Task 6: From Finder to Fixer - Writing a Security Recommendation

Name :- Rushikesh Sanjay Kumavat

INTERN ID:- SN1000726

DOMAIN:- Cyber Security

Aim :-

To identify a web application vulnerability and provide a formal security recommendation report with proper remediation steps.

OBJECTIVE :-

- Analyze vulnerabilities discovered during web scanning
- Select one vulnerability for detailed reporting
- Understand its risk and business impact
- Provide clear reproduction steps
- Suggest proper remediation methods
- Verify mitigation strategy

Tools Used :-

- Kali Linux
- Metasploitable 2
- OWASP ZAP

VULNERABILITY DETAILS:-

Vulnerability Name: Content Security Policy (CSP) Header Not Set
Risk Level: Medium
Confidence Level: High
CWE ID: 693

DESCRIPTION:-

The web application does not implement a Content Security Policy (CSP) header.

CSP is a browser security mechanism that controls which resources (scripts, images, styles, etc.) are allowed to load on a webpage.

Without CSP:

- Browsers may execute malicious injected scripts
- XSS risks increase
- Third-party content injection becomes easier

Procedure :-

Step 1: Launch OWASP ZAP

Open ZAP in Kali Linux**.**

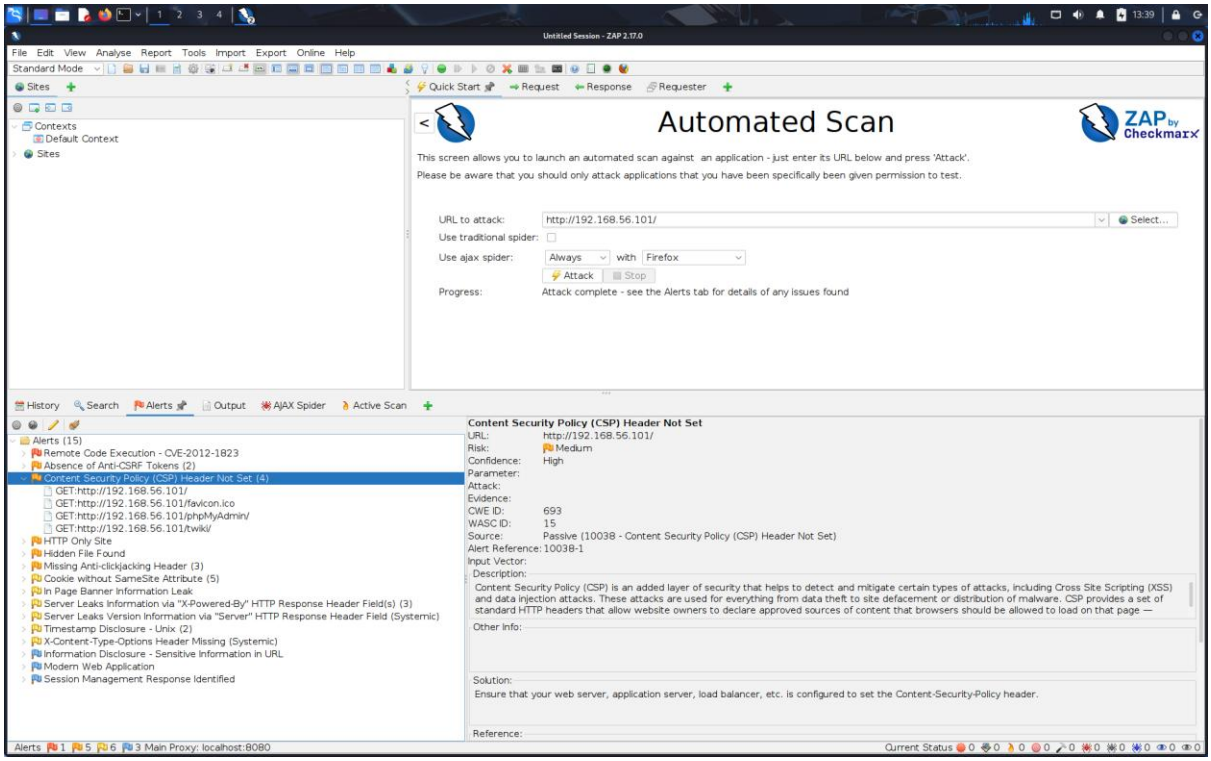
Step 2: Perform Automated Scan

Enter the target URL:

➔ http://192.168.56.101

Click Attack.

