ZAP by Checkmarx Scanning Report

Generated with ZAP on Sun 22 Dec 2024, at 13:20:35

ZAP Version: 2.15.0

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:

- `http://localhost:3000`

(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

		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%)	3 (60.0%)	0 (0.0%)	0 (0.0%)	3 (60.0%)
	Low	0 (0.0%)	1 (20.0%)	0 (0.0%)	0 (0.0%)	1 (20.0%)
	Informational	0 (0.0%)	1 (20.0%)	0 (0.0%)	0 (0.0%)	1 (20.0%)
	Total	0 (0.0%)	5 (100.0%)	0 (0.0%)	0 (0.0%)	5 (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://localhost:3000	0 (0)	3 (3)	1 (4)	1 (5)

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
CSP: Wildcard Directive	Medium	15 (300.0%)
CSP: style-src unsafe-inline	Medium	6 (120.0%)
Hidden File Found	Medium	1 (20.0%)
CSP: Notices	Low	6 (120.0%)
Authentication Request Identified	Informational	1 (20.0%)
Total		5

Alerts

Risk=Medium, Confidence=High (3)

http://localhost:3000 (3)

CSP: Wildcard Directive (1)

▼ GET http://localhost:3000/

Alert tags
- CWE-693
- OWASP_2021_A05
- OWASP_2017_A06

Alert description
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data

injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Other info

The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined:

style-src, font-src

Request

▼ Request line and header section (198 bytes)

```
GET http://localhost:3000/ HTTP/1.1
host: localhost:3000
user-agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64; rv:125.0) Gecko/20100101
Firefox/125.0
pragma: no-cache
cache-control: no-cache
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (957 bytes)

```
HTTP/1.1 200 OK
Content-Security-Policy: default-src
'self';base-uri 'self';font-src 'self'
https: data:;form-action 'self';frame-
ancestors 'self';img-src 'self' data:;object-
src 'none';script-src 'self';script-src-attr
'none';style-src 'self' https: 'unsafe-
inline';upgrade-insecure-requests
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Origin-Agent-Cluster: ?1
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000;
includeSubDomains
X-Content-Type-Options: nosniff
```

```
X-DNS-Prefetch-Control: off
X-Download-Options: noopen
X-Frame-Options: SAMEORIGIN
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 0
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Sun, 22 Dec 2024 03:01:42 GMT
ETag: W/"aff-193ec503eb9"
Content-Type: text/html; charset=UTF-8
Content-Length: 2815
Date: Sun, 22 Dec 2024 13:09:36 GMT
Connection: keep-alive
Keep-Alive: timeout=5
```

▶ Response body (2815 bytes)

Parameter Content-Security-Policy

Evidence `default-src 'self';base-uri 'self';font-src 'self' https: data:;form-action 'self';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests`

Solution Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.

CSP: style-src unsafe-inline (1)

▶ GET http://localhost:3000/

Hidden File Found (1)

▼ GET http://localhost:3000/.git/config

Alert tags

- OWASP_2021_A05
- OWASP_2017_A06
- CWE-538
- WSTG-v42-CONF-05

Alert description

A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

Other info

git_dir

Request

▼ Request line and header section (209 bytes)

```
GET http://localhost:3000/.git/config HTTP/1.1
host: localhost:3000
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:125.0) Gecko/20100101 Firefox/125.0
pragma: no-cache
cache-control: no-cache
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (956 bytes)

```
HTTP/1.1 200 OK
Content-Security-Policy: default-src 'self';base-uri
'self';font-src 'self' https: data:;form-action
'self';frame-ancestors 'self';img-src 'self'
data:;object-src 'none';script-src 'self';script-src-
attr 'none';style-src 'self' https: 'unsafe-
inline';upgrade-insecure-requests
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Origin-Agent-Cluster: ?1
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000;
includeSubDomains
X-Content-Type-Options: nosniff
X-DNS-Prefetch-Control: off
X-Download-Options: noopen
X-Frame-Options: SAMEORIGIN
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 0
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Sat, 21 Dec 2024 22:35:31 GMT
ETag: W/"264-193eb5c8cab"
Content-Type: application/octet-stream
Content-Length: 612
```

```
Date: Sun, 22 Dec 2024 13:09:42 GMT
Connection: keep-alive
Keep-Alive: timeout=5
```

▼ Response body (612 bytes)

```
[core]
        repositoryformatversion = 0
        filemode = false
        bare = false
        logallrefupdates = true
        symlinks = false
        ignorecase = true
[submodule]
        active = .
[remote "origin"]
        url = https://github.com/YOUSSIFBB/SAP-CA2.git
        fetch = +refs/heads/*:refs/remotes/origin/*
[branch "main"]
        remote = origin
        merge = refs/heads/main
[lfs]
        repositoryformatversion = 0
[branch "Vulnerable-App"]
        remote = origin
        merge = refs/heads/Vulnerable-App
        vscode-merge-base = origin/Vulnerable-App
[branch "Secure-App-Version"]
        remote = origin
        merge = refs/heads/Secure-App-Version
        vscode-merge-base = origin/Secure-App-Version
```

Evidence `HTTP/1.1 200 OK`

Solution Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.

Risk=Low, Confidence=High (1)

http://localhost:3000 (1)

CSP: Notices (1)

▶ GET http://localhost:3000/

Risk=Informational, Confidence=High (1)

http://localhost:3000 (1)

Authentication Request Identified (1)

▶ POST http://localhost:3000/api/login

Appendix

Alert types

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

CSP: Wildcard Directive

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CSP: style-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

Hidden File Found

Source	raised by an active scanner (Hidden File Finder)
CWE ID	538
WASC ID	13
Reference	▪ https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html ▪ https://git-scm.com/docs/git-config

CSP: Notices

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/

- https://caniuse.com/#search=content+security+policy
- https://content-security-policy.com/
- https://github.com/HtmlUnit/htmlunit-csp
- https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

Authentication Request Identified

Source raised by a passive scanner (Authentication Request Identified)

Reference

- https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/