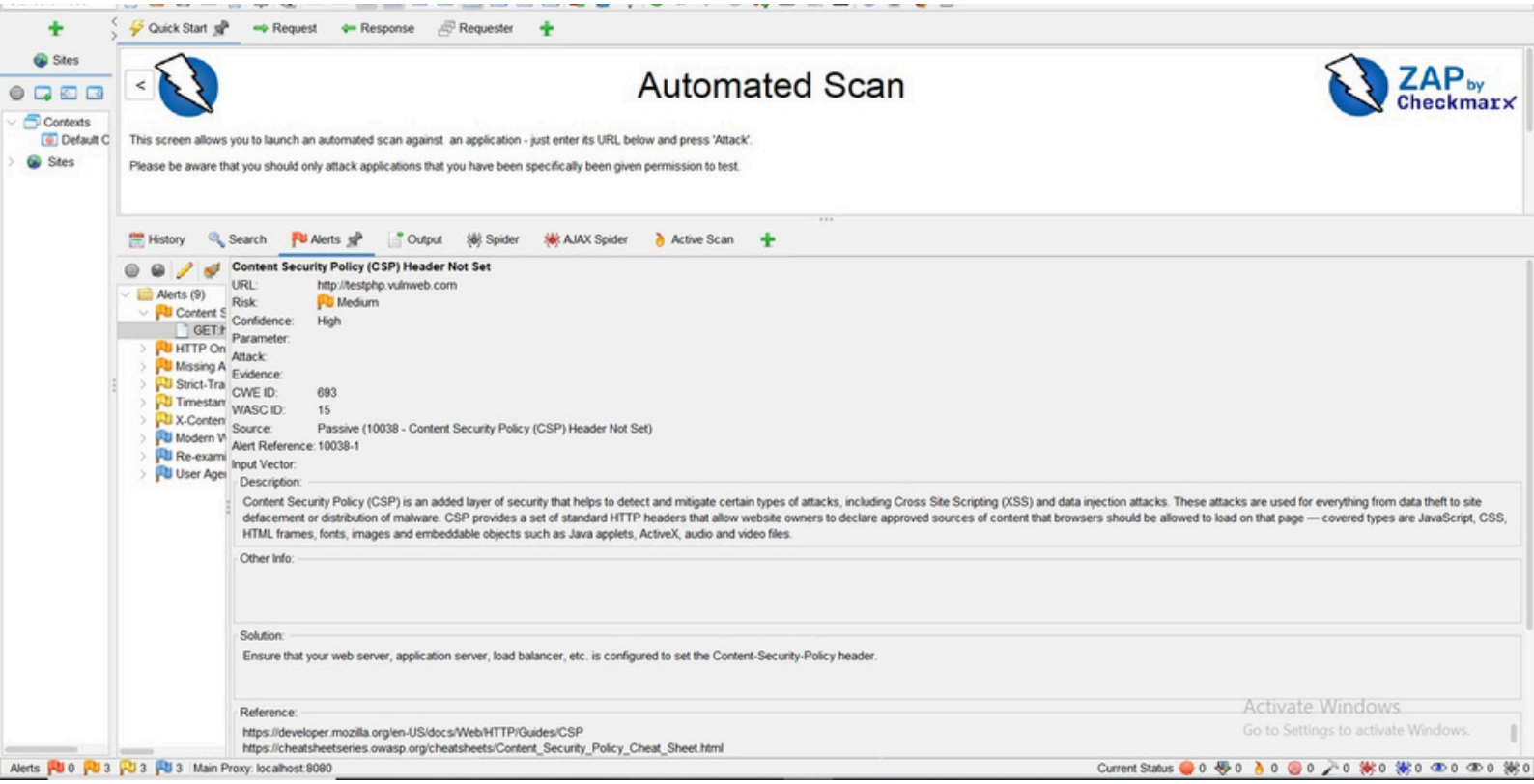
Without CSP, attackers may inject malicious scripts into the application, potentially leading to data theft or session hijacking.

Recommendation:

Implement a properly configured Content Security Policy header to restrict trusted content sources.

Evidence:

Thefollowing screenshot from OWASP ZAP shows the detailed alert information for the Content Security Policy (CSP) Header Not Set vulnerability. The alert confirms that the CSP header is missing in the HTTP response for the tested URL.



The alert is classified as Medium risk with high confidence, indicating a verified security misconfiguration rather than a false positive.

Conclusion

The vulnerability assessment conducted on http://testphp.vulnweb.com identified open HTTP and HTTPS services along with several medium, low, and informational level security findings. No critical or high-risk vulnerabilities were detected during the assessment.

The primary issues identified relate to missing HTTP security headers and configuration weaknesses, which may increase the risk of client-side attacks if not properly addressed. These vulnerabilities do not indicate active exploitation but highlight areas where security hardening is required.

Implementing the recommended security controls, particularly proper configuration of security headers, will enhance the overall security posture of the web application and reduce potential attack vectors.