ZAP Scanning Report

Generated with  ZAP on Thu 8 Sep 2022, at 17:49:57

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 (8.3%)	2 (16.7%)	1 (8.3%)	4 (33.3%)
	Low	0 (0.0%)	0 (0.0%)	4 (33.3%)	1 (8.3%)	5 (41.7%)
	Informational	0 (0.0%)	0 (0.0%)	2 (16.7%)	1 (8.3%)	3 (25.0%)
	Total	0 (0.0%)	1 (8.3%)	8 (66.7%)	3 (25.0%)	12 (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	4 (33.3%)
Content Security Policy (CSP) Header Not Set	Medium	2 (16.7%)
Cross-Domain Misconfiguration	Medium	2 (16.7%)
Vulnerable JS Library	Medium	3 (25.0%)
Cookie Without Secure Flag	Low	3 (25.0%)
Cookie with SameSite Attribute None	Low	1 (8.3%)
Cookie without SameSite Attribute	Low	4 (33.3%)
Cross-Domain JavaScript Source File Inclusion	Low	1 (8.3%)
Timestamp Disclosure - Unix	Low	26 (216.7%)
Information Disclosure - Sensitive Information in URL	Informational	1 (8.3%)
Information Disclosure - Suspicious Comments	Informational	30 (250.0%)
Re-examine Cache-control Directives	Informational	2 (16.7%)
Total		12

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%2Fcas%2Foauth2.0%2FcallbackAuthorize%3Fclient_id%3Dcocgateway%26redirect_uri%3Dhttps%253A%252F%25ctfraxCzreijboA001R36xLxO3a_J0czI4Y%253D%26nonce%3D3U0GvE8rflYSYXh84Mle5-la4eefNGBAScAxNMjMLbs%26client_name%3DCasOAuthClient
2. **Risk=Medium, Confidence=Medium (2)**
    1. **https://qa.contilink.com (1)**
        1. Vulnerable JS Library **(1)**
            1. ▶ GET https://qa.contilink.com/coc/colordering/webjars/angularjs/1.4.3/angular-animate.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/cas/login?service=https%3A%2F%2Fqa.contilink.com%2Fcas%2Foauth2.0%2FcallbackAuthorize%3Fclient_id%3Dcocgateway%26redirect_uri%3Dhttps%253A%252F%25ctfraxCzreijboA001R36xLxO3a_J0czI4Y%253D%26nonce%3D3U0GvE8rflYSYXh84Mle5-la4eefNGBAScAxNMjMLbs%26client_name%3DCasOAuthClient
4. **Risk=Low, Confidence=Medium (4)**

1. **https://qa.contilink.com (4)**

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

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

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

        1. ▶ POST https://qa.contilink.com/cas/login?
service=https%3A%2F%2Fqa.contilink.com%2Fcas%2Foauth2.0%2FcallbackAuthorize%3Fclient_id%3Dcocgateway%26redirect_uri%3Dhttps%253A%252F%25
ctfraxCzreijboA001R36xLxO3a_J0czI4Y%253D%26nonce%3D3U0GvE8rflYSYXh84Mle5-la4eefNGBAScAxNMjMLbs%26client_name%3DCasOAuthClient

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

        1. ▶ GET https://qa.contilink.com/cas/login?
service=https%3A%2F%2Fqa.contilink.com%2Fcas%2Foauth2.0%2FcallbackAuthorize%3Fclient_id%3Dcocgateway%26redirect_uri%3Dhttps%253A%252F%25
ctfraxCzreijboA001R36xLxO3a_J0czI4Y%253D%26nonce%3D3U0GvE8rflYSYXh84Mle5-la4eefNGBAScAxNMjMLbs%26client_name%3DCasOAuthClient

    4. **Cross-Domain JavaScript Source File Inclusion (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/css/bootstrap/bootstrap-3.3.6.min.css

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

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

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

            1. ▶ GET https://qa.contilink.com/cas/oauth2.0/callbackAuthorize?
client_id=cocgateway&redirect_uri=https%3A%2F%2Fqa.contilink.com%2Flogin%2Foauth2%2Fcode%2Fcocgateway&response_type=code&state=okLbw17-
ctfraxCzreijboA001R36xLxO3a_J0czI4Y%3D&nonce=3U0GvE8rflYSYXh84Mle5-la4eefNGBAScAxNMjMLbs&client_name=CasOAuthClient&ticket=ST-
8917-Yi7R5gnOMtOQ5F5n1CaL1iH7sck-e83d9c351ead

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

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

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

            1. ▶ GET https://qa.contilink.com/cas/login?
service=https%3A%2F%2Fqa.contilink.com%2Fcas%2Foauth2.0%2FcallbackAuthorize%3Fclient_id%3Dcocgateway%26redirect_uri%3Dhttps%253A%252F%25
ctfraxCzreijboA001R36xLxO3a_J0czI4Y%253D%26nonce%3D3U0GvE8rflYSYXh84Mle5-la4eefNGBAScAxNMjMLbs%26client_name%3DCasOAuthClient

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. **Cross-Domain Misconfiguration**

Source raised by a passive scanner (Cross-Domain Misconfiguration)
CWE ID 264
WASC ID 14
Reference
1. https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

4. **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-r5fx-8r73-v86c
2. https://github.com/angular/angular.js/blob/master/CHANGELOG.md
3. https://github.com/angular/angular.js/blob/master/CHANGELOG.md#150-beta1-dense-dispersion-2015-09-29
4. https://github.com/advisories/GHSA-5cp4-xmrw-59wf
5. https://github.com/angular/angular.js/blob/master/CHANGELOG.md#1230-patronal-resurrection-2016-07-21
6. https://github.com/angular/angular.js/commit/8f31f1ff43b673a24f84422d5c13d6312b2c4d94
7. https://nvd.nist.gov/vuln/detail/CVE-2020-7676
8. https://github.com/angular/angular.js/pull/15699
9. https://blog.angular.io/discontinued-long-term-support-for-angularjs-cc066b82e65a?gi=9d3103b5445c
10. https://github.com/mozilla/addons-linter/issues/1000#issuecomment-282083435
11. http://pastebin.com/raw/kGrdaypP
12. https://github.com/angular/angular.js/commit/726f49dcf6c23106ddaf5cfd5e2e592841db743a
13. https://github.com/angular/angular.js/blob/master/CHANGELOG.md#179-pollution-eradication-2019-11-19

5. **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

6. **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

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. **Cross-Domain JavaScript Source File Inclusion**

Source raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID 829
WASC ID 15

9. **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

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

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

11. **Information Disclosure - Suspicious Comments**

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

12. **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