**Vulnerability Scan Report**

**Demo Website Used: *Zero Web App Security***

**Free Scan Tool: *OWASP ZAP***

**Alerts:** Based on the OWASP ZAP scan, the following vulnerabilities were detected:

1. **Content Security Policy (CSP) Header Not Set** (7 instances)
   * Risk Level: Medium
   * Description: Lack of a CSP header allows attackers to inject malicious scripts (Cross-Site Scripting - XSS).
   * Recommendation: Implement a strict CSP policy to mitigate XSS attacks.
2. **Cross-Domain Misconfiguration** (42 instances)
   * Risk Level: High
   * Description: This vulnerability indicates improper handling of cross-domain policies, making it easier for attackers to exploit sensitive data.
   * Recommendation: Configure cross-domain policies securely and restrict access to trusted domains.
3. **Missing Anti-Clickjacking Header** (5 instances)
   * Risk Level: Medium
   * Description: The application lacks headers that prevent UI redress attacks (Clickjacking).
   * Recommendation: Implement X-Frame-Options headers.
4. **Vulnerable JavaScript Libraries**
   * Risk Level: High
   * Description: Outdated or insecure JavaScript libraries increase the risk of exploitation.
   * Recommendation: Update JavaScript libraries to secure versions.



