OWASP ZAP Vulnerability Scan Report

Prepared by: Nikhil Kumar Yadav

Internship: Cyber Security Internship - Future Interns

Task: Vulnerability Assessment & Reporting using ZAP

# Table of Contents

1. 1. Executive Summary
2. 2. Scan Methodology
3. 3. Findings
4. 4. Screenshots
5. 5. Recommendations (OWASP Top 10 Mapping)
6. 6. Conclusion

# 1. Executive Summary

This report provides the results of a web application vulnerability scan conducted using OWASP ZAP. The objective was to identify common security flaws such as SQL Injection, Cross-Site Scripting (XSS), and CSRF vulnerabilities. The findings help demonstrate potential risks and provide mitigation strategies.

# 2. Scan Methodology

The following steps were taken during the vulnerability assessment:  
1. Configured OWASP ZAP as a proxy and captured requests.  
2. Performed an automated active scan against the target application (DVWA/Juice Shop).  
3. Reviewed alerts generated by ZAP and validated vulnerabilities.  
4. Collected evidence and mapped issues to OWASP Top 10 categories.

# 3. Findings

Below are sample vulnerabilities identified during the scan:

1. SQL Injection (High Risk)  
Impact: Allows attackers to manipulate database queries.  
Mitigation: Use parameterized queries, input validation.

2. Cross-Site Scripting (Medium Risk)  
Impact: Attacker can inject malicious JavaScript.  
Mitigation: Encode output, validate inputs, use Content Security Policy (CSP).

3. CSRF (Medium Risk)  
Impact: Exploits authenticated sessions to perform unauthorized actions.  
Mitigation: Use anti-CSRF tokens, validate referrer headers.

# 4. Screenshots

Screenshots of ZAP scan results and attack vectors should be added here.

# 5. Recommendations (OWASP Top 10 Mapping)

The following recommendations are provided based on OWASP Top 10:  
- Implement strong input validation (A03: Injection)  
- Apply proper authentication and session management (A07: Identification and Authentication Failures)  
- Enable security headers and CSP (A05: Security Misconfiguration)  
- Use secure frameworks and keep dependencies updated (A06: Vulnerable and Outdated Components)

# 6. Conclusion

The vulnerability scan highlighted critical and medium-risk issues that require immediate attention. Addressing these vulnerabilities will improve the security posture of the web application and reduce the risk of exploitation.