ZAP Scanning Report

Generated with The ZAP logoZAP on Sat 20 Jul 2024, at 18:16:06

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

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://ginandjuice.shop
- http://ginandjuice.shop

(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%)	1 (5.6%)	1 (5.6%)
	Medium	0 (0.0%)	1 (5.6%)	1 (5.6%)	2 (11.1%)	4 (22.2%)
	Low	0 (0.0%)	2 (11.1%)	5 (27.8%)	0 (0.0%)	7 (38.9%)
	Informational	0 (0.0%)	0 (0.0%)	3 (16.7%)	3 (16.7%)	6 (33.3%)
	Total	0 (0.0%)	3 (16.7%)	9 (50.0%)	6 (33.3%)	18 (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://ginandjuice.shop	0 (0)	2 (2)	2 (4)	3 (7)
	http://ginandjuice.shop	1 (1)	2 (3)	5 (8)	3 (11)

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
Cloud Metadata Potentially Exposed	High	1 (5.6%)
Absence of Anti-CSRF Tokens	Medium	40 (222.2%)
Content Security Policy (CSP) Header Not Set	Medium	43 (238.9%)
Hidden File Found	Medium	4 (22.2%)
Vulnerable JS Library	Medium	1 (5.6%)
Cookie No HttpOnly Flag	Low	190 (1,055.6%)
Cookie Without Secure Flag	Low	94 (522.2%)
Cookie with SameSite Attribute None	Low	102 (566.7%)
Cookie without SameSite Attribute	Low	96 (533.3%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	10 (55.6%)
Strict-Transport-Security Header Not Set	Low	92 (511.1%)
X-Content-Type-Options Header Missing	Low	81 (450.0%)
Information Disclosure - Suspicious Comments	Informational	27 (150.0%)
Modern Web Application	Informational	43 (238.9%)
Re-examine Cache-control Directives	Informational	32 (177.8%)
Session Management Response Identified	Informational	296 (1,644.4%)
User Agent Fuzzer	Informational	60 (333.3%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	16 (88.9%)
Total		18

Alerts

1. **Risk=High, Confidence=Low (1)**
   1. **http://ginandjuice.shop (1)**
      1. Cloud Metadata Potentially Exposed (1)
         1. ▶ GET http://ginandjuice.shop/latest/meta-data/
2. **Risk=Medium, Confidence=High (1)**
   1. **http://ginandjuice.shop (1)**
      1. Content Security Policy (CSP) Header Not Set (1)
         1. ▶ GET http://ginandjuice.shop
3. **Risk=Medium, Confidence=Medium (1)**
   1. **https://ginandjuice.shop (1)**
      1. Vulnerable JS Library (1)
         1. ▶ GET https://ginandjuice.shop/resources/js/angular_1-7-7.js
4. **Risk=Medium, Confidence=Low (2)**
   1. **https://ginandjuice.shop (1)**
      1. Absence of Anti-CSRF Tokens (1)
         1. ▶ GET https://ginandjuice.shop/blog
   2. **http://ginandjuice.shop (1)**
      1. Hidden File Found (1)
         1. ▶ GET http://ginandjuice.shop/.hg
5. **Risk=Low, Confidence=High (2)**
   1. **https://ginandjuice.shop (1)**
      1. Strict-Transport-Security Header Not Set (1)
         1. ▶ GET https://ginandjuice.shop/sitemap.xml
   2. **http://ginandjuice.shop (1)**
      1. Server Leaks Version Information via "Server" HTTP Response Header Field (1)
         1. ▶ GET http://ginandjuice.shop/sitemap.xml
6. **Risk=Low, Confidence=Medium (5)**
   1. **https://ginandjuice.shop (1)**
      1. Cookie Without Secure Flag (1)
         1. ▶ GET https://ginandjuice.shop/robots.txt
   2. **http://ginandjuice.shop (4)**
      1. Cookie No HttpOnly Flag (1)
         1. ▶ GET http://ginandjuice.shop
      2. Cookie with SameSite Attribute None (1)
         1. ▶ GET http://ginandjuice.shop
      3. Cookie without SameSite Attribute (1)
         1. ▶ GET http://ginandjuice.shop
      4. X-Content-Type-Options Header Missing (1)
         1. ▶ GET http://ginandjuice.shop
7. **Risk=Informational, Confidence=Medium (3)**
   1. **http://ginandjuice.shop (3)**
      1. Modern Web Application (1)
         1. ▶ GET http://ginandjuice.shop
      2. Session Management Response Identified (1)
         1. ▶ GET http://ginandjuice.shop
      3. User Agent Fuzzer (1)
         1. ▶ GET http://ginandjuice.shop
8. **Risk=Informational, Confidence=Low (3)**
   1. **https://ginandjuice.shop (3)**
      1. Information Disclosure - Suspicious Comments (1)
         1. ▶ GET https://ginandjuice.shop/resources/images/not-found.svg
      2. Re-examine Cache-control Directives (1)
         1. ▶ GET https://ginandjuice.shop/about
      3. User Controllable HTML Element Attribute (Potential XSS) (1)
         1. ▶ GET https://ginandjuice.shop/catalog/product?productId=10

