JSBank-Scan-Report

Generated with ZAP on Tue 6 Dec 2022, at 13:08:56

Contents

- About this report
  - Report parameters
- Summaries
  - Alert counts by risk and confidence
  - Alert counts by site and risk
  - Alert counts by alert type
- Alerts
  - Risk=Medium, Confidence=High (4)
  - Risk=Medium, Confidence=Medium (1)
  - Risk=Medium, Confidence=Low (1)
  - Risk=Low, Confidence=High (1)
  - Risk=Low, Confidence=Medium (1)
  - Risk=Informational, Confidence=Medium (2)
  - Risk=Informational, Confidence=Low (4)

- Appendix
  - Alert types

About this report

Report parameters

Contexts

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

Sites

The following sites were included:

- `https://jsbl.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%)	4 (28.6%)	1 (7.1%)	1 (7.1%)	6 (42.9%)
	Low	0 (0.0%)	1 (7.1%)	1 (7.1%)	0 (0.0%)	2 (14.3%)
	Informational	0 (0.0%)	0 (0.0%)	2 (14.3%)	4 (28.6%)	6 (42.9%)
	Total	0 (0.0%)	5 (35.7%)	4 (28.6%)	5 (35.7%)	14 (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://jsbl.com	0 (0)	6 (6)	2 (8)	6 (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
Absence of Anti-CSRF Tokens	Medium	17 (121.4%)
CSP: Wildcard Directive	Medium	166 (1,185.7%)
CSP: script-src unsafe-inline	Medium	166 (1,185.7%)
CSP: style-src unsafe-inline	Medium	166 (1,185.7%)
Content Security Policy (CSP) Header Not Set	Medium	3 (21.4%)
Total		14

Alert type	Risk	Count
Vulnerable JS Library	Medium	1 (7.1%)
Cross-Domain JavaScript Source File Inclusion	Low	437 (3,121.4%)
Strict-Transport-Security Header Not Set	Low	1 (7.1%)
Charset Mismatch	Informational	3 (21.4%)
Information Disclosure - Suspicious Comments	Informational	317 (2,264.3%)
Modern Web Application	Informational	146 (1,042.9%)
Re-examine Cache-control Directives	Informational	139 (992.9%)
Retrieved from Cache	Informational	164 (1,171.4%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	5 (35.7%)
Total		14

Alerts

Risk=Medium, Confidence=High (4)

https://jsbl.com (4)

CSP: Wildcard Directive (1)

▶ GET https://jsbl.com/

CSP: script-src unsafe-inline (1)

▶ GET https://jsbl.com/

CSP: style-src unsafe-inline (1)

▶ GET https://jsbl.com/

Content Security Policy (CSP) Header Not Set (1)

▶ GET https://jsbl.com/%3C?php%23%20echo%20site_url('/').'personal/wealth-management/takaful/'%20?%3E

Risk=Medium, Confidence=Medium (1)

https://jsbl.com (1)

Vulnerable JS Library (1)

▶ GET https://jsbl.com/wp-content/themes/jsbankmain/js/jquery.min.js?ver=22a88578c8f140a7ca7709dc5bb3faeb

Risk=Medium, Confidence=Low (1)

https://jsbl.com (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://jsbl.com/

Risk=Low, Confidence=High (1)

https://jsbl.com (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://jsbl.com/wp-content/uploads/2020/04/internet_banking.mp4

Risk=Low, Confidence=Medium (1)

https://jsbl.com (1)

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://jsbl.com/

Risk=Informational, Confidence=Medium (2)

https://jsbl.com (2)

Modern Web Application (1)

▶ GET https://jsbl.com/

Retrieved from Cache (1)

▶ GET https://jsbl.com/robots.txt

Risk=Informational, Confidence=Low (4)

https://jsbl.com (4)

Charset Mismatch (1)

▶ GET https://jsbl.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fjsbl.com%2F

Information Disclosure - Suspicious Comments (1)

▶ GET https://jsbl.com/

Re-examine Cache-control Directives (1)

▶ GET https://jsbl.com/robots.txt

User Controllable HTML Element Attribute (Potential XSS) (1)

▶ GET https://jsbl.com/iban-generator/?Generate=Generate&acount=ZAP&branch=L9001&city=abbottabad

Appendix

Alert types

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

Absence of Anti-CSRF Tokens

Source	raised by a passive scanner (Absence of Anti-CSRF Tokens)
CWE ID	352
WASC ID	9

Reference	▪ http://projects.webappsec.org/Cross-Site-Request-Forgery ▪ http://cwe.mitre.org/data/definitions/352.html

CSP: Wildcard Directive

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ http://www.w3.org/TR/CSP2/ ▪ http://www.w3.org/TR/CSP/ ▪ http://caniuse.com/#search=content+security+policy ▪ http://content-security-policy.com/ ▪ https://github.com/shapesecurity/salvation ▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CSP: script-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15

Reference

- http://www.w3.org/TR/CSP2/
- http://www.w3.org/TR/CSP/
- http://caniuse.com/#search=content+security+policy
- http://content-security-policy.com/
- https://github.com/shapesecurity/salvation
- https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CSP: style-src unsafe-inline

Source raised by a passive scanner (CSP)

CWE ID 693

WASC ID 15

Reference

- http://www.w3.org/TR/CSP2/
- http://www.w3.org/TR/CSP/
- http://caniuse.com/#search=content+security+policy
- http://content-security-policy.com/
- https://github.com/shapesecurity/salvation
- https://developers.google.com/web/fundamental

s/security/csp#policy_applies_to_a_wide_variety_of_resources

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	▪ https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy ▪ https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html ▪ http://www.w3.org/TR/CSP/ ▪ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html ▪ http://www.html5rocks.com/en/tutorials/security/content-security-policy/ ▪ http://caniuse.com/#feat=contentsecuritypolicy ▪ http://content-security-policy.com/

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829
Reference	▪ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ ▪ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 ▪ https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b ▪ https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

Cross-Domain JavaScript Source File Inclusion

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

Strict-Transport-Security Header Not Set

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15

Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html ▪ https://owasp.org/www-community/Security_Headers ▪ http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security ▪ http://caniuse.com/stricttransportsecurity ▪ http://tools.ietf.org/html/rfc6797

Charset Mismatch

Source	raised by a passive scanner (Charset Mismatch)
CWE ID	436
WASC ID	15
Reference	▪ http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection

Information Disclosure - Suspicious Comments

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

Modern Web Application

Source raised by a passive scanner (Modern Web Application)

Re-examine Cache-control Directives

Source raised by a passive scanner (Re-examine Cache-control Directives)

CWE ID 525

WASC ID 13

Reference

- https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
- https://grayduck.mn/2021/09/13/cache-control-recommendations/

Retrieved from Cache

Source raised by a passive scanner (Retrieved from Cache)

Reference

- https://tools.ietf.org/html/rfc7234
- https://tools.ietf.org/html/rfc7231
- http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)

User Controllable HTML Element Attribute (Potential XSS)

Source	raised by a passive scanner (User Controllable HTML Element Attribute (Potential XSS))
CWE ID	20
WASC ID	20
Reference	▪ http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute