ZAP Scanning Report

Generated with The ZAP logoZAP on Mon 28 Nov 2022, at 21:23:20

Contents

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- http://qa.contilink.com
- 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%)	1 (6.2%)	0 (0.0%)	1 (6.2%)
	Medium	0 (0.0%)	1 (6.2%)	3 (18.8%)	1 (6.2%)	5 (31.2%)
	Low	0 (0.0%)	0 (0.0%)	6 (37.5%)	1 (6.2%)	7 (43.8%)
	Informational	0 (0.0%)	0 (0.0%)	2 (12.5%)	1 (6.2%)	3 (18.8%)
	Total	0 (0.0%)	1 (6.2%)	12 (75.0%)	3 (18.8%)	16 (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**	1 (1)	4 (5)	7 (12)	2 (14)

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
SQL Injection	High	2 (12.5%)
Absence of Anti-CSRF Tokens	Medium	14 (87.5%)
Content Security Policy (CSP) Header Not Set	Medium	9 (56.2%)
Cross-Domain Misconfiguration	Medium	1 (6.2%)
Missing Anti-clickjacking Header	Medium	3 (18.8%)
Vulnerable JS Library	Medium	4 (25.0%)
Application Error Disclosure	Low	2 (12.5%)
Cookie Without Secure Flag	Low	7 (43.8%)
Cookie with SameSite Attribute None	Low	3 (18.8%)
Cookie without SameSite Attribute	Low	11 (68.8%)
Cross Site Scripting Weakness (Persistent in JSON Response)	Low	12 (75.0%)
Cross-Domain JavaScript Source File Inclusion	Low	5 (31.2%)
Information Disclosure - Debug Error Messages	Low	2 (12.5%)
Information Disclosure - Sensitive Information in URL	Informational	5 (31.2%)
Information Disclosure - Suspicious Comments	Informational	22 (137.5%)
Re-examine Cache-control Directives	Informational	2 (12.5%)
Total		16

Alerts

1. **Risk=High, Confidence=Medium (1)**
    1. **https://qa.contilink.com (1)**
        1. **SQL Injection (1)**
            1. ▶ POST https://qa.contilink.com/coc/ctagold/prospect/data/saveprospect
2. **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%25
3. **Risk=Medium, Confidence=Medium (3)**
    1. **https://qa.contilink.com (2)**

        1. **Missing Anti-clickjacking Header (1)**
            1. ▶ GET https://qa.contilink.com/cite/servlet/page/cite-plt-en-us
        2. **Vulnerable JS Library (1)**
            1. ▶ GET https://qa.contilink.com/cas/js/jquery/jquery-1.11.3.min.js

4. **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%25
5. **Risk=Low, Confidence=Medium (6)**
    1. **https://qa.contilink.com (6)**
        1. **Application Error Disclosure (1)**
            1. ▶ GET https://qa.contilink.com/coc/ctagold/prospect/data/read/number/00857188
        2. **Cookie Without Secure Flag (1)**
            1. ▶ GET https://qa.contilink.com/coc/ctagold/prospect?ref=3872980&navigationPath=cite-plt-en-us%2Fmarketing
        3. **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
        4. **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
        5. **Cross-Domain JavaScript Source File Inclusion (1)**
            1. ▶ GET https://qa.contilink.com/coc/ctagold/prospect?ref=3872980&navigationPath=cite-plt-en-us%2Fmarketing
        6. **Information Disclosure - Debug Error Messages (1)**
            1. ▶ GET https://qa.contilink.com/coc/ctagold/prospect/data/read/number/00857188
6. **Risk=Low, Confidence=Low (1)**
    1. **https://qa.contilink.com (1)**
        1. **Cross Site Scripting Weakness (Persistent in JSON Response) (1)**
            1. ▶ GET https://qa.contilink.com/coc/ctagold/prospect/data/0007400022
7. **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/cas/oauth2.0/callbackAuthorize?
               client_id=cocgateway&redirect_uri=https%3A%2F%2Fqa.contilink.com%2Flogin%2Foauth2%2Fcode%2Fcocgateway&response_type=code&state=Hs6jzCaXTQ
               15655-ZIjN3HQWFmX8In6ZR8Lud93yPuE-ce8ddafae540
        2. **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
8. **Risk=Informational, Confidence=Low (1)**

Appendix

Alert types

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

1. **SQL Injection**

Source	raised by an active scanner (SQL Injection)
CWE ID	89
WASC ID	19
Reference	1. https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

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. http://projects.webappsec.org/Cross-Site-Request-Forgery 2. http://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. 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. **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

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. **Application Error Disclosure**

Source	raised by a passive scanner (Application Error Disclosure)
CWE ID	200
WASC ID	13

8. **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

9. **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

10. **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

11. **Cross Site Scripting Weakness (Persistent in JSON Response)**

Source	raised by an active scanner (Cross Site Scripting (Persistent))
CWE ID	79
WASC ID	8
Reference	1. http://projects.webappsec.org/Cross-Site-Scripting 2. http://cwe.mitre.org/data/definitions/79.html

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

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

13. **Information Disclosure - Debug Error Messages**

Source	raised by a passive scanner (Information Disclosure - Debug Error Messages)
CWE ID	200
WASC ID	13

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

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

15. **Information Disclosure - Suspicious Comments**

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

16. **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/