ZAP by Checkmarx Scanning Report

Generated with ZAP on 금 14 2월 2025, at 15:51:07

ZAP Version: 2.16.0

ZAP by Checkmarx

Contents

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- https://cdn.jsdelivr.net
- https://www.gstatic.com
- https://www.google.com
- http://localhost:8090

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

Risk levels

Included: High, Medium, Low, Informational

Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, 거짓 긍정

Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	1 (4.8%)	0 (0.0%)	1 (4.8%)
	Medium	0 (0.0%)	2 (9.5%)	4 (19.0%)	0 (0.0%)	6 (28.6%)
	Low	0 (0.0%)	1 (4.8%)	5 (23.8%)	1 (4.8%)	7 (33.3%)
	Informational	0 (0.0%)	1 (4.8%)	4 (19.0%)	2 (9.5%)	7 (33.3%)
	Total	0 (0.0%)	4 (19.0%)	14 (66.7%)	3 (14.3%)	21 (100%)

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://www.gstatic.com	0 (0)	1 (1)	1 (2)	1 (3)
	https://www.google.com	0 (0)	0 (0)	1 (1)	0 (1)
	http://localhost:8090	1 (1)	5 (6)	5 (11)	6 (17)

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Path Traversal	High	1 (4.8%)
Content Security Policy (CSP) Header Not Set	Medium	16 (76.2%)
Cross-Domain Misconfiguration	Medium	4 (19.0%)
Format String Error	Medium	1 (4.8%)
Missing Anti-clickjacking Header	Medium	16 (76.2%)
Session ID in URL Rewrite	Medium	2 (9.5%)
XSLT Injection	Medium	1 (4.8%)
Application Error Disclosure	Low	1 (4.8%)
Cookie without SameSite Attribute	Low	1 (4.8%)
Cross-Domain JavaScript Source File Inclusion	Low	16 (76.2%)
Referer Exposes Session ID	Low	2 (9.5%)
Strict-Transport-Security Header Not Set	Low	3 (14.3%)
Timestamp Disclosure - Unix	Low	36 (171.4%)
X-Content-Type-Options Header Missing	Low	23 (109.5%)
Authentication Request Identified	Informational	1 (4.8%)
Information Disclosure - Sensitive Information in URL	Informational	2 (9.5%)
Information Disclosure - Suspicious Comments	Informational	26 (123.8%)
Loosely Scoped Cookie	Informational	2 (9.5%)
Modern Web Application	Informational	13 (61.9%)
Retrieved from Cache	Informational	20 (95.2%)
Session Management Response Identified	Informational	3 (14.3%)
Total		21

Alerts

1. **Risk=High, Confidence=Medium (1)**
    1. **http://localhost:8090 (1)**
        1. **Path Traversal (1)**
            - ▶ GET http://localhost:8090/board/download?filename=c%3A%2FWindows%2Fsystem.ini
2. **Risk=Medium, Confidence=High (2)**
    1. **http://localhost:8090 (2)**
        1. **Content Security Policy (CSP) Header Not Set (1)**
            - ▶ GET http://localhost:8090/login2
        2. **Session ID in URL Rewrite (1)**
            - ▶ GET http://localhost:8090/login2;jsessionid=43A0364F9361D79E699F5B3A3D808D6D
3. **Risk=Medium, Confidence=Medium (4)**
    1. **https://www.gstatic.com (1)**
        1. **Cross-Domain Misconfiguration (1)**
            - ▶ GET https://www.gstatic.com/recaptcha/releases/IyZ984yGrXrBd6ihLOYGwy9X/recaptcha__ko.js
    2. **http://localhost:8090 (3)**
        1. **Format String Error (1)**
            - ▶ GET http://localhost:8090/board/download?
filename=ZAP%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%
        2. **Missing Anti-clickjacking Header (1)**
            - ▶ GET http://localhost:8090/board/search?query=ZAP
        3. **XSLT Injection (1)**
            - ▶ GET http://localhost:8090/board/download?filename=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E
4. **Risk=Low, Confidence=High (1)**
    1. **https://www.google.com (1)**
        1. **Strict-Transport-Security Header Not Set (1)**
            - ▶ GET https://www.google.com/recaptcha/api.js
5. **Risk=Low, Confidence=Medium (5)**
    1. **http://localhost:8090 (5)**
        1. **Application Error Disclosure (1)**
            - ▶ POST http://localhost:8090/board/update
        2. **Cookie without SameSite Attribute (1)**

        - ▶ POST http://localhost:8090/login

    3. **Cross-Domain JavaScript Source File Inclusion (1)**
        - ▶ GET http://localhost:8090/login2
    4. **Referer Exposes Session ID (1)**
        - ▶ GET http://localhost:8090/login2;jsessionid=43A0364F9361D79E699F5B3A3D808D6D
    5. **X-Content-Type-Options Header Missing (1)**
        - ▶ GET http://localhost:8090/board/download?filename=%EC%8B%9C%ED%97%98%20%EC%A0%95%EB%A6%AC.txt

