Report Date: Mon 25 Mar 2024
ZAP Version: 2.14.0
Generated with ZAP on: Mon 25 Mar 2024, at 19:39:52

---

1. About this report

The report provides an overview of the vulnerabilities identified through the scanning process using ZAP.

---

2. Summaries

Alert counts by risk and confidence

High Risk: 1 (3.6%)
Medium Risk: 15 (53.6%)
Low Risk: 7 (25.0%)
Informational: 5 (17.9%)

Alert counts by site and risk

The site https://imagekit.io has the highest number of alerts across all risk levels.

Alert counts by alert type

Most prevalent alert types include Content Security Policy (CSP) issues and Information Disclosure.

---

3. Alerts

High Risk, Confidence=Medium: Hash Disclosure - Mac OSX salted SHA-1.
Medium Risk, Confidence=High: Absence of Anti-CSRF Tokens, CSP: Wildcard Directive, Content Security Policy (CSP) Header Not Set.
Medium Risk, Confidence=Medium: Missing Anti-clickjacking Header, Cross-Domain Misconfiguration.
Medium Risk, Confidence=Low: Absence of Anti-CSRF Tokens.
Low Risk, Confidence=High: Strict-Transport-Security Header Not Set.
Low Risk, Confidence=Medium: Cross-Domain JavaScript Source File Inclusion, X-Content-Type-Options Header Missing, Cookie No HttpOnly Flag, Secure Pages Include Mixed Content, Timestamp Disclosure - Unix.
Low Risk, Confidence=Low: Timestamp Disclosure - Unix.
Informational, Confidence=High: Session Management Response Identified.
Informational, Confidence=Medium: Modern Web Application, Retrieved from Cache.
Informational, Confidence=Low: Information Disclosure - Suspicious Comments, Authentication Request Identified, Re-examine Cache-control Directives, User Controllable HTML Element Attribute (Potential XSS).

Recommendations:

- Implement proper Content Security Policy (CSP) to mitigate the risk of content injection attacks.
- Ensure the presence of Anti-CSRF Tokens to prevent Cross-Site Request Forgery (CSRF) attacks.
- Configure Strict-Transport-Security Headers to enforce secure communication over HTTPS.
- Review and fix cross-domain misconfigurations to prevent unauthorized data access.
- Regularly review cache-control directives to maintain data confidentiality and integrity.
- Implement input validation mechanisms to prevent potential XSS vulnerabilities

---

Conclusion:

The scanning report reveals several vulnerabilities across different risk levels, with the majority falling under the medium risk category. It's crucial to address these issues promptly to enhance the security posture of the scanned websites.