ZAP Scanning Report

Generated with  ZAP on Fri 30 Sep 2022, at 12:41:25

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%)	3 (25.0%)	0 (0.0%)	3 (25.0%)
	Total	0 (0.0%)	1 (8.3%)	9 (75.0%)	2 (16.7%)	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)	4 (4)	5 (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	5 (41.7%)
Buffer Overflow	Medium	37 (308.3%)
Content Security Policy (CSP) Header Not Set	Medium	2 (16.7%)
Vulnerable JS Library	Medium	3 (25.0%)
Cookie Without Secure Flag	Low	1 (8.3%)
Cookie with SameSite Attribute None	Low	1 (8.3%)
Cookie without SameSite Attribute	Low	5 (41.7%)
Cross-Domain JavaScript Source File Inclusion	Low	1 (8.3%)
Timestamp Disclosure - Unix	Low	115 (958.3%)
Information Disclosure - Sensitive Information in URL	Informational	1 (8.3%)
Information Disclosure - Suspicious Comments	Informational	34 (283.3%)
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%2Fgco%2Fj_spring_cas_security_check

Alert tags
- OWASP_2021_A05
- OWASP_2017_A06

Alert description
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Request

▼ Request line and header section (497 bytes)

```
GET https://qa.contilink.com/cas/login?service=https%3A%2F%2Fqa.contilink.com%2Fgco%2Fj_spring_cas_security_check HTTP/1.1
Host: qa.contilink.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (852 bytes)

```
HTTP/1.1 200 OK
Date: Fri, 30 Sep 2022 16:57:39 GMT
```

```
Server: Apache
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
X-Content-Type-Options: nosniff
X-Application-Context: cas:native
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Content-Language: en
Content-Type: text/html;charset=UTF-8
Expires: 0
Pragma: no-cache
Requestid: 620c5117-eab4-4c86-9ea2-9d80f9dce081
Strict-Transport-Security: max-age=15768000 ; includeSubDomains
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Xss-Protection: 1; mode=block
Set-Cookie: org.springframework.web.servlet.i18n.CookieLocaleResolver.LOCALE=en; Path=/; Secure; HttpOnly
Set-Cookie: TGC=; Max-Age=0; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/cas; Secure; HttpOnly
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
```

▶ Response body (21010 bytes)

Solution Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.

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

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

        1. **Buffer Overflow (1)**

            1. ▶ GET https://qa.contilink.com/gco/complaint/overview/search/result?showBatchNumber=false&complaintCustomerNumber=0008500379&showcustomerLetter=true&_searchAllShipToLocations=on&searchBy=formNumberSearch&

        2. **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/overview/list?cm8=true&js=h&ref=967678&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/overview/list?cm8=true&js=h&ref=967678&navigationPath=cite-plt-en-us/claims

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

            1. ▶ GET https://qa.contilink.com/gco/complaint/overview/list?cm8=true&js=h&ref=967678&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/overview/list?cm8=true&js=h&ref=967678&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-1748-ycpMxL9XCZZMj2ZJuwZsGVoEpPs-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. **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. **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

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