Task 1 Report

Abdullah Akram
ID: DHC-3606

July 8, 2025

1 Introduction

This report summarizes the findings of a security scan conducted using ZAP by Checkmarx on July 8, 2025, at 14:51:27. The scan targeted the site `http://localhost`, with no specific contexts selected, resulting in all contexts being included by default. The report includes vulnerabilities across High, Medium, Low, and Informational risk levels, with confidence levels ranging from Low to High.

2 Summary of Findings

The scan identified a total of 18 alerts across various risk and confidence levels, as detailed below:

- **High Risk (2 Alerts)**:
  - Cross Site Scripting (Reflected): 5 alerts (27.8%) affecting `http://localhost/home`
  - SQL Injection - MySQL: 4 alerts (22.2%) affecting `http://localhost/home-rental`
- **Medium Risk (5 Alerts)**:
  - Content Security Policy (CSP) Header Not Set: 1 alert on `http://localhost/sitem`
  - Application Error Disclosure: 1 alert on `http://localhost/home-rental/app/r`
  - Missing Anti-clickjacking Header: 1 alert on `http://localhost/home-rental/`.
  - Vulnerable JS Library: 1 alert on `http://localhost/home-rental/assets/plug`
  - Absence of Anti-CSRF Tokens: 1 alert on `http://localhost/home-rental/auth/`
- **Low Risk (6 Alerts)**:
  - Server Leaks Version Information: 1 alert on `http://localhost/home-rental/a`
  - Big Redirect Detected: 1 alert on `http://localhost/home-rental/app/registe`
  - Cookie No HttpOnly Flag: 1 alert on `http://localhost/home-rental/`.
  - Cookie without SameSite Attribute: 1 alert on `http://localhost/home-rental/`.
  - Server Leaks Information via "X-Powered-By": 1 alert on `http://localhost/home`

  - X-Content-Type-Options Header Missing: 1 alert on `http://localhost/home-ren`
- **Informational (5 Alerts)**:
  - Authentication Request Identified: 1 alert on `http://localhost/home-rental/a`
  - Information Disclosure - Suspicious Comments: 2 alerts.
  - Modern Web Application: 1 alert.
  - Session Management Response Identified: 1 alert.
  - User Controllable HTML Element Attribute: 1 alert.

3 Recommendations

To address the identified vulnerabilities, the following actions are recommended:

- **Mitigate High-Risk Vulnerabilities**: Implement input validation and parameterized queries to prevent XSS and SQL Injection attacks.
- **Enhance Security Headers**: Add CSP, X-Frame-Options, X-Content-Type-Options, and secure cookie attributes (HttpOnly, SameSite).
- **Update Dependencies**: Replace vulnerable JavaScript libraries with secure versions.
- **Implement CSRF Protection**: Add anti-CSRF tokens to state-changing requests.
- **Reduce Information Leakage**: Suppress server and framework version information, disable detailed error messages, and sanitize code comments.

4 Conclusion

The ZAP scan revealed critical vulnerabilities that require immediate remediation to secure the `http://localhost` site. By implementing the recommended actions, the site's security posture can be significantly improved, reducing the risk of exploitation.