ICBCBank-Scan-Report

Generated with ZAP on Tue 13 Dec 2022