Dated: 12th March 2025

**Week 1: Crud APP**

Intern: Hassan Nawaz

**OWASP ZAP Security Assessment Report (Week 1)**

**1. Overview**

* **Project Name:** CRUD React App
* **Testing Tool:** OWASP ZAP
* **Target URL:** http://localhost:3000
* **Objective:** Identify security vulnerabilities in the application before implementing security fixes.

**2. Summary of Findings**

The OWASP ZAP scan revealed the following vulnerabilities:

**🔴 High-Risk Vulnerabilities**

1. **Cross-Site Scripting (XSS) - Input Fields Not Sanitized**

* **Issue:** User input fields accepted <script>alert('XSS');</script> and executed JavaScript in the browser.
* **Risk:** Allows attackers to steal session cookies, deface the site, or perform malicious actions.
* **Recommendation:** Implement input sanitization using DOMPurify.

1. **CSP (Content Security Policy) Header Missing**

* **Issue:** The application does not have a Content-Security-Policy header.
* **Risk:** Increases the risk of **XSS and data injection attacks**.
* **Recommendation:** Set a strict CSP policy using react-helmet.

**🔴 Medium-Risk Vulnerabilities**

1. **CORS Misconfiguration (Allowing \* Requests)**

* **Issue:** Access-Control-Allow-Origin: \* was found in the response headers.
* **Risk:** Any website can make API requests, potentially exposing user data.
* **Recommendation:** Restrict CORS to trusted domains only.

1. **Clickjacking Vulnerability - Missing X-Frame-Options Header**

* **Issue:** The app can be embedded inside an iframe.
* **Risk:** Users can be tricked into performing unintended actions (Clickjacking attack).
* **Recommendation:** Use X-Frame-Options: DENY to prevent iframe embedding.

**🔴 Low-Risk Vulnerabilities**

1. **Missing Security Headers (X-Content-Type-Options, Strict-Transport-Security)**

* **Issue:** The application lacks essential security headers.
* **Risk:** Attackers can exploit MIME type sniffing or downgrade HTTPS security.
* **Recommendation:** Use helmet middleware to add missing headers.



