DeutscheBank-Scan-Report

Generated with ZAP on Fri 2 Dec 2022, at 22:30:47

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://www.db.com
- https://www.db.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%)	0 (0.0%)	1 (7.7%)	2 (15.4%)
	Low	0 (0.0%)	2 (15.4%)	4 (30.8%)	1 (7.7%)	7 (53.8%)
	Informational	0 (0.0%)	0 (0.0%)	1 (7.7%)	3 (23.1%)	4 (30.8%)
	Total	0 (0.0%)	3 (23.1%)	5 (38.5%)	5 (38.5%)	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://www.db.com	0 (0)	2 (2)	7 (9)	4 (13)

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	9 (69.2%)
Content Security Policy (CSP) Header Not Set	Medium	143 (1,100.0%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	4 (30.8%)
Cookie Without Secure Flag	Low	4 (30.8%)
Cookie without SameSite Attribute	Low	6 (46.2%)
Total		13

Alert type	Risk	Count
Cross-Domain JavaScript Source File Inclusion	Low	589 (4,530.8%)
Strict-Transport-Security Header Not Set	Low	12 (92.3%)
Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)	Low	344 (2,646.2%)
Timestamp Disclosure - Unix	Low	4 (30.8%)
Information Disclosure - Suspicious Comments	Informational	304 (2,338.5%)
Modern Web Application	Informational	149 (1,146.2%)
Re-examine Cache-control Directives	Informational	116 (892.3%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	93 (715.4%)
Total		13

Alerts

Risk=Medium, Confidence=High (1)

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

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

▶ GET https://www.db.com/index?language_id=1&kid=sl.redirect-en.shortcut

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.db.com/media/events

Risk=Low, Confidence=High (2)

https://www.db.com (2)

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.db.com/application/~entryImage~

Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec) (1)

▶ GET https://www.db.com/robots.txt

Risk=Low, Confidence=Medium (4)

https://www.db.com (4)

Big Redirect Detected (Potential Sensitive Information Leak) (1)

▶ GET https://www.db.com/who-we-are/global-network/index

Cookie Without Secure Flag (1)

▶ GET https://www.db.com/index?language_id=1&kid=sl.redirect-en.shortcut

Cookie without SameSite Attribute (1)

▶ GET https://www.db.com/robots.txt

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.db.com/index?language_id=1&kid=sl.redirect-en.shortcut

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

▶ GET https://www.db.com/eye-able/public/js/eyeAble.js

Risk=Informational, Confidence=Medium (1)

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

Modern Web Application (1)

▶ GET https://www.db.com/index?language_id=1&kid=sl.redirect-en.shortcut

Risk=Informational, Confidence=Low (3)

https://www.db.com (3)

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.db.com/index?language_id=1&kid=sl.redirect-en.shortcut

Re-examine Cache-control Directives (1)

▶ GET https://www.db.com/robots.txt

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

▶ GET https://www.db.com/index?language_id=1&kid=sl.redirect-en.shortcut

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/

Big Redirect Detected (Potential Sensitive Information Leak)

Source	raised by a passive scanner (Big Redirect Detected (Potential Sensitive Information Leak))
CWE ID	201
WASC ID	13

Cookie Without Secure Flag

Source	raised by a passive scanner (Cookie Without Secure Flag)
CWE ID	614
WASC ID	13
Reference	▪ 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

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

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

Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15
Reference	▪ http://tools.ietf.org/html/rfc6797#section-8.1

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	200
WASC ID	13
Reference	▪ http://projects.webappsec.org/w/page/13246936/Information%20Leakage

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/

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