ZAP Scanning Report

Generated with ZAP on 10 Apr 2023, at 13:49:53

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://beacons.gcp.gvt2.com
- https://update.googleapis.com
- https://optimizationguide-pa.googleapis.com
- https://content-autofill.googleapis.com
- https://cdn.jsdelivr.net
- https://fonts.googleapis.com
- http://192.168.1.119:3000
- https://accounts.google.com

(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%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (6.7%)	2 (13.3%)	1 (6.7%)	4 (26.7%)
	Low	0 (0.0%)	1 (6.7%)	2 (13.3%)	1 (6.7%)	4 (26.7%)
	Informational	0 (0.0%)	0 (0.0%)	4 (26.7%)	3 (20.0%)	7 (46.7%)
	Total	0 (0.0%)	2 (13.3%)	8 (53.3%)	5 (33.3%)	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	https://optimizationguide-pa.googleapis.com	0 (0)	1 (1)	1 (2)	0 (2)
	https://content-autofill.googleapis.com	0 (0)	0 (0)	1 (1)	1 (2)
	https://cdn.jsdelivr.net	0 (0)	0 (0)	0 (0)	1 (1)
	https://fonts.googleapis.com	0 (0)	1 (1)	0 (1)	0 (1)
	http://192.168.1.119:3000	0 (0)	2 (2)	2 (4)	5 (9)

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
Absence of Anti-CSRF Tokens	Medium	19 (126.7%)
Content Security Policy (CSP) Header Not Set	Medium	30 (200.0%)
Cross-Domain Misconfiguration	Medium	2
Total		15

Alert type	Risk	Count
Missing Anti-clickjacking Header	Medium	4 (26.7%)
Application Error Disclosure	Low	2 (13.3%)
Strict-Transport-Security Header Not Set	Low	13 (86.7%)
Timestamp Disclosure - Unix	Low	3 (20.0%)
X-Content-Type-Options Header Missing	Low	16 (106.7%)
Information Disclosure - Sensitive Information in URL	Informational	1 (6.7%)
Information Disclosure - Suspicious Comments	Informational	15 (100.0%)
Modern Web Application	Informational	8 (53.3%)
Re-examine Cache-control Directives	Informational	7 (46.7%)
Retrieved from Cache	Informational	1 (6.7%)
User Agent Fuzzer	Informational	48 (320.0%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	10 (66.7%)
Total		15

Alerts

Risk=Medium, Confidence=High (1)

http://192.168.1.119:3000 (1)

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

▶ GET http://192.168.1.119:3000/

Risk=Medium, Confidence=Medium (2)

https://optimizationguide-pa.googleapis.com (1)

Missing Anti-clickjacking Header (1)

▶ GET https://optimizationguide-pa.googleapis.com/downloads?name=1679922153&target=OPTIMIZATION_TARGET_NOTIFICATION_PERMISSION_PREDICTIONS

https://fonts.googleapis.com (1)

Cross-Domain Misconfiguration (1)

▶ GET https://fonts.googleapis.com/css?family=Inter:300italic,400italic,600italic,700italic,800italic,400,300,600,700,800&display=swap

Risk=Medium, Confidence=Low (1)

http://192.168.1.119:3000 (1)

Absence of Anti-CSRF Tokens (1)

▶ GET http://192.168.1.119:3000/

Risk=Low, Confidence=High (1)

https://content-autofill.googleapis.com (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTExLjAuNTU2My4xNDcSFwlunE71hp83uBIFDTQ30ysSBQ3c5Mos?alt=proto

Risk=Low, Confidence=Medium (2)

http://192.168.1.119:3000 (2)

Application Error Disclosure (1)

▶ GET http://192.168.1.119:3000/search?q%5Bs%5D=user_name+asc

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

▶ GET http://192.168.1.119:3000/assets/es-module-shims.min-d89e73202ec09dede55fb74115af9c5f9f2bb965433de1c2446e1faa6dac2470.js

Risk=Low, Confidence=Low (1)

https://optimizationguide-pa.googleapis.com (1)

Timestamp Disclosure - Unix (1)

▶ POST https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw

Risk=Informational, Confidence=Medium (4)

https://cdn.jsdelivr.net (1)

Retrieved from Cache (1)

▶ GET https://cdn.jsdelivr.net/npm/bootstrap@5.0.2/dist/css/bootstrap.min.css

http://192.168.1.119:3000 (3)

Information Disclosure - Sensitive Information in URL (1)

▶ GET http://192.168.1.119:3000/?email=foo-bar%40example.com

Modern Web Application (1)

▶ GET http://192.168.1.119:3000/sitemap.xml

User Agent Fuzzer (1)

▶ GET http://192.168.1.119:3000/

Risk=Informational, Confidence=Low (3)

https://content-autofill.googleapis.com (1)

Re-examine Cache-control Directives (1)

▶ GET https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTExLjAuNTU2My4xNDcSFwlunE71hp83uBIFDTQ30ysSBQ3c5Mos?alt=proto

http://192.168.1.119:3000 (2)

Information Disclosure - Suspicious Comments (1)

▶ GET http://192.168.1.119:3000/assets/es-module-shims.min-d89e73202ec09dede55fb74115af9c5f9f2bb965433de1c2446e1faa6dac2470.js

User Controllable HTML Element Attribute (Potential XSS) (1)

▶ GET http://192.168.1.119:3000/search?commit=Search%21&q%5Btitle_or_context_cont%5D

Appendix

Alert types

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

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/

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

Application Error Disclosure

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

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 - Sensitive Information in URL

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

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)

User Agent Fuzzer

Source raised by an active scanner (User Agent Fuzzer)

Reference
- https://owasp.org/wstg

User Controllable HTML Element Attribute (Potential XSS)

Source raised by a passive scanner (User Controllable HTML Element Attribute (Potential XSS))

CWE ID 20

WASC ID 20

Reference
- http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute