ZAP Scanning Report

Generated with The ZAP logoZAP on Fri 30 Sep 2022, at 11:39:33

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%)	1 (9.1%)	1 (9.1%)	3 (27.3%)
	Low	0 (0.0%)	0 (0.0%)	4 (36.4%)	1 (9.1%)	5 (45.5%)
	Informational	0 (0.0%)	0 (0.0%)	3 (27.3%)	0 (0.0%)	3 (27.3%)
	Total	0 (0.0%)	1 (9.1%)	8 (72.7%)	2 (18.2%)	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)	3 (3)	5 (8)	2 (10)

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%)
Content Security Policy (CSP) Header Not Set	Medium	4 (36.4%)
Vulnerable JS Library	Medium	3 (27.3%)
Total		11

Alert type	Risk	Count
Cookie Without Secure Flag	Low	1 (9.1%)
Cookie with SameSite Attribute None	Low	1 (9.1%)
Cookie without SameSite Attribute	Low	5 (45.5%)
Cross-Domain JavaScript Source File Inclusion	Low	2 (18.2%)
Timestamp Disclosure - Unix	Low	36 (327.3%)
Information Disclosure - Sensitive Information in URL	Informational	1 (9.1%)
Information Disclosure - Suspicious Comments	Informational	42 (381.8%)
Re-examine Cache-control Directives	Informational	2 (18.2%)
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/cas/login?service=https%3A%2F%2Fqa.contilink.com%2Fgco%2Fj_spring_cas_security_check
2. **Risk=Medium, Confidence=Medium (1)**
    1. **https://qa.contilink.com (1)**
        1. **Vulnerable JS Library (1)**
            1. ▶ GET https://qa.contilink.com/gco/js/bootstrap.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/cas/login?service=https%3A%2F%2Fqa.contilink.com%2Fgco%2Fj_spring_cas_security_check
4. **Risk=Low, Confidence=Medium (4)**
    1. **https://qa.contilink.com (4)**
        1. **Cookie Without Secure Flag (1)**

1. ▶ GET https://qa.contilink.com/gco/complaint/create?cm8=true&js=h&tzo=-4&ref=967676&navigationPath=cite-plt-en-us/claims

2. **Cookie with SameSite Attribute None** **(1)**

   1. ▶ POST https://qa.contilink.com/cas/login?service=https%3A%2F%2Fqa.contilink.com%2Fgco%2Fj_spring_cas_security_check

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

   1. ▶ GET https://qa.contilink.com/gco/complaint/create?cm8=true&js=h&tzo=-4&ref=967676&navigationPath=cite-plt-en-us/claims

4. **Cross-Domain JavaScript Source File Inclusion** **(1)**

   1. ▶ GET https://qa.contilink.com/gco/complaint/create?cm8=true&js=h&tzo=-4&ref=967676&navigationPath=cite-plt-en-us/claims

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

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

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

         1. ▶ GET https://qa.contilink.com/gco/complaint/create?cm8=true&js=h&tzo=-4&ref=967676&navigationPath=cite-plt-en-us/claims

6. **Risk=Informational, Confidence=Medium (3)**

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

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

         1. ▶ GET https://qa.contilink.com/gco/j_spring_cas_security_check?ticket=ST-1300-RmBFp2ryp0i8mX-xa5l-Pj0E590-57040cd07f83

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

         1. ▶ GET https://qa.contilink.com/cas/login?service=https%3A%2F%2Fqa.contilink.com%2Fgco%2Fj_spring_cas_security_check

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. Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829
Reference	1. https://github.com/twbs/bootstrap/issues/28236 2. https://github.com/twbs/bootstrap/issues/20184 3. https://github.com/advisories/GHSA-4p24-vmcr-4gqj

4. 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

5. 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

6. 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

7. Cross-Domain JavaScript Source File Inclusion

Source	raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID	829

WASC ID	15

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