BankOfPunjab-Scan-Report

Generated with ZAP on Mon 28 Nov 2022, at 17:48:35

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.bop.com.pk
- https://www.google-analytics.com
- https://d2liqplnt17rh6.cloudfront.net
- https://maps.googleapis.com
- https://secure-sdk.peekaboo.guru
- https://fonts.gstatic.com
- https://fonts.googleapis.com
- https://bop-web.peekaboo.guru
- https://www.gstatic.com
- https://digibop.com.pk
- https://cdnjs.cloudflare.com
- https://www.bop.com.pk
- http://ocsp.digicert.com

- http://ocsp.pki.goog

(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 (3.7%)	1 (3.7%)	0 (0.0%)	2 (7.4%)

	Confidence				
	User Confirmed	High	Medium	Low	Total
Medium	0 (0.0%)	4 (14.8%)	4 (14.8%)	1 (3.7%)	9 (33.3%)
Low	0 (0.0%)	3 (11.1%)	6 (22.2%)	1 (3.7%)	10 (37.0%)
Informational	0 (0.0%)	0 (0.0%)	2 (7.4%)	4 (14.8%)	6 (22.2%)
Total	0 (0.0%)	8 (29.6%)	13 (48.1%)	6 (22.2%)	27 (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://bop-web.peekaboo.guru	0 (0)	1 (1)	0 (1)	0 (1)
	https://digibop.com.pk	0 (0)	3 (3)	3 (6)	0 (6)

	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
https://cdnjs.cloudflare.com	0 (0)	1 (1)	0 (1)	0 (1)
https://www.bop.com.pk	2 (2)	3 (5)	5 (10)	5 (15)
http://ocsp.digicert.com	0 (0)	0 (0)	2 (2)	1 (3)
http://ocsp.pki.goog	0 (0)	1 (1)	0 (1)	0 (1)

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	5 (18.5%)
PII Disclosure	High	29 (107.4%)
Absence of Anti-CSRF Tokens	Medium	547 (2,025.9%)
Total		27

Alert type	Risk	Count
Application Error Disclosure	Medium	2 (7.4%)
CSP: Wildcard Directive	Medium	1 (3.7%)
CSP: script-src unsafe-inline	Medium	1 (3.7%)
CSP: style-src unsafe-inline	Medium	1 (3.7%)
Content Security Policy (CSP) Header Not Set	Medium	632 (2,340.7%)
Cross-Domain Misconfiguration	Medium	7 (25.9%)
Missing Anti-clickjacking Header	Medium	2 (7.4%)
Vulnerable JS Library	Medium	6 (22.2%)
Cookie No HttpOnly Flag	Low	39 (144.4%)
Cookie Without Secure Flag	Low	77 (285.2%)
Cookie without SameSite Attribute	Low	79 (292.6%)
Information Disclosure - Debug Error Messages	Low	2 (7.4%)
Total		27

Alert type	Risk	Count
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	351 (1,300.0%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	60 (222.2%)
Strict-Transport-Security Header Not Set	Low	2078 (7,696.3%)
Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)	Low	54 (200.0%)
Timestamp Disclosure - Unix	Low	77 (285.2%)
X-Content-Type-Options Header Missing	Low	440 (1,629.6%)
Information Disclosure - Suspicious Comments	Informational	182 (674.1%)
Loosely Scoped Cookie	Informational	3 (11.1%)
Modern Web Application	Informational	588 (2,177.8%)
Re-examine Cache-control Directives	Informational	14 (51.9%)
Retrieved from Cache	Informational	8 (29.6%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	566 (2,096.3%)
Total		27

Alerts

Risk=High, Confidence=High (1)

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

PII Disclosure (1)

▶ GET https://www.bop.com.pk/RoshanSamaajiKhidmat

Risk=High, Confidence=Medium (1)

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

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

▶ GET https://www.bop.com.pk/Documents/Resource_Center/FATCA%20Status%20BOP%20W-8BEN-E.pdf

Risk=Medium, Confidence=High (4)

https://digibop.com.pk (3)