Step 3: Wait for Scan Completion



Step 4: Check Alerts Tab

Navigate to the Alerts section.

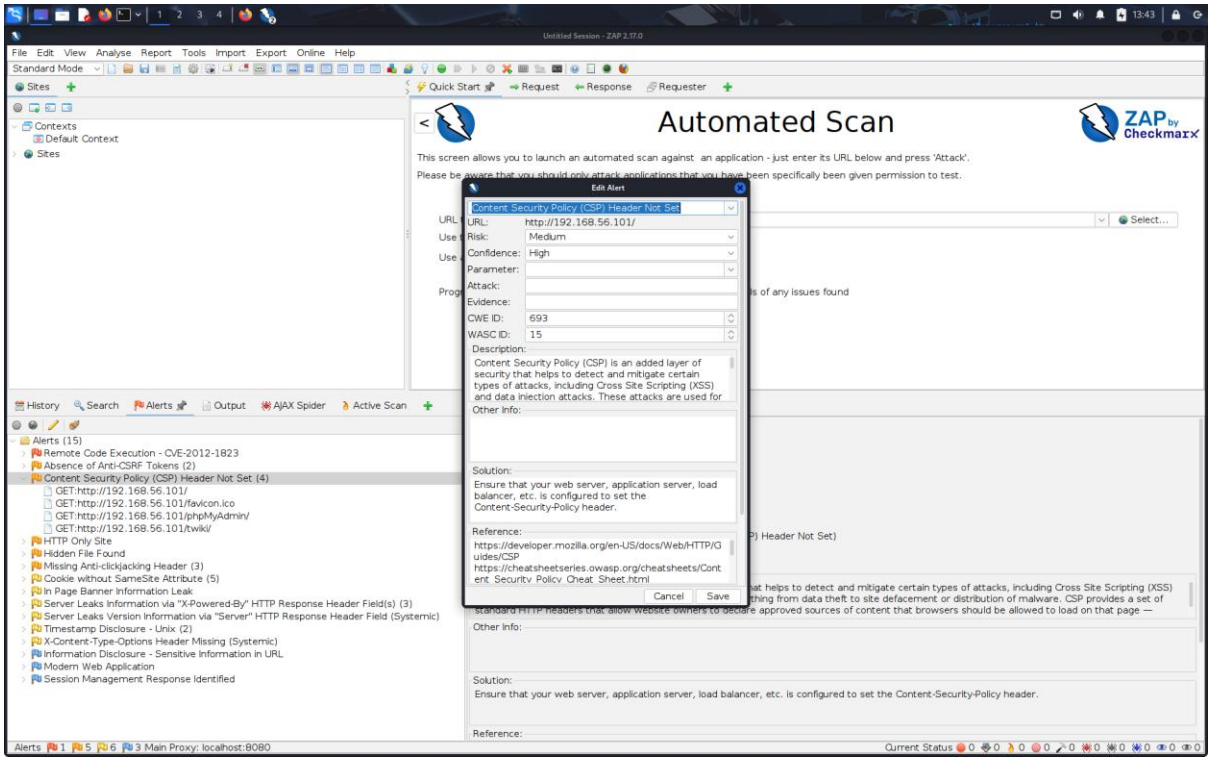
Step 5: Identify Vulnerability

Locate:

➔ Content Security Policy (CSP) Header Not Set

Step 6: Inspect HTTP Response

Confirm that the Content-Security-Policy header is missing.



IMPACT:-

If exploited, an attacker could:

- Inject malicious JavaScript
- Perform Cross-Site Scripting (XSS)
- Steal session cookies
- Hijack user sessions
- Redirect users to malicious sites

In real-world applications, this may result in:

- Data breaches
- Account compromise
- Reputation damage

RESULT :-

The automated scan successfully identified that the web application does not implement a Content Security Policy header. A formal security recommendation was prepared including remediation steps.

CONCLUSION :-

The absence of a CSP header increases exposure to client-side attacks such as XSS. Implementing a strong Content Security Policy significantly improves web application security.

This task demonstrates the ability to transition from vulnerability detection to professional security reporting and solution recommendation.