ZAP Scanning Report

Generated with ZAP on Tue 12 Apr 2022, at 11:49:17

Contents

About this report

Report parameters

Contexts

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

Sites

The following sites were included:

- http://monitoring.thomsen-it.dk:9090
- https://www.thomsen-it.dk
- https://grafana.thomsen-it.dk

(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, False Positive

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 (8.3%)	1 (8.3%)	2 (16.7%)
	Medium	0 (0.0%)	1 (8.3%)	1 (8.3%)	1 (8.3%)	3 (25.0%)
	Low	0 (0.0%)	0 (0.0%)	3 (25.0%)	1 (8.3%)	4 (33.3%)
	Informational	0 (0.0%)	0 (0.0%)	1 (8.3%)	2 (16.7%)	3 (25.0%)

	Confidence				
	User Confirmed	High	Medium	Low	Total
Total	0 (0.0%)	1 (8.3%)	6 (50.0%)	5 (41.7%)	12 (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.thomsen-it.dk	2 (2)	1 (3)	1 (4)	1 (5)
	https://grafana.thomsen-it.dk	0 (0)	2 (2)	3 (5)	2 (7)

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 (8.3%)
SQL Injection	High	1 (8.3%)
Absence of Anti-CSRF Tokens	Medium	8 (66.7%)
Content Security Policy (CSP) Header Not Set	Medium	39 (325.0%)
Missing Anti-clickjacking Header	Medium	37 (308.3%)
Total		12

Alert type	Risk	Count
Cookie Without Secure Flag	Low	4 (33.3%)
Cookie without SameSite Attribute	Low	1 (8.3%)
Timestamp Disclosure - Unix	Low	701 (5,841.7%)
X-Content-Type-Options Header Missing	Low	57 (475.0%)
Information Disclosure - Suspicious Comments	Informational	51 (425.0%)
Loosely Scoped Cookie	Informational	1 (8.3%)
Re-examine Cache-control Directives	Informational	38 (316.7%)
Total		12

Alerts

Risk=High, Confidence=Medium (1)

https://www.thomsen-it.dk (1)

SQL Injection (1)

▶ POST https://www.thomsen-it.dk/register

Risk=High, Confidence=Low (1)

https://www.thomsen-it.dk (1)

Path Traversal (1)

▶ POST https://www.thomsen-it.dk/register

Risk=Medium, Confidence=High (1)

https://grafana.thomsen-it.dk (1)

Content Security Policy (CSP) Header Not Set (1)

▶ GET https://grafana.thomsen-it.dk/

Risk=Medium, Confidence=Medium (1)

https://www.thomsen-it.dk (1)

Missing Anti-clickjacking Header (1)

▶ GET https://www.thomsen-it.dk/

Risk=Medium, Confidence=Low (1)

https://grafana.thomsen-it.dk (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://grafana.thomsen-it.dk/public/build/app.b86cc30c452b708f8c31.js

Risk=Low, Confidence=Medium (3)

https://www.thomsen-it.dk (1)

Cookie without SameSite Attribute (1)

▶ POST https://www.thomsen-it.dk/login

https://grafana.thomsen-it.dk (2)

Cookie Without Secure Flag (1)

▶ GET https://grafana.thomsen-it.dk

X-Content-Type-Options Header Missing (1)

▶ GET https://grafana.thomsen-it.dk/robots.txt

Risk=Low, Confidence=Low (1)

https://grafana.thomsen-it.dk (1)

Timestamp Disclosure - Unix (1)

▶ GET https://grafana.thomsen-it.dk/

Risk=Informational, Confidence=Medium (1)

https://grafana.thomsen-it.dk (1)

Re-examine Cache-control Directives (1)

▶ GET https://grafana.thomsen-it.dk/

Risk=Informational, Confidence=Low (2)

https://www.thomsen-it.dk (1)

Loosely Scoped Cookie (1)

▶ POST https://www.thomsen-it.dk/login

https://grafana.thomsen-it.dk (1)

Information Disclosure - Suspicious Comments (1)

▶ GET https://grafana.thomsen-it.dk/

Appendix

Alert types

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

Path Traversal

Source	raised by an active scanner (Path Traversal)
CWE ID	22
WASC ID	33
Reference	▪ http://projects.webappsec.org/Path-Traversal ▪ http://cwe.mitre.org/data/definitions/22.html

SQL Injection

Source	raised by an active scanner (SQL Injection)
CWE ID	89

WASC ID	19
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Absence of Anti-CSRF Tokens

Source	raised by a passive scanner (Absence of Anti-CSRF Tokens)
CWE ID	352
WASC ID	9
Reference	▪ http://projects.webappsec.org/Cross-Site-Request-Forgery ▪ http://cwe.mitre.org/data/definitions/352.html

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	▪ https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy ▪ https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html ▪ http://www.w3.org/TR/CSP/ ▪ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html ▪ http://www.html5rocks.com/en/tutorials/security/content-security-policy/ ▪ http://caniuse.com/#feat=contentsecuritypolicy ▪ http://content-security-policy.com/

Missing Anti-clickjacking Header

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15

Reference	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Cookie Without Secure Flag

Source	raised by a passive scanner (Cookie Without Secure Flag)
CWE ID	614
WASC ID	13
Reference	▪ 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

Cookie without SameSite Attribute

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

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	200
WASC ID	13
Reference	▪ http://projects.webappsec.org/w/page/13246936/Information%20Leakage

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	▪ http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx ▪ https://owasp.org/www-community/Security_Headers

Information Disclosure - Suspicious Comments

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

Loosely Scoped Cookie

Source	raised by a passive scanner (Loosely Scoped Cookie)
CWE ID	565
WASC ID	15
Reference	▪ https://tools.ietf.org/html/rfc6265#section-4.1 ▪ 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 ▪ http://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies

Re-examine Cache-control Directives

Source	raised by a passive scanner (Re-examine Cache-control Directives)
CWE ID	525
WASC ID	13
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching ▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control