ZAP by Checkmarx Scanning Report

Generated with ZAP on Fri 18 Jul 2025, at 07:42:08

ZAP Version: 2.16.1

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://tracking-protection.cdn.mozilla.net`
- `https://google-gruyere.appspot.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%)	1 (5.3%)	1 (5.3%)	0 (0.0%)	2 (10.5%)
	Medium	0 (0.0%)	1 (5.3%)	1 (5.3%)	0 (0.0%)	2 (10.5%)
	Low	0 (0.0%)	2 (10.5%)	4 (21.1%)	1 (5.3%)	7 (36.8%)
	Informational	0 (0.0%)	0 (0.0%)	4 (21.1%)	4 (21.1%)	8 (42.1%)
	Total	0 (0.0%)	4 (21.1%)	10 (52.6%)	5 (26.3%)	19 (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://tracking-protection.cdn.mozilla.net	0 (0)	0 (0)	2 (2)	0 (2)
	https://google-gruyere.appspot.com	2 (2)	2 (4)	5 (9)	8 (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
Cross Site Scripting (DOM Based)	High	3 (15.8%)
Cross Site Scripting (Reflected)	High	2 (10.5%)
Content Security Policy (CSP) Header Not Set	Medium	67 (352.6%)
Total		19

Alert type	Risk	Count
Missing Anti-clickjacking Header	Medium	66 (347.4%)
Cookie No HttpOnly Flag	Low	5 (26.3%)
Cookie Without Secure Flag	Low	5 (26.3%)
Cookie without SameSite Attribute	Low	5 (26.3%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	1 (5.3%)
Strict-Transport-Security Header Not Set	Low	101 (531.6%)
Timestamp Disclosure - Unix	Low	1 (5.3%)
X-Content-Type-Options Header Missing	Low	82 (431.6%)
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	6 (31.6%)
Cookie Poisoning	Informational	7 (36.8%)
Information Disclosure - Suspicious Comments	Informational	2 (10.5%)
Modern Web Application	Informational	13 (68.4%)
Re-examine Cache-control Directives	Informational	67 (352.6%)
Total		19

Alert type	Risk	Count
Retrieved from Cache	Informational	16 (84.2%)
Session Management Response Identified	Informational	5 (26.3%)
User Agent Fuzzer	Informational	48 (252.6%)
Total		19

Alerts

Risk=High, Confidence=High (1)

https://google-gruyere.appspot.com (1)

Cross Site Scripting (DOM Based) (1)

▶ GET https://google-gruyere.appspot.com/526725182993338172609076211357288313081/feed.gtl?uid=%3Cscript%3Ealert(5397)%3C/script%3E

Risk=High, Confidence=Medium (1)

https://google-gruyere.appspot.com (1)

Cross Site Scripting (Reflected) (1)

▶ GET https://google-gruyere.appspot.com/526725182993338172609076211357288313081/feed.gtl?uid=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E

Risk=Medium, Confidence=High (1)

https://google-gruyere.appspot.com (1)

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

▶ GET https://google-gruyere.appspot.com/526725182993338172609076211357288313081/

Risk=Medium, Confidence=Medium (1)

https://google-gruyere.appspot.com (1)

Missing Anti-clickjacking Header (1)

▶ GET https://google-gruyere.appspot.com/526725182993338172609076211357288313081/

Risk=Low, Confidence=High (2)

https://tracking-protection.cdn.mozilla.net (1)

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

▶ GET https://tracking-protection.cdn.mozilla.net/ads-track-digest256/128.0/1732308867

https://google-gruyere.appspot.com (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://google-gruyere.appspot.com/526725182993338172609076211357288313081/

Risk=Low, Confidence=Medium (4)

https://google-gruyere.appspot.com (4)

Cookie No HttpOnly Flag (1)

▶ GET https://google-gruyere.appspot.com/start

Cookie Without Secure Flag (1)

