Vulnerability Assessment Report

Future Interns Task 1

By Aayush Kussial

INTRODUCTION

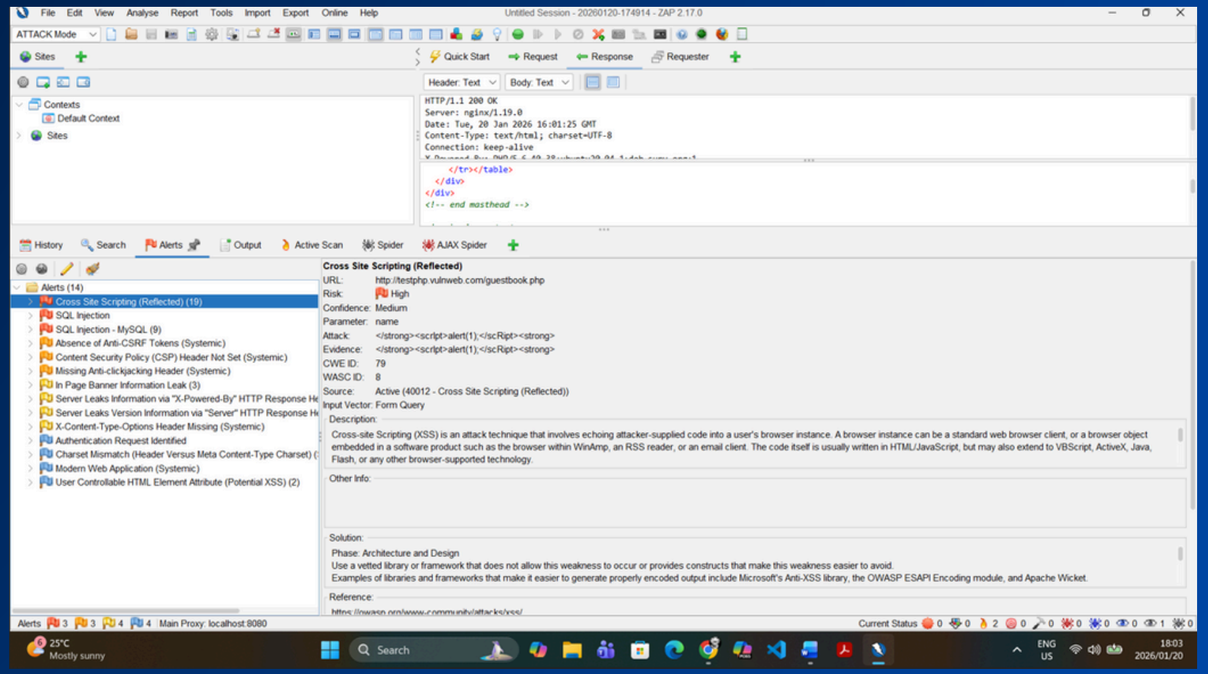
This is a task given to me by Future interns to complete which involved doing a vulnerability assessment report on a live public website. The website i had selected to do this report on is http://testphp.vulnweb.com. The scope of this assessment had included passive and non intrusive testing only, manual inspection using browser developer tools, automated scanning using the tool OWASP ZAP and no exploitation or active attacks were performed.
Tools used were: OWASP ZAP, Google chrome developer tools and Canva

Scope and Methodology

- Website tested : http://testphp.vulnweb.com.
- Passive testing only
- Tools used : OWASP ZAP, Google chrome developer tools, Canva
- No exploitation

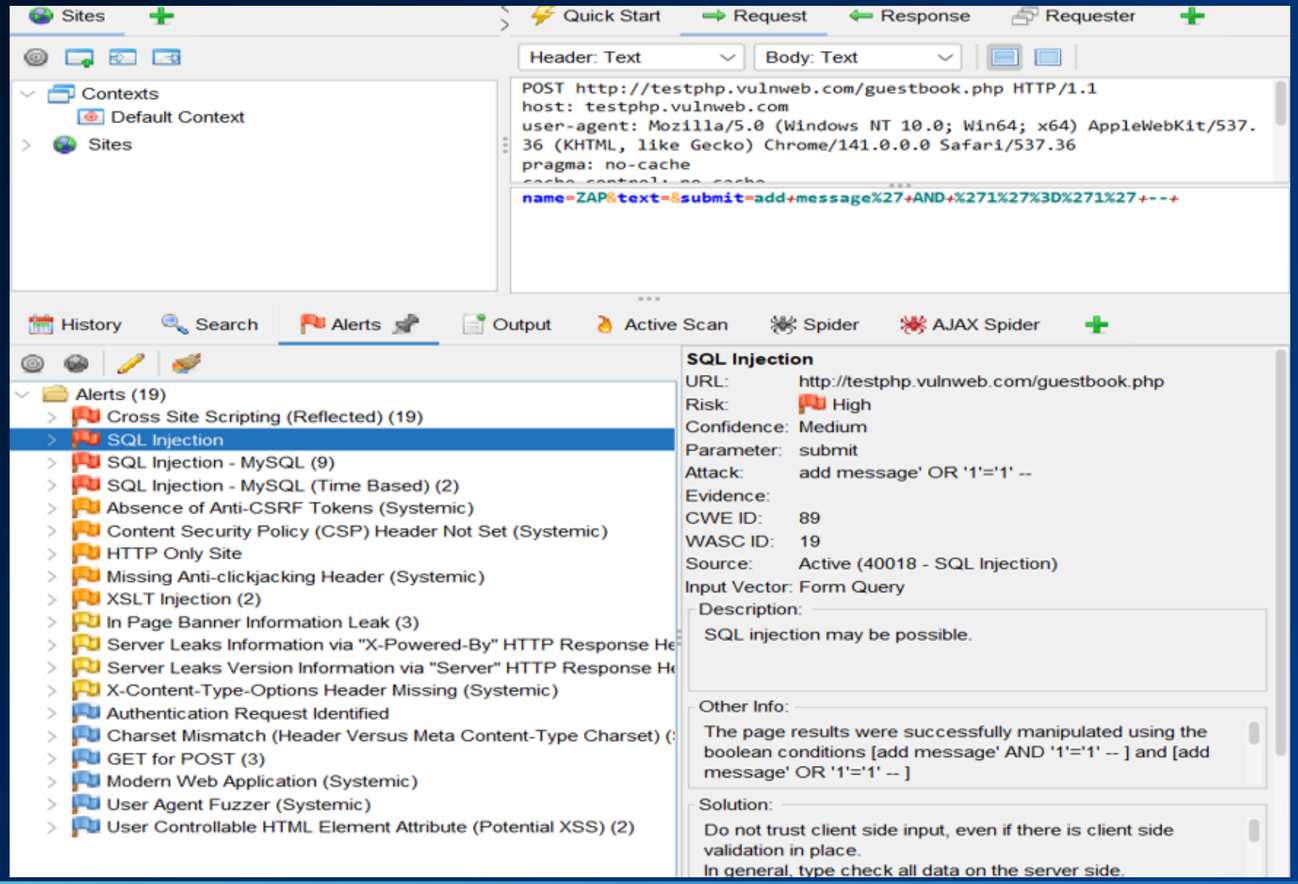
Vulnerabilities

- Cross site scripting(Risk Level: High):attack technique that involves echoing attacker-supplied code into a user's browser instance



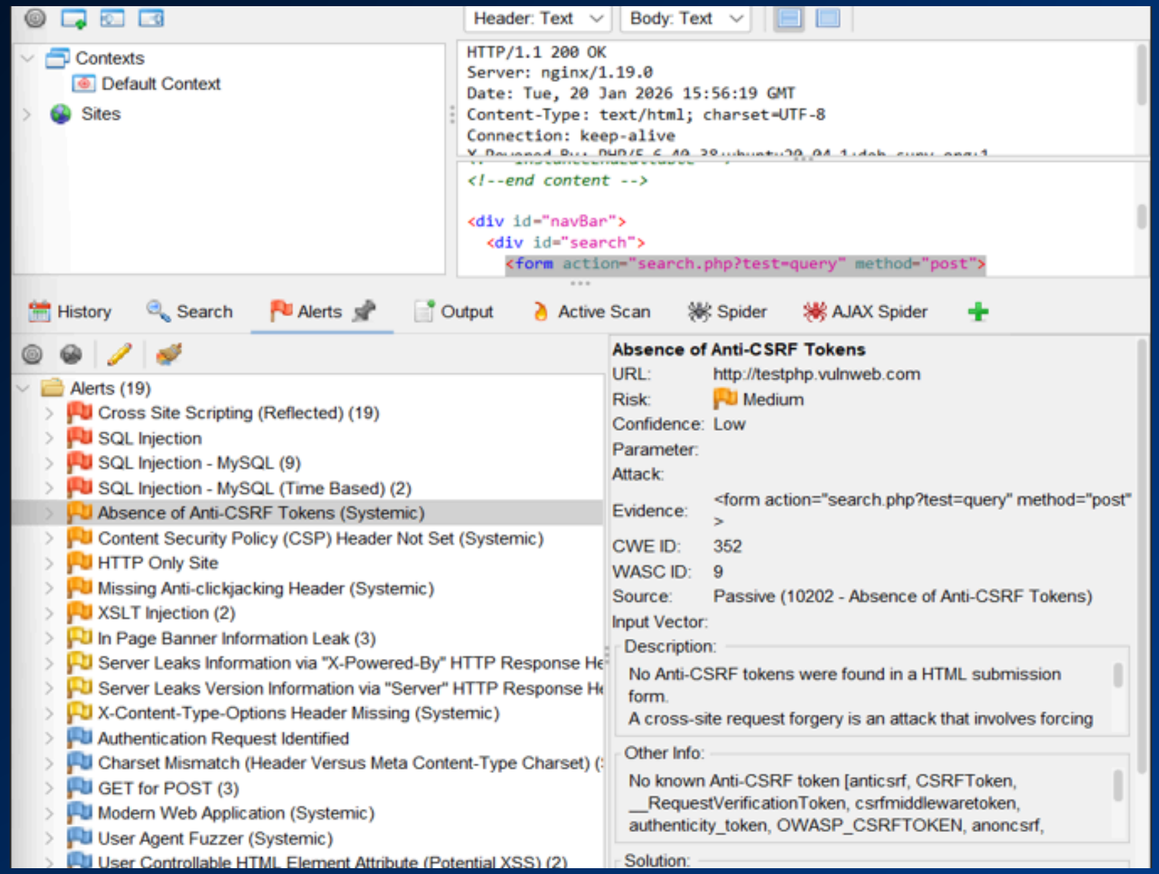
SQL Injection (Risk Level:High):

A cyber attack where malicious SQL code is inserted into database queries.



Absence of anti CSRF token (Risk Level: Medium) :

No anti CSRF tokens were found in HTML submission form.



Remediation Recommendations

- Cross site scripting – encode output before rendering in HTML, validate all user input on server side, implement a strong content security policy.
- SQL Injection – use parameterized queries, apply strict server side input validations, use least privilege database accounts.
- Absence of anti CSRF token – Implement unique CSRF tokens in all state changing forms, validate tokens on the server.

Conclusion

The vulnerability assessment identified multiple security weaknesses including high risk issues such as cross site scripting and SQL injection. These vulnerabilities could potentially be exploited if not resolved. Implementing the recommended remediation measures would improve the security of the application.

THANK YOU