BurjBank-Scan-Report

Generated with ZAP on Tue 6 Dec 2022, at 17:03:25

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://www.burjbankltd.com`
- `http://www.burjbankltd.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%)	1 (8.3%)	1 (8.3%)	3 (25.0%)
	Low	0 (0.0%)	1 (8.3%)	3 (25.0%)	0 (0.0%)	4 (33.3%)
	Informational	0 (0.0%)	0 (0.0%)	1 (8.3%)	4 (33.3%)	5 (41.7%)
	Total	0 (0.0%)	2 (16.7%)	5 (41.7%)	5 (41.7%)	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://www.burjbankltd.com	0 (0)	0 (0)	1 (1)	0 (1)
	http://www.burjbankltd.com	0 (0)	3 (3)	3 (6)	5 (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	215 (1,791.7%)
Content Security Policy (CSP) Header Not Set	Medium	124 (1,033.3%)
Missing Anti-clickjacking Header	Medium	116 (966.7%)
Cookie No HttpOnly Flag	Low	8 (66.7%)
Total		12

Alert type	Risk	Count
Cookie without SameSite Attribute	Low	8 (66.7%)
Strict-Transport-Security Header Not Set	Low	2 (16.7%)
X-Content-Type-Options Header Missing	Low	347 (2,891.7%)
Charset Mismatch	Informational	34 (283.3%)
Cookie Poisoning	Informational	2 (16.7%)
Information Disclosure - Suspicious Comments	Informational	133 (1,108.3%)
Modern Web Application	Informational	51 (425.0%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	22 (183.3%)
Total		12

Alerts

Risk=Medium, Confidence=High (1)

http://www.burjbankltd.com (1)

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

▶ GET http://www.burjbankltd.com/

Risk=Medium, Confidence=Medium (1)

http://www.burjbankltd.com (1)

Missing Anti-clickjacking Header (1)

▶ GET http://www.burjbankltd.com/

Risk=Medium, Confidence=Low (1)

http://www.burjbankltd.com (1)

Absence of Anti-CSRF Tokens (1)

▶ GET http://www.burjbankltd.com/

Risk=Low, Confidence=High (1)

https://www.burjbankltd.com (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.burjbankltd.com/wp-content/uploads/2020/08/Informasi-Perbankan-Terbaru.png

Risk=Low, Confidence=Medium (3)

http://www.burjbankltd.com (3)

Cookie No HttpOnly Flag (1)

▶ GET http://www.burjbankltd.com/wp-login.php

Cookie without SameSite Attribute (1)

▶ GET http://www.burjbankltd.com/wp-login.php

X-Content-Type-Options Header Missing (1)

▶ GET http://www.burjbankltd.com/robots.txt

Risk=Informational, Confidence=Medium (1)

http://www.burjbankltd.com (1)

Modern Web Application (1)

▶ GET http://www.burjbankltd.com/wp-content/plugins/table-of-contents-plus/front.min.js?ver=2106

Risk=Informational, Confidence=Low (4)

http://www.burjbankltd.com (4)

Charset Mismatch (1)

▶ GET http://www.burjbankltd.com/wp-json/oembed/1.0/embed?format=xml&url=http%3A%2F%2Fwww.burjbankltd.com%2Fjenis-kpr-dan-pengertiannya%2F

Cookie Poisoning (1)

▶ GET http://www.burjbankltd.com/wp-login.php?wp_lang=id_ID

Information Disclosure - Suspicious Comments (1)

▶ GET http://www.burjbankltd.com/

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

▶ GET http://www.burjbankltd.com/wp-login.php?action=lostpassword

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

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/

Missing Anti-clickjacking Header

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Cookie No HttpOnly Flag

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

Cookie without SameSite Attribute

Source	raised by a passive scanner (Cookie without SameSite Attribute)
CWE ID	1275
WASC ID	13
Reference	▪ https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

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

X-Content-Type-Options Header Missing

Source	raised by a passive scanner (X-Content-Type-Options Header Missing)
CWE ID	693
WASC ID	15
Reference	- http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx - https://owasp.org/www-community/Security_Headers

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

Cookie Poisoning

Source	raised by a passive scanner (Cookie Poisoning)
CWE ID	20
WASC ID	20
Reference	▪ http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-cookie

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)

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