6. **Risk=Low, Confidence=Low (1)**
    1. **https://www.gstatic.com (1)**
        1. **Timestamp Disclosure - Unix (1)**
            - ▶ GET https://www.gstatic.com/recaptcha/releases/IyZ984yGrXrBd6ihLOYGwy9X/recaptcha__ko.js
7. **Risk=Informational, Confidence=High (1)**
    1. **http://localhost:8090 (1)**
        1. **Authentication Request Identified (1)**
            - ▶ POST http://localhost:8090/login
8. **Risk=Informational, Confidence=Medium (4)**
    1. **https://www.gstatic.com (1)**
        1. **Retrieved from Cache (1)**
            - ▶ GET https://www.gstatic.com/recaptcha/releases/IyZ984yGrXrBd6ihLOYGwy9X/recaptcha__ko.js
    2. **http://localhost:8090 (3)**
        1. **Information Disclosure - Sensitive Information in URL (1)**
            - ▶ GET http://localhost:8090/board/search?price=1&publisher=test_file.txt&query=ZAP&saleUser=ZAP&status=N&title=ZAP&writer=ZAP
        2. **Modern Web Application (1)**
            - ▶ GET http://localhost:8090/board/search?query=ZAP
        3. **Session Management Response Identified (1)**
            - ▶ POST http://localhost:8090/login
9. **Risk=Informational, Confidence=Low (2)**
    1. **http://localhost:8090 (2)**
        1. **Information Disclosure - Suspicious Comments (1)**
            - ▶ GET http://localhost:8090/board/search?query=ZAP
        2. **Loosely Scoped Cookie (1)**
            - ▶ POST http://localhost:8090/login

Appendix

Alert types

This section contains additional information on the types of alerts in the report.

1. **Path Traversal**

Source	raised by an active scanner (Path Traversal)
CWE ID	22
WASC ID	33
Reference	1. https://owasp.org/www-community/attacks/Path_Traversal 2. https://cwe.mitre.org/data/definitions/22.html

2. **Content Security Policy (CSP) Header Not Set**

Source	raised by a passive scanner (Content Security Policy (CSP) Header Not Set)
CWE ID	693
WASC ID	15
Reference	1. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy 2. https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html 3. https://www.w3.org/TR/CSP/ 4. https://w3c.github.io/webappsec-csp/ 5. https://web.dev/articles/csp 6. https://caniuse.com/#feat=contentsecuritypolicy 7. https://content-security-policy.com/

3. **Cross-Domain Misconfiguration**

Source	raised by a passive scanner (Cross-Domain Misconfiguration)
CWE ID	264
WASC ID	14
Reference	1. https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

4. **Format String Error**

Source	raised by an active scanner (Format String Error)
CWE ID	134
WASC ID	6
Reference	1. https://owasp.org/www-community/attacks/Format_string_attack

5. **Missing Anti-clickjacking Header**

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	1. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

6. **Session ID in URL Rewrite**

Source	raised by a passive scanner (Session ID in URL Rewrite)
CWE ID	200
WASC ID	13
Reference	1. https://seclists.org/webappsec/2002/q4/111

7. **XSLT Injection**

Source	raised by an active scanner (XSLT Injection)
CWE ID	91
WASC ID	23
Reference	1. https://www.contextis.com/blog/xslt-server-side-injection-attacks

8. **Application Error Disclosure**

Source	raised by a passive scanner (Application Error Disclosure)
CWE ID	200
WASC ID	13

9. **Cookie without SameSite Attribute**

Source	raised by a passive scanner (Cookie without SameSite Attribute)
CWE ID	1275
WASC ID	13
Reference	1. https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

10. **Cross-Domain JavaScript Source File Inclusion**

Source	raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID	829
WASC ID	15

11. **Referer Exposes Session ID**

Source	raised by a passive scanner (Session ID in URL Rewrite)
CWE ID	200
WASC ID	13
Reference	1. https://seclists.org/webappsec/2002/q4/111

12. **Strict-Transport-Security Header Not Set**

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15
Reference	1. https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html 2. https://owasp.org/www-community/Security_Headers 3. https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security 4. https://caniuse.com/stricttransportsecurity 5. https://datatracker.ietf.org/doc/html/rfc6797

13. **Timestamp Disclosure - Unix**

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	200
WASC ID	13
Reference	1. https://cwe.mitre.org/data/definitions/200.html

14. **X-Content-Type-Options Header Missing**

Source	raised by a passive scanner (X-Content-Type-Options Header Missing)
CWE ID	693
WASC ID	15
Reference	1. https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) 2. https://owasp.org/www-community/Security_Headers

15. **Authentication Request Identified**

Source	raised by a passive scanner (Authentication Request Identified)
Reference	1. https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/

16. **Information Disclosure - Sensitive Information in URL**

Source	raised by a passive scanner (Information Disclosure - Sensitive Information in URL)
CWE ID	200
WASC ID	13

17. **Information Disclosure - Suspicious Comments**

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	200
WASC ID	13

18. **Loosely Scoped Cookie**

Source	raised by a passive scanner (Loosely Scoped Cookie)
CWE ID	565
WASC ID	15
Reference	1. https://tools.ietf.org/html/rfc6265#section-4.1 2. https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html 3. https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies

19. **Modern Web Application**

Source	raised by a passive scanner (Modern Web Application)

20. **Retrieved from Cache**

Source	raised by a passive scanner (Retrieved from Cache)
Reference	1. https://tools.ietf.org/html/rfc7234 2. https://tools.ietf.org/html/rfc7231 3. https://www.rfc-editor.org/rfc/rfc9110.html

21. **Session Management Response Identified**

Source	raised by a passive scanner (Session Management Response Identified)
Reference	1. https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id