ZAP Scanning Report

Generated with ZAP on Tue 29 Nov 2022, at 12:12:33

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 (7.7%)	4 (30.8%)	1 (7.7%)	6 (46.2%)
	Low	0 (0.0%)	0 (0.0%)	4 (30.8%)	0 (0.0%)	4 (30.8%)
	Informational	0 (0.0%)	0 (0.0%)	2 (15.4%)	1 (7.7%)	3 (23.1%)
	Total	0 (0.0%)	1 (7.7%)	10 (76.9%)	2 (15.4%)	13 (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)	5 (5)	4 (9)	2 (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	3 (23.1%)
Buffer Overflow	Medium	1 (7.7%)
Content Security Policy (CSP) Header Not Set	Medium	2 (15.4%)
Cross-Domain Misconfiguration	Medium	1 (7.7%)
		1

[Format String Error](#)	Medium	(7.7%)
[Vulnerable JS Library](#)	Medium	4 (30.8%)
[Cookie Without Secure Flag](#)	Low	3 (23.1%)
[Cookie with SameSite Attribute None](#)	Low	1 (7.7%)
[Cookie without SameSite Attribute](#)	Low	4 (30.8%)
[Cross-Domain JavaScript Source File Inclusion](#)	Low	1 (7.7%)
[Information Disclosure - Sensitive Information in URL](#)	Informational	1 (7.7%)
[Information Disclosure - Suspicious Comments](#)	Informational	16 (123.1%)
[Re-examine Cache-control Directives](#)	Informational	3 (23.1%)
Total		13

Alerts

1. **Risk=Medium, Confidence=High (1)**

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

        1. **[Content Security Policy (CSP) Header Not Set](#) (1)**

            ▶ GET https://qa.contilink.com/cas/login?service=https%3A%2F%2Fqa.contilink.com%2Fcas%2Foauth2.0%2FcallbackAuthorize%3Fclient_id%3Docgateway%26redirect_uri%3Dhttps%253A%252F%252Fqa.contilink

2. **Risk=Medium, Confidence=Medium (4)**

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

        1. **[Buffer Overflow](#) (1)**

            ▶ POST https://qa.contilink.com/coc/ctagold/secondaryapproval/data/updatestatus

        2. **[Format String Error](#) (1)**

            ▶ POST https://qa.contilink.com/coc/ctagold/secondaryapproval/data/updatestatus

        3. **[Vulnerable JS Library](#) (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)**

            ▶ GET https://qa.contilink.com/cas/login?service=https%3A%2F%2Fqa.contilink.com%2Fcas%2Foauth2.0%2FcallbackAuthorize%3Fclient_id%3Docgateway%26redirect_uri%3Dhttps%253A%252F%252Fqa.contilink

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

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

        1. **[Cookie Without Secure Flag](#) (1)**

            ▶ GET https://qa.contilink.com/coc/ctagold/secondaryapproval?ref=3243458&navigationPath=cite-plt-en-us%2Fmarketing

        2. **[Cookie with SameSite Attribute None](#) (1)**

            ▶ POST https://qa.contilink.com/cas/login?service=https%3A%2F%2Fqa.contilink.com%2Fcas%2Foauth2.0%2FcallbackAuthorize%3Fclient_id%3Docgateway%26redirect_uri%3Dhttps%253A%252F%252Fqa.contilink

        3. **[Cookie without SameSite Attribute](#) (1)**

            ▶ GET https://qa.contilink.com/cas/login?service=https%3A%2F%2Fqa.contilink.com%2Fcas%2Foauth2.0%2FcallbackAuthorize%3Fclient_id%3Docgateway%26redirect_uri%3Dhttps%253A%252F%252Fqa.contilink

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

            ▶ GET https://qa.contilink.com/coc/ctagold/secondaryapproval?ref=3243458&navigationPath=cite-plt-en-us%2Fmarketing

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

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

        1. **[Information Disclosure - Sensitive Information in URL](#) (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=5XWLyNc7gMfTee5l3xNh 404-8v9gf08DoAc6J47algO0YgTBIvA-5aa8e8a5db15

        2. **[Information Disclosure - Suspicious Comments](#) (1)**

            ▶ GET https://qa.contilink.com/cas/login?service=https%3A%2F%2Fqa.contilink.com%2Fcas%2Foauth2.0%2FcallbackAuthorize%3Fclient_id%3Docgateway%26redirect_uri%3Dhttps%253A%252F%252Fqa.contilink

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

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. **Buffer Overflow**

   Source   raised by an active scanner ([Buffer Overflow](#))
   CWE ID   [120](#)
   WASC ID   7
   Reference   1. [https://owasp.org/www-community/attacks/Buffer_overflow_attack](#)

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. [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/](#)

4. **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](#)

5. **Format String Error**

   Source   raised by an active scanner ([Format String Error](#))
   CWE ID   [134](#)
   WASC ID   6
   Reference   1. [https://owasp.org/www-community/attacks/Format_string_attack](#)

6. **Vulnerable JS Library**

   Source   raised by a passive scanner ([Vulnerable JS Library (Powered by Retire.js)](#))
   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/](#)

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

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

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

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

12. **Information Disclosure - Suspicious Comments**

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

13. **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/](#)