ZAP Scanning Report

Generated with  ZAP on Tue 6 Sep 2022, at 19:57:33

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%)	2 (15.4%)	1 (7.7%)	4 (30.8%)
	Low	0 (0.0%)	0 (0.0%)	5 (38.5%)	1 (7.7%)	6 (46.2%)
	Informational	0 (0.0%)	0 (0.0%)	2 (15.4%)	1 (7.7%)	3 (23.1%)
	Total	0 (0.0%)	1 (7.7%)	9 (69.2%)	3 (23.1%)	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)	3 (3)	6 (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	1 (7.7%)
Content Security Policy (CSP) Header Not Set	Medium	3 (23.1%)
Cross-Domain Misconfiguration	Medium	8 (61.5%)
Vulnerable JS Library	Medium	1 (7.7%)
Cookie No HttpOnly Flag	Low	2 (15.4%)
Cookie Without Secure Flag	Low	5 (38.5%)
Cookie with SameSite Attribute None	Low	1 (7.7%)
Cookie without SameSite Attribute	Low	9 (69.2%)
Cross-Domain JavaScript Source File Inclusion	Low	1 (7.7%)
Timestamp Disclosure - Unix	Low	66 (507.7%)
Information Disclosure - Sensitive Information in URL	Informational	2 (15.4%)
Information Disclosure - Suspicious Comments	Informational	15 (115.4%)
Re-examine Cache-control Directives	Informational	2 (15.4%)
Total		13

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%25BKcc%253D%26nonce%3DJc-wHUR0PYK-5fKSLRJfiFz3qN7kzn1YNp2UQHpmZrs%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/cite/resources/script/main-cite.4fff304446e7ef00a539.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%25BKcc%253D%26nonce%3DJc-wHUR0PYK-5fKSLRJfiFz3qN7kzn1YNp2UQHpmZrs%26client_name%3DCasOAuthClient

4. **Risk=Low, Confidence=Medium (5)**

    1. **https://qa.contilink.com (5)**

        1. **Cookie No HttpOnly Flag (1)**

            1. ▶ GET https://qa.contilink.com/j_spring_cas_security_check?ticket=ST-7112-qu8oK1biPLJW21olZEJ2Ks67PXM-e83d9c351ead

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

            1. ▶ GET https://qa.contilink.com/coc/invoicepreapproval/invPreApp/invoicesPending?ref=3967702

        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
BKcc%253D%26nonce%3DJc-wHUR0PYK-5fKSLRJfiFz3qN7kzn1YNp2UQHpmZrs%26client_name%3DCasOAuthClient

        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
BKcc%253D%26nonce%3DJc-wHUR0PYK-5fKSLRJfiFz3qN7kzn1YNp2UQHpmZrs%26client_name%3DCasOAuthClient

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

            1. ▼ GET https://qa.contilink.com/coc/invoicepreapproval/invPreApp/invoicesPending?ref=3967702

Alert tags
- OWASP_2021_A08

Alert description
The page includes one or more script files from a third-party domain.

Request

▼ Request line and header section (603 bytes)

```
GET https://qa.contilink.com/coc/invoicepreapproval/invPreApp/invoicesPending?ref=3967702 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
Cookie: SESSION=949cdf38-7106-4bf7-b598-2bcb3acfc770; org.springframework.web.servlet.i18n.CookieLocaleResolver.LOCALE=en
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (907 bytes)

```
HTTP/1.1 200 OK
Date: Wed, 07 Sep 2022 00:00:03 GMT
Server: Apache
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
X-Content-Type-Options: nosniff
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept
Access-Control-Allow-Methods: POST, GET, PUT, OPTIONS, DELETE, PATCH
Access-Control-Allow-Origin: *
Access-Control-Max-Age: 3600
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Content-Language: en-US
Content-Type: text/html;charset=UTF-8
Expires: 0
Pragma: no-cache
Referrer-Policy: no-referrer
Vary: Origin,Accept-Encoding,Access-Control-Request-Method,Access-Control-Request-Headers
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Xss-Protection: 1; mode=block
Set-Cookie: JSESSIONID=D8E5C03A94666EEBAF2D4DB4EC774F17; Path=/coc/invoicepreapproval; HttpOnly
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
```

▶ Response body (16006 bytes)

Parameter
`https://www.googletagmanager.com/gtag/js?id=UA-121373122-1`

Evidence
`<script async src="https://www.googletagmanager.com/gtag/js?id=UA-121373122-1"></script>`

Solution
Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

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=spLOSqcjiTSv
BKcc%3D&nonce=Jc-wHUR0PYK-5fKSLRJfiFz3qN7kzn1YNp2UQHpmZrs&client_name=CasOAuthClient&ticket=ST-7111-Gi7Sv2llbebqwzbbN9THyxQc7X8-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
BKcc%253D%26nonce%3DJc-wHUR0PYK-5fKSLRJfiFz3qN7kzn1YNp2UQHpmZrs%26client_name%3DCasOAuthClient

Alert tags
- OWASP_2021_A01
- OWASP_2017_A03

Alert description The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entir

Other info

The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script language="javascript" type="text/javascript">

$(document).ready(function() {

try {

", see evidence field for the suspicious comment/snippet.

Request

▼ Request line and header section (901 bytes)

```
GET https://qa.contilink.com/cas/login?service=https%3A%2F%2Fqa.contilink.com%2Fcas%2Foauth2.0%2FcallbackAuthorize%3Fclient_i
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
Cookie: SESSION=NGVkMzNjYzMtYjQzMy00ZGJlLWIxNWYtNTliZGEyMDU3ZmIw; SESSION=69e240d0-2233-41b1-9f68-7a95df980c85
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: Tue, 06 Sep 2022 23:59:24 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: 6e951153-d220-42c2-8382-7bcf10472908
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=97
Connection: Keep-Alive
```

▶ Response body (20643 bytes)

Evidence `username`

Solution Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

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/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/

5. **Cookie No HttpOnly Flag**

   Source raised by a passive scanner (Cookie No HttpOnly Flag)
   CWE ID 1004
   WASC ID 13
   Reference
   1. https://owasp.org/www-community/HttpOnly

6. **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

7. **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

8. **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

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

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

10. **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

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