NBP-Scan-Report

Generated with ZAP on Tue 22 Nov 2022, at 21:14:00

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.nbp.com.pk
- https://www.nbp.com.pk

(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 (4.8%)	1 (4.8%)	0 (0.0%)	2 (9.5%)
	Medium	0 (0.0%)	1 (4.8%)	2 (9.5%)	1 (4.8%)	4 (19.0%)
	Low	0 (0.0%)	1 (4.8%)	6 (28.6%)	1 (4.8%)	8 (38.1%)
	Informational	0 (0.0%)	1 (4.8%)	3 (14.3%)	3 (14.3%)	7 (33.3%)
	Total	0 (0.0%)	4 (19.0%)	12 (57.1%)	5 (23.8%)	21 (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.nbp.com.pk	2 (2)	4 (6)	8 (14)	7 (21)

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
Hash Disclosure - Mac OSX salted SHA-1	High	32 (152.4%)
PII Disclosure	High	84 (400.0%)
Total		21

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	35 (166.7%)
Content Security Policy (CSP) Header Not Set	Medium	237 (1,128.6%)
Emails Found in the Viewstate	Medium	2 (9.5%)
Missing Anti-clickjacking Header	Medium	210 (1,000.0%)
Cookie without SameSite Attribute	Low	8 (38.1%)
Cross-Domain JavaScript Source File Inclusion	Low	208 (990.5%)
Information Disclosure - Debug Error Messages	Low	2 (9.5%)
Secure Pages Include Mixed Content	Low	7 (33.3%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	2712 (12,914.3%)
Strict-Transport-Security Header Not Set	Low	2665 (12,690.5%)
Timestamp Disclosure - Unix	Low	252 (1,200.0%)
X-Content-Type-Options Header Missing	Low	2622 (12,485.7%)
Total		21

Alert type	Risk	Count
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	132 (628.6%)
Content Security Policy (CSP) Report-Only Header Found	Informational	21 (100.0%)
Information Disclosure - Suspicious Comments	Informational	221 (1,052.4%)
Modern Web Application	Informational	20 (95.2%)
Re-examine Cache-control Directives	Informational	226 (1,076.2%)
Retrieved from Cache	Informational	272 (1,295.2%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	28 (133.3%)
Total		21

Alerts

Risk=High, Confidence=High (1)

https://www.nbp.com.pk (1)

PII Disclosure (1)

▶ GET https://www.nbp.com.pk/News/PIA_Sukuk/Term%20sheet%20-%20PIA%20Sukuk.pdf

Risk=High, Confidence=Medium (1)

https://www.nbp.com.pk (1)

Hash Disclosure - Mac OSX salted SHA-1 (1)

▶ GET https://www.nbp.com.pk/enquiries/Complaint-Form-Urdu.pdf

Risk=Medium, Confidence=High (1)

https://www.nbp.com.pk (1)

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

▶ GET https://www.nbp.com.pk/robots.txt

Risk=Medium, Confidence=Medium (2)

https://www.nbp.com.pk (2)

Emails Found in the Viewstate (1)

▶ GET https://www.nbp.com.pk/TENDER/Tenders.aspx?t=all

Missing Anti-clickjacking Header (1)

▶ GET https://www.nbp.com.pk/

Risk=Medium, Confidence=Low (1)

https://www.nbp.com.pk (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.nbp.com.pk/SITEMAP/index.aspx

Risk=Low, Confidence=High (1)

https://www.nbp.com.pk (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.nbp.com.pk/robots.txt

Risk=Low, Confidence=Medium (6)

https://www.nbp.com.pk (6)

Cookie without SameSite Attribute (1)

▶ GET https://www.nbp.com.pk/indexUrdu.aspx

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.nbp.com.pk/

Information Disclosure - Debug Error Messages (1)

▶ GET https://www.nbp.com.pk/TENDER/Tenders.aspx?t=all

Secure Pages Include Mixed Content (1)

▶ GET https://www.nbp.com.pk/Aamdani/index.aspx

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)

▶ GET https://www.nbp.com.pk/robots.txt

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

▶ GET https://www.nbp.com.pk/

Risk=Low, Confidence=Low (1)

https://www.nbp.com.pk (1)

Timestamp Disclosure - Unix (1)

▶ GET https://www.nbp.com.pk/Treasury/index.aspx

Risk=Informational, Confidence=High (1)

https://www.nbp.com.pk (1)

Content Security Policy (CSP) Report-Only Header Found (1)

▶ GET https://www.nbp.com.pk/Treasury/index.aspx

Risk=Informational, Confidence=Medium (3)

https://www.nbp.com.pk (3)

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.nbp.com.pk/

Modern Web Application (1)

▶ GET https://www.nbp.com.pk/

Retrieved from Cache (1)

▶ GET https://www.nbp.com.pk/News/PIA_Sukuk/Additional%20Payment%20Form.pdf

Risk=Informational, Confidence=Low (3)

https://www.nbp.com.pk (3)

Charset Mismatch (Header Versus Meta Content-Type Charset) (1)

▶ GET https://www.nbp.com.pk/careers/index.aspx

Re-examine Cache-control Directives (1)

▶ GET https://www.nbp.com.pk/

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

▶ GET https://www.nbp.com.pk/TENDER/Tenders.aspx?t=50

Appendix

Alert types

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

Hash Disclosure - Mac OSX salted SHA-1

Source	raised by a passive scanner (Hash Disclosure)
CWE ID	200

WASC ID	13
Reference	▪ http://projects.webappsec.org/w/page/13246936/Information%20Leakage ▪ http://openwall.info/wiki/john/sample-hashes

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/

Emails Found in the Viewstate

Source raised by a passive scanner (Viewstate)

CWE ID 642

WASC ID 14

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 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

Information Disclosure - Debug Error Messages

Source	raised by a passive scanner (Information Disclosure - Debug Error Messages)
CWE ID	200
WASC ID	13

Secure Pages Include Mixed Content

Source	raised by a passive scanner (Secure Pages Include Mixed Content)
CWE ID	311
WASC ID	4
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Source	raised by a passive scanner (Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))
CWE ID	200
WASC ID	13
Reference	▪ 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 (Header Versus Meta Content-Type Charset)

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

Content Security Policy (CSP) Report-Only Header Found

Source raised by a passive scanner (Content Security Policy (CSP) Header Not Set)

CWE ID 693

WASC ID 15

Reference
- https://www.w3.org/TR/CSP2/
- https://w3c.github.io/webappsec-csp/
- http://caniuse.com/#feat=contentsecuritypolicy
- http://content-security-policy.com/

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