▶ GET https://google-gruyere.appspot.com/start

Cookie without SameSite Attribute (1)

▶ GET https://google-gruyere.appspot.com/start

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

▶ GET https://google-gruyere.appspot.com/526725182993338172609076211357288313081/

Risk=Low, Confidence=Low (1)

https://tracking-protection.cdn.mozilla.net (1)

Timestamp Disclosure - Unix (1)

▶ GET https://tracking-protection.cdn.mozilla.net/ads-track-digest256/128.0/1732308867

Risk=Informational, Confidence=Medium (4)

https://google-gruyere.appspot.com (4)

Modern Web Application (1)

▶ GET https://google-gruyere.appspot.com/526725182993338172609076211357288313081/

Retrieved from Cache (1)

▶ GET https://google-gruyere.appspot.com/robots.txt

Session Management Response Identified (1)

▶ GET https://google-gruyere.appspot.com/start

User Agent Fuzzer (1)

▶ GET https://google-gruyere.appspot.com/526725182993338172609076211357288313081/

Risk=Informational, Confidence=Low (4)

https://google-gruyere.appspot.com (4)

Charset Mismatch (Header Versus Meta Content-Type Charset) (1)

▶ GET https://google-gruyere.appspot.com/

Cookie Poisoning (1)

▶ GET https://google-gruyere.appspot.com/526725182993338172609076211357288313081/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP

Information Disclosure - Suspicious Comments (1)

▶ GET https://google-gruyere.appspot.com/526725182993338172609076211357288313081/lib.js

Re-examine Cache-control Directives (1)

```
▶ GET https://google-gruyere.appspot.com/526725182993338172609076211357288313081/
```

Appendix

Alert Types

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

Cross Site Scripting (DOM Based)

Source	raised by an active scanner (Cross Site Scripting (DOM Based))
CWE ID	79
WASC ID	8
Reference	▪ https://owasp.org/www-community/attacks/xss/ ▪ https://cwe.mitre.org/data/definitions/79.html

Cross Site Scripting (Reflected)

Source	raised by an active scanner (Cross Site Scripting (Reflected))
CWE ID	79
WASC ID	8
Reference	▪ https://owasp.org/www-community/attacks/xss/

- https://cwe.mitre.org/data/definitions/79.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 ▪ https://www.w3.org/TR/CSP/ ▪ https://w3c.github.io/webappsec-csp/ ▪ https://web.dev/articles/csp ▪ https://caniuse.com/#feat=contentsecuritypolicy ▪ https://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 No HttpOnly Flag

Source	raised by a passive scanner (Cookie No HttpOnly Flag)
CWE ID	1004
WASC ID	13
Reference	- https://owasp.org/www-community/HttpOnly

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

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

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	497
WASC ID	13
Reference	- https://httpd.apache.org/docs/current/mod/core.html#servertokens - https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) - https://www.troyhunt.com/shhh-dont-let-your-response-headers/

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

- https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
- https://caniuse.com/stricttransportsecurity
- https://datatracker.ietf.org/doc/html/rfc6797

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	497
WASC ID	13
Reference	https://cwe.mitre.org/data/definitions/200.html

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	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers

Charset Mismatch (Header Versus Meta Content-Type Charset)

Source	raised by a passive scanner (Charset Mismatch)
CWE ID	436
WASC ID	15
Reference	- https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection

Cookie Poisoning

Source	raised by a passive scanner (Cookie Poisoning)
CWE ID	565
WASC ID	20
Reference	- https://en.wikipedia.org/wiki/HTTP_cookie - https://cwe.mitre.org/data/definitions/565.html

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	615
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 - https://www.rfc-editor.org/rfc/rfc9110.html

Session Management Response Identified

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

User Agent Fuzzer

Source	raised by an active scanner ([User Agent Fuzzer](https://www.zaproxy.org/docs/alerts/10104/))
Reference	- https://owasp.org/wstg