NIBBank-Scan-Report

Generated with ZAP on Tue 6 Dec 2022, at 21:17:24

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://ocsp.digicert.com
- http://ocsp.pki.goog
- http://r3.o.lencr.org
- https://nibpk.org

(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%)	1 (6.2%)	0 (0.0%)	0 (0.0%)	1 (6.2%)
	Medium	0 (0.0%)	1 (6.2%)	2 (12.5%)	1 (6.2%)	4 (25.0%)
	Low	0 (0.0%)	2 (12.5%)	2 (12.5%)	1 (6.2%)	5 (31.2%)
	Informational	0 (0.0%)	0 (0.0%)	2 (12.5%)	4 (25.0%)	6 (37.5%)
	Total	0 (0.0%)	4 (25.0%)	6 (37.5%)	6 (37.5%)	16 (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	http://ocsp.digicert.com	0 (0)	0 (0)	1 (1)	1 (2)
	https://nibpk.org	1 (1)	4 (5)	4 (9)	5 (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
PII Disclosure	High	2 (12.5%)
Absence of Anti-CSRF Tokens	Medium	844 (5,275.0%)
Total		16

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	894 (5,587.5%)
Missing Anti-clickjacking Header	Medium	828 (5,175.0%)
Vulnerable JS Library	Medium	1 (6.2%)
Cross-Domain JavaScript Source File Inclusion	Low	1818 (11,362.5%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	1 (6.2%)
Strict-Transport-Security Header Not Set	Low	3718 (23,237.5%)
Timestamp Disclosure - Unix	Low	1684 (10,525.0%)
X-Content-Type-Options Header Missing	Low	2784 (17,400.0%)
Charset Mismatch	Informational	266 (1,662.5%)
Information Disclosure - Suspicious Comments	Informational	2528 (15,800.0%)
Modern Web Application	Informational	1140 (7,125.0%)
Re-examine Cache-control Directives	Informational	1861 (11,631.2%)
Total		16

Alert type	Risk	Count
Retrieved from Cache	Informational	1 (6.2%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	4891 (30,568.8%)
Total		16

Alerts

Risk=High, Confidence=High (1)

https://nibpk.org (1)

PII Disclosure (1)

▶ GET https://nibpk.org/wp-content/plugins/elementor/assets/js/preloaded-modules.min.js?ver=3.8.1

Risk=Medium, Confidence=High (1)

https://nibpk.org (1)

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

▶ GET https://nibpk.org/wp-content/uploads/wpforms/

Risk=Medium, Confidence=Medium (2)

https://nibpk.org (2)

Missing Anti-clickjacking Header (1)

▶ GET https://nibpk.org/

Vulnerable JS Library (1)

▶ GET https://nibpk.org/wp-includes/js/jquery/ui/core.min.js?ver=1.13.1

Risk=Medium, Confidence=Low (1)

https://nibpk.org (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://nibpk.org/contact-us-page/

Risk=Low, Confidence=High (2)

http://ocsp.digicert.com (1)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

▶ GET http://ocsp.digicert.com/

https://nibpk.org (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://nibpk.org/robots.txt

Risk=Low, Confidence=Medium (2)

https://nibpk.org (2)

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://nibpk.org/

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

▶ GET https://nibpk.org/robots.txt

Risk=Low, Confidence=Low (1)

https://nibpk.org (1)

Timestamp Disclosure - Unix (1)

▶ GET https://nibpk.org/

Risk=Informational, Confidence=Medium (2)

http://ocsp.digicert.com (1)

Retrieved from Cache (1)

▶ GET http://ocsp.digicert.com/

https://nibpk.org (1)

Modern Web Application (1)

▶ GET https://nibpk.org/

Risk=Informational, Confidence=Low (4)

https://nibpk.org (4)

Charset Mismatch (1)

▶ GET https://nibpk.org/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fnibpk.org%2F

Information Disclosure - Suspicious Comments (1)

▶ GET https://nibpk.org/

Re-examine Cache-control Directives (1)

▶ GET https://nibpk.org/robots.txt

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

▶ POST https://nibpk.org/contact-us-page/

Appendix

Alert types

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

PII Disclosure

Source raised by a passive scanner (PII Disclosure)

CWE ID	359
WASC ID	13

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

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829
Reference	• https://nvd.nist.gov/vuln/detail/CVE-2022-31160 • https://github.com/jquery/jquery-ui/security/advisories/GHSA-h6gj-6jjq-h8g9

Cross-Domain JavaScript Source File Inclusion

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

Server Leaks Version Information via "Server" HTTP Response Header Field

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	200
WASC ID	13
Reference	▪ http://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 ▪ http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx ▪ http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

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

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

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

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