Appendix

Alert types

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

1. **Cloud Metadata Potentially Exposed**

   Source raised by an active scanner (Cloud Metadata Potentially Exposed)
   Reference
   1. https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/

2. **Absence of Anti-CSRF Tokens**

   Source raised by a passive scanner (Absence of Anti-CSRF Tokens)
   CWE ID 352
   WASC ID 9
   Reference
   1. https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html
   2. https://cwe.mitre.org/data/definitions/352.html

3. **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
   1. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
   2. https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
   3. https://www.w3.org/TR/CSP/
   4. https://w3c.github.io/webappsec-csp/
   5. https://web.dev/articles/csp
   6. https://caniuse.com/#feat=contentsecuritypolicy
   7. https://content-security-policy.com/

4. **Hidden File Found**

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

5. **Vulnerable JS Library**

   Source raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
   CWE ID 829
   Reference
   1. https://github.com/advisories/GHSA-2vrf-hf26-jrp5
   2. https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746
   3. https://nvd.nist.gov/vuln/detail/CVE-2024-21490
   4. https://github.com/advisories/GHSA-5cp4-xmrw-59wf
   5. https://nvd.nist.gov/vuln/detail/CVE-2020-7676
   6. https://github.com/advisories/GHSA-4w4v-5hc9-xrr2
   7. https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747
   8. https://blog.angular.io/discontinued-long-term-support-for-angularjs-cc066b82e65a?gi=9d3103b5445c
   9. https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113
   10. https://github.com/angular/angular.js
   11. https://github.com/advisories/GHSA-qwqh-hm9m-p5hr
   12. https://github.com/advisories/GHSA-m2h2-264f-f486
   13. https://github.com/advisories/GHSA-prc3-vjfx-vhm9
   14. https://github.com/angular/angular.js/commit/726f49dcf6c23106ddaf5cfd5e2e592841db743a
   15. https://github.com/advisories/GHSA-2qqx-w9hr-q5gx
   16. https://github.com/angular/angular.js/blob/master/CHANGELOG.md#179-pollution-eradication-2019-11-19
   17. https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos

6. **Cookie No HttpOnly Flag**

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

7. **Cookie Without Secure Flag**

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

8. **Cookie with SameSite Attribute None**

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

9. **Cookie without SameSite Attribute**

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

10. **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
    1. https://httpd.apache.org/docs/current/mod/core.html#servertokens
    2. https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)
    3. https://www.troyhunt.com/shhh-dont-let-your-response-headers/

11. **Strict-Transport-Security Header Not Set**

    Source raised by a passive scanner (Strict-Transport-Security Header)
    CWE ID 319
    WASC ID 15
    Reference
    1. https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
    2. https://owasp.org/www-community/Security_Headers
    3. https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
    4. https://caniuse.com/stricttransportsecurity
    5. https://datatracker.ietf.org/doc/html/rfc6797

12. **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
    1. https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)
    2. https://owasp.org/www-community/Security_Headers

13. **Information Disclosure - Suspicious Comments**

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

14. **Modern Web Application**

    Source raised by a passive scanner (Modern Web Application)

15. **Re-examine Cache-control Directives**

    Source raised by a passive scanner (Re-examine Cache-control Directives)
    CWE ID 525
    WASC ID 13
    Reference
    1. https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
    2. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
    3. https://grayduck.mn/2021/09/13/cache-control-recommendations/

16. **Session Management Response Identified**

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

17. **User Agent Fuzzer**

    Source raised by an active scanner (User Agent Fuzzer)
    Reference
    1. https://owasp.org/wstg

18. **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
    1. https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html