PICICBank-Scan-Report

Generated with ZAP on Tue 13 Dec 2022, at 15:54:40

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.icicibank.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%)	4 (21.1%)	2 (10.5%)	1 (5.3%)	7 (36.8%)
	Low	0 (0.0%)	2 (10.5%)	6 (31.6%)	1 (5.3%)	9 (47.4%)
	Informational	0 (0.0%)	0 (0.0%)	1 (5.3%)	2 (10.5%)	3 (15.8%)
	Total	0 (0.0%)	6 (31.6%)	9 (47.4%)	4 (21.1%)	19 (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.icicibank.com	0 (0)	7 (7)	9 (16)	3 (19)

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	130 (684.2%)
CSP: Wildcard Directive	Medium	253 (1,331.6%)
CSP: script-src unsafe-inline	Medium	253 (1,331.6%)
CSP: style-src unsafe-inline	Medium	253 (1,331.6%)
Content Security Policy (CSP) Header Not Set	Medium	2 (10.5%)
Total		19

Alert type	Risk	Count
Missing Anti-clickjacking Header	Medium	2 (10.5%)
Vulnerable JS Library	Medium	1 (5.3%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	6 (31.6%)
CSP: Notices	Low	8 (42.1%)
Cookie Without Secure Flag	Low	1 (5.3%)
Cookie without SameSite Attribute	Low	1 (5.3%)
Cross-Domain JavaScript Source File Inclusion	Low	532 (2,800.0%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	249 (1,310.5%)
Strict-Transport-Security Header Not Set	Low	2 (10.5%)
Timestamp Disclosure - Unix	Low	1510 (7,947.4%)
X-Content-Type-Options Header Missing	Low	2 (10.5%)
Information Disclosure - Suspicious Comments	Informational	67 (352.6%)
Total		19

Alert type	Risk	Count
Modern Web Application	Informational	245 (1,289.5%)
Re-examine Cache-control Directives	Informational	11 (57.9%)
Total		19

Alerts

Risk=Medium, Confidence=High (4)

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

CSP: Wildcard Directive (1)

▶ GET https://www.icicibank.com/

CSP: script-src unsafe-inline (1)

▶ GET https://www.icicibank.com/

CSP: style-src unsafe-inline (1)

▶ GET https://www.icicibank.com/

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

▶ GET https://www.icicibank.com/Personal-Banking/offers/offer-detail.page%3Fid%3Doffer-pepperfry-offer-20141107165424255.page

Risk=Medium, Confidence=Medium (2)

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

Missing Anti-clickjacking Header (1)

▶ GET https://www.icicibank.com/Personal-Banking/offers/offer-detail.page%3Fid%3Doffer-pepperfry-offer-20141107165424255.page

Vulnerable JS Library (1)

▶ GET https://www.icicibank.com/mobile-banking/imobile-pay.page?ITM=nli_cms_MOBILE_imobile_pay_app_topnavigation

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.icicibank.com/

Risk=Low, Confidence=High (2)

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

CSP: Notices (1)

▶ GET https://www.icicibank.com/

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.icicibank.com/Personal-Banking/offers/offer-detail.page%3Fid%3Doffer-pepperfry-offer-20141107165424255.page

Risk=Low, Confidence=Medium (6)

https://www.icicibank.com (6)

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

▶ GET https://www.icicibank.com/aboutus/academia-partnership/e-learning.page

Cookie Without Secure Flag (1)

▶ GET https://www.icicibank.com/Important-Notice-b2.page

Cookie without SameSite Attribute (1)

▶ GET https://www.icicibank.com/Important-Notice-b2.page

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.icicibank.com/

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

▶ GET https://www.icicibank.com/robots.txt

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

▶ GET https://www.icicibank.com/Personal-Banking/offers/offer-detail.page%3Fid%3Doffer-pepperfry-offer-20141107165424255.page

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

▶ GET https://www.icicibank.com/robots.txt

Risk=Informational, Confidence=Medium (1)

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

Modern Web Application (1)

▶ GET https://www.icicibank.com/aboutus/archive/usdmarch311997.html

Risk=Informational, Confidence=Low (2)

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

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.icicibank.com/

Re-examine Cache-control Directives (1)

▶ GET https://www.icicibank.com/robots.txt

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

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+p

olicy

- 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/

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/

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

CSP: Notices

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

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

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

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/