ZAP Scanning Report for ATSLITE

Generated with ZAP on Sun 6 Nov 2022, at 22:22:55

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://ocsp.digicert.com`
- `https://apis.google.com`
- `https://fonts.gstatic.com`
- `https://placegenix.com:5051`
- `https://www.clarity.ms`
- `https://dfrnc.com`
- `https://fonts.googleapis.com`
- `https://unpkg.com`
- `http://ciscobinary.openh264.org`
- `https://cdnjs.cloudflare.com`
- `https://atslite.staffgenix.com`
- `http://r3.o.lencr.org`

(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%)	1 (6.7%)	0 (0.0%)	0 (0.0%)	1 (6.7%)
	Medium	0 (0.0%)	1 (6.7%)	2 (13.3%)	0 (0.0%)	3 (20.0%)
	Low	0 (0.0%)	2 (13.3%)	4 (26.7%)	1 (6.7%)	7 (46.7%)
	Informational	0 (0.0%)	0 (0.0%)	2 (13.3%)	2 (13.3%)	4 (26.7%)

	Confidence				
	User Confirmed	High	Medium	Low	Total
Total	0 (0.0%)	4 (26.7%)	8 (53.3%)	3 (20.0%)	15 (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	http://ocsp.digicert.com	0 (0)	0 (0)	1 (1)	0 (1)
	https://www.clarity.ms	0 (0)	0 (0)	1 (1)	0 (1)
	https://dfrnc.com	0 (0)	0 (0)	1 (1)	0 (1)
	http://ciscobinary.openh264.org	0 (0)	0 (0)	1 (1)	0 (1)
	https://cdnjs.cloudflare.com	0 (0)	1 (1)	0 (1)	0 (1)

	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
https://atslite.staffgenix.com	1 (1)	2 (3)	3 (6)	4 (10)

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
PII Disclosure	High	4 (26.7%)
Content Security Policy (CSP) Header Not Set	Medium	3 (20.0%)
Cross-Domain Misconfiguration	Medium	10 (66.7%)
Missing Anti-clickjacking Header	Medium	2 (13.3%)
Cookie with SameSite Attribute None	Low	1 (6.7%)
Cross-Domain JavaScript Source File Inclusion	Low	10
Total		15

Alert type	Risk	Count
		(66.7%)
Private IP Disclosure	Low	1 (6.7%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	1 (6.7%)
Strict-Transport-Security Header Not Set	Low	8 (53.3%)
Timestamp Disclosure - Unix	Low	68 (453.3%)
X-Content-Type-Options Header Missing	Low	13 (86.7%)
Information Disclosure - Suspicious Comments	Informational	14 (93.3%)
Modern Web Application	Informational	3 (20.0%)
Re-examine Cache-control Directives	Informational	2 (13.3%)
Retrieved from Cache	Informational	12 (80.0%)
Total		15

Alerts

Risk=High, Confidence=High (1)

`https://atslite.staffgenix.com` (1)

PII Disclosure (1)

▶ GET https://atslite.staffgenix.com/main.ecaf69303ae895f8ed05.chunk.js

Risk=`Medium`, Confidence=`High` (1)

`https://atslite.staffgenix.com` (1)

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

▶ GET https://atslite.staffgenix.com/

Risk=`Medium`, Confidence=`Medium` (2)

`https://cdnjs.cloudflare.com` (1)

Cross-Domain Misconfiguration (1)

▶ GET https://cdnjs.cloudflare.com/ajax/libs/gsap/3.5.1/TimelineMax.min.js

`https://atslite.staffgenix.com` (1)

Missing Anti-clickjacking Header (1)

▶ GET https://atslite.staffgenix.com/

Risk=Low, Confidence=High (2)

http://ocsp.digicert.com (1)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

▶ GET http://ocsp.digicert.com/

https://dfrnc.com (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://dfrnc.com/lib/morph3.min.js

Risk=Low, Confidence=Medium (4)

https://www.clarity.ms (1)

Cookie with SameSite Attribute None (1)

▶ GET https://www.clarity.ms/tag/dvseml8izf

https://atslite.staffgenix.com (3)

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://atslite.staffgenix.com/

Private IP Disclosure (1)

▶ GET
https://atslite.staffgenix.com/vendor.82f3683872afb11ad6d5.chunk.

js

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

▶ GET https://atslite.staffgenix.com/

Risk=Low, Confidence=Low (1)

http://ciscobinary.openh264.org (1)

Timestamp Disclosure - Unix (1)

▶ GET http://ciscobinary.openh264.org/openh264-win64-2e1774ab6dc6c43debb0b5b628bdf122a391d521.zip

Risk=Informational, Confidence=Medium (2)

https://atslite.staffgenix.com (2)

Modern Web Application (1)

▶ GET https://atslite.staffgenix.com/

Retrieved from Cache (1)

▶ GET https://atslite.staffgenix.com/

Risk=Informational, Confidence=Low (2)

https://atslite.staffgenix.com (2)

Information Disclosure - Suspicious Comments (1)

▶ GET https://atslite.staffgenix.com/

Re-examine Cache-control Directives (1)

▶ GET https://atslite.staffgenix.com/

Appendix

Alert types

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

PII Disclosure

Source	raised by a passive scanner (PII Disclosure)
CWE ID	359
WASC ID	13

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/

Cross-Domain Misconfiguration

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

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 with SameSite Attribute None

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

Cross-Domain JavaScript Source File Inclusion

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

Private IP Disclosure

Source	raised by a passive scanner (Private IP Disclosure)
CWE ID	200
WASC ID	13
Reference	▪ https://tools.ietf.org/html/rfc1918

Server Leaks Version Information via "Server" HTTP Response Header Field

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	200
WASC ID	13
Reference	▪ http://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 ▪ http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx ▪ http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Strict-Transport-Security Header Not Set

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

- https://owasp.org/www-community/Security_Headers
- http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
- http://caniuse.com/stricttransportsecurity
- http://tools.ietf.org/html/rfc6797

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

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)

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 ▪ https://grayduck.mn/2021/09/13/cache-control-recommendations/

Retrieved from Cache

Source	raised by a passive scanner (Retrieved from Cache)
Reference	▪ https://tools.ietf.org/html/rfc7234 ▪ https://tools.ietf.org/html/rfc7231 ▪ http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)