CSP: Wildcard Directive (1)

▶ GET https://digibop.com.pk/apps/OnlineBanking/

CSP: script-src unsafe-inline (1)

▶ GET https://digibop.com.pk/apps/OnlineBanking/

CSP: style-src unsafe-inline (1)

▶ GET https://digibop.com.pk/apps/OnlineBanking/

http://ocsp.pki.goog (1)

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

▶ GET http://ocsp.pki.goog/gts1c3

Risk=Medium, Confidence=Medium (4)

https://bop-web.peekaboo.guru (1)

Missing Anti-clickjacking Header (1)

▶ GET https://bop-web.peekaboo.guru/?type=locator

https://cdnjs.cloudflare.com (1)

Cross-Domain Misconfiguration (1)

▶ GET https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css

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

Application Error Disclosure (1)

▶ GET https://www.bop.com.pk/Documents/Islamic%20Banking/Profit%2520Rates%2520May%25202013-1.pdf

Vulnerable JS Library (1)

▶ GET https://www.bop.com.pk/js/jquery1.1.js

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.bop.com.pk/BoP

Risk=Low, Confidence=High (3)

https://digibop.com.pk (1)

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

▶ GET https://digibop.com.pk/apps/OnlineBanking/

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

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.bop.com.pk/css/li-scroller.css

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

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

▶ GET http://ocsp.digicert.com/

Risk=Low, Confidence=Medium (6)

https://digibop.com.pk (1)

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

▶ GET https://digibop.com.pk/apps/OnlineBanking/

https://www.bop.com.pk (4)

Cookie No HttpOnly Flag (1)

▶ GET https://www.bop.com.pk/

Cookie Without Secure Flag (1)

▶ GET https://www.bop.com.pk/

Cookie without SameSite Attribute (1)

▶ GET https://www.bop.com.pk/

Information Disclosure - Debug Error Messages (1)

▶ GET https://www.bop.com.pk/Documents/Islamic%20Banking/Profit%2520Rates%2520May%25202013-1.pdf

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

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

▶ GET http://ocsp.digicert.com/

Risk=Low, Confidence=Low (1)

https://digibop.com.pk (1)

Timestamp Disclosure - Unix (1)

▶ GET https://digibop.com.pk/apps/OnlineBanking/1075331552/desktopweb/lib/fw.js

Risk=Informational, Confidence=Medium (2)

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

Modern Web Application (1)

▶ GET https://www.bop.com.pk/js/jquery1.1.js

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

Retrieved from Cache (1)

▶ GET http://ocsp.digicert.com/

Risk=Informational, Confidence=Low (4)

https://www.bop.com.pk (4)

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.bop.com.pk/js/respond.min.js

Loosely Scoped Cookie (1)

▶ GET https://www.bop.com.pk/

Re-examine Cache-control Directives (1)

▶ GET https://www.bop.com.pk/_Incapsula_Resource?SWKMTFSR=1&e=0.37506779572478777

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

▶ POST https://www.bop.com.pk/BoP

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

Application Error Disclosure

Source	raised by a passive scanner (Application Error Disclosure)
CWE ID	200
WASC ID	13

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/fundamentals/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/

Cross-Domain Misconfiguration

Source raised by a passive scanner (Cross-Domain Misconfiguration)

CWE ID 264

WASC ID 14

Reference

- https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

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://github.com/jquery/jquery/issues/2432 ▪ http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ ▪ http://research.insecurelabs.org/jquery/test/ ▪ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ ▪ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 ▪ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 ▪ https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b ▪ https://bugs.jquery.com/ticket/11974

- https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

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 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

Information Disclosure - Debug Error Messages

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

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

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

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

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

Information Disclosure - Suspicious Comments

Source raised by a passive scanner (Information Disclosure - Suspicious Comments)

CWE ID 200

WASC ID 13

Loosely Scoped Cookie

Source raised by a passive scanner (Loosely Scoped Cookie)

CWE ID 565

WASC ID 15

Reference

- https://tools.ietf.org/html/rfc6265#section-4.1
- 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
- http://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies

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