ZAP Scanning Report

Generated with  ZAP on Fri 29 Jul 2022, at 16:21:28

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://qa.contilink.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 (9.1%)	2 (18.2%)	1 (9.1%)	4 (36.4%)
	Low	0 (0.0%)	0 (0.0%)	3 (27.3%)	1 (9.1%)	4 (36.4%)
	Informational	0 (0.0%)	0 (0.0%)	2 (18.2%)	1 (9.1%)	3 (27.3%)
	Total	0 (0.0%)	1 (9.1%)	7 (63.6%)	3 (27.3%)	11 (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://qa.contilink.com	0 (0)	4 (4)	4 (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
Absence of Anti-CSRF Tokens	Medium	7 (63.6%)
Total		11

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	11 (100.0%)
Missing Anti-clickjacking Header	Medium	7 (63.6%)
Vulnerable JS Library	Medium	3 (27.3%)
Cookie No HttpOnly Flag	Low	1 (9.1%)
Cookie Without Secure Flag	Low	5 (45.5%)
Cookie without SameSite Attribute	Low	8 (72.7%)
Timestamp Disclosure - Unix	Low	15 (136.4%)
Information Disclosure - Sensitive Information in URL	Informational	5 (45.5%)
Information Disclosure - Suspicious Comments	Informational	24 (218.2%)
Re-examine Cache-control Directives	Informational	1 (9.1%)
Total		11

Alerts

1. **Risk=Medium, Confidence=High (1)**
    1. **https://qa.contilink.com (1)**
        1. Content Security Policy (CSP) Header Not Set **(1)**
            1. ▶ GET https://qa.contilink.com/coc/colordering/order?ref=1074762&navigationPath=cite-plt-en-us/ordering
2. **Risk=Medium, Confidence=Medium (2)**
    1. **https://qa.contilink.com (2)**
        1. Missing Anti-clickjacking Header **(1)**
            1. ▶ GET https://qa.contilink.com/cite/servlet/page/cite-bicycle-de-en/public/cookie-policy
        2. Vulnerable JS Library **(1)**
            1. ▶ GET https://qa.contilink.com/cas/js/jquery/jquery-1.11.3.min.js
3. **Risk=Medium, Confidence=Low (1)**
    1. **https://qa.contilink.com (1)**
        1. Absence of Anti-CSRF Tokens **(1)**

1. ▶ GET https://qa.contilink.com/coc/colordering/order?ref=1074762&navigationPath=cite-plt-en-us/ordering

4. **Risk=Low, Confidence=Medium (3)**

    1. **https://qa.contilink.com (3)**

        1. **Cookie No HttpOnly Flag (1)**

            1. ▶ GET https://qa.contilink.com/home?d=%7B%7BserverObj.d%7D%7D

        2. **Cookie Without Secure Flag (1)**

            1. ▶ GET https://qa.contilink.com/oauth2/authorization/cocgateway

        3. **Cookie without SameSite Attribute (1)**

            1. ▶ GET https://qa.contilink.com/coc/colordering/order?ref=1074762&navigationPath=cite-plt-en-us/ordering

5. **Risk=Low, Confidence=Low (1)**

    1. **https://qa.contilink.com (1)**

        1. **Timestamp Disclosure - Unix (1)**

            1. ▶ GET https://qa.contilink.com/cas/webjars/bootstrap/5.1.3/css/bootstrap-grid.min.css

6. **Risk=Informational, Confidence=Medium (2)**

    1. **https://qa.contilink.com (2)**

        1. **Information Disclosure - Sensitive Information in URL (1)**

            1. ▶ GET https://qa.contilink.com/?userEmail=foo-bar%40example.com&userId=ZAP

        2. **Re-examine Cache-control Directives (1)**

            1. ▶ GET https://qa.contilink.com/home/pub/resetpassword

7. **Risk=Informational, Confidence=Low (1)**

    1. **https://qa.contilink.com (1)**

        1. **Information Disclosure - Suspicious Comments (1)**

            1. ▶ GET https://qa.contilink.com/coc/colordering/order?ref=1074762&navigationPath=cite-plt-en-us/ordering

Appendix

Alert types

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

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

Source	raised by a passive scanner (Absence of Anti-CSRF Tokens)
CWE ID	352
WASC ID	9
Reference	1. http://projects.webappsec.org/Cross-Site-Request-Forgery 2. http://cwe.mitre.org/data/definitions/352.html

2. **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. http://www.w3.org/TR/CSP/ 4. http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html 5. http://www.html5rocks.com/en/tutorials/security/content-security-policy/ 6. http://caniuse.com/#feat=contentsecuritypolicy 7. http://content-security-policy.com/

3. **Missing Anti-clickjacking Header**

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	1. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

4. **Vulnerable JS Library**

Source	raised by a passive scanner (Vulnerable JS Library)
CWE ID	829
Reference	1. https://github.com/jquery/jquery/issues/2432 2. http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ 3. http://research.insecurelabs.org/jquery/test/ 4. https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ 5. https://nvd.nist.gov/vuln/detail/CVE-2019-11358 6. https://nvd.nist.gov/vuln/detail/CVE-2015-9251 7. https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b 8. https://bugs.jquery.com/ticket/11974 9. https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

5. **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

6. **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

7. **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

8. **Timestamp Disclosure - Unix**

Source raised by a passive scanner (Timestamp Disclosure)
CWE ID 200
WASC ID 13
Reference
1. http://projects.webappsec.org/w/page/13246936/Information%20Leakage

9. **Information Disclosure - Sensitive Information in URL**

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

10. **Information Disclosure - Suspicious Comments**

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

11. **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