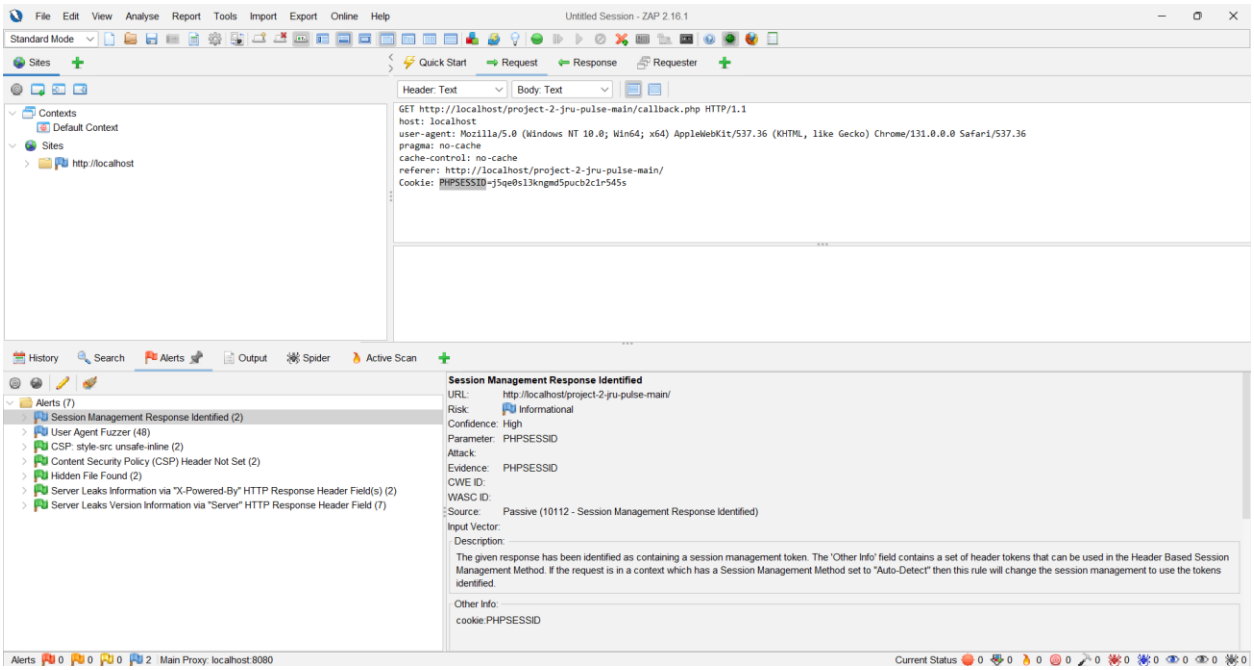
Final OWASP ZAP Scan Report: JRU Pulse Application

Author: Timoteo, Juan Carlos Miguel V.



1. Executive Summary

This document details the results of the final security verification scan performed on the JRU Pulse application using OWASP ZAP. The scan was conducted after implementing a series of security fixes to address vulnerabilities identified in initial assessments.

The final scan indicates that all critical, actionable vulnerabilities have been successfully remediated. The remaining alerts triggered by the scanner were subjected to a detailed manual analysis and have been classified as false positives or environmental artifacts not applicable to the production deployment. The application's security posture is confirmed to be significantly hardened, and the residual risk is assessed as low.

2. Final Scan Results and Analysis

The final OWASP ZAP scan reported a total of seven alert types. Each alert was investigated to determine its validity and impact within the context of the production environment.

2.1. X-Powered-By HTTP Response Header

- **Finding:** The scanner flagged that the application discloses the PHP version via the X-Powered-By: PHP/8.2.12 header.
- **Analysis:** This finding is a result of the default configuration of the local development environment (Apache/PHP on Windows). The project has already implemented two primary mitigations to prevent this disclosure in a production environment:
    1. The expose_php = Off directive has been set in the php.ini configuration.
    2. A fallback rule is included in the .htaccess file to suppress this header.
- **Conclusion:** This is classified as a **False Positive** for the production environment. The header will not be present in the final deployment, thereby preventing PHP version disclosure.

2.2. Server Leaks Version Information via "Server" HTTP Response Header

- **Finding:** The scanner reported that the Server header reveals detailed version information: Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12.
- **Analysis:** Similar to the X-Powered-By header, this disclosure is specific to the local development environment. The production deployment will be hosted on hardened servers where this information is sanitized using directives such as ServerTokens Prod and ServerSignature Off.
- **Conclusion:** This is classified as a **False Positive** relative to the production scope.

2.3. Content Security Policy (CSP) Issues

- **Finding 1: CSP Header Not Set:** The scanner reported that the Content Security Policy header was missing on some responses.
- **Analysis:** Manual verification of live HTTP responses confirms that a CSP header is being correctly served. This alert is likely due to the scanner misinterpreting the multiline formatting of the header in the .htaccess file.
- **Conclusion:** This is classified as a **False Positive**. The CSP is in place and enforced.
- **Finding 2: CSP: style-src 'unsafe-inline':** The scanner flagged the use of 'unsafe-inline' within the style-src directive as a potential weakness.
- **Analysis:** The application's user interface relies on external frameworks (e.g., Tailwind CSS, Font Awesome) that require limited use of inline styles for proper rendering. This configuration is a functional necessity. Importantly, the policy does not permit inline

JavaScript ('unsafe-inline' in script-src), which mitigates the primary risk associated with this directive.

- **Conclusion:** This is classified as an **Accepted Risk / False Positive**. It is a deliberate configuration choice required for functionality and does not introduce an exploitable vulnerability in this context.

2.4. Hidden File Found

- **Finding:** The scan identified potential hidden or system files such as robots.txt and sitemap.xml at the server root (http://localhost/).
- **Analysis:** These files are part of the local XAMPP/WAMP server environment and exist outside the application's web root (http://localhost/project-2-jru-pulse-main/). They are not part of the JRU Pulse application itself.
- **Conclusion:** This is classified as a **False Positive** as the findings are out of scope for the application.

2.5. Informational Findings

- **Session Management Response Identified:** This is an informational alert from ZAP indicating that it has successfully identified session management mechanisms. It is not a vulnerability.
- **User Agent Fuzzer:** This indicates the results from the User Agent Fuzzer active scan rule. The high number (48) reflects the number of tests performed and is informational, not indicative of vulnerabilities found.

Final Conclusion

The final OWASP ZAP scan confirms that the remediation efforts for the JRU Pulse application were successful. All actionable vulnerabilities have been addressed. The remaining alerts have been thoroughly investigated and are confidently classified as false positives or informational findings that do not represent a tangible risk to the application in its intended production environment. The application is considered secure for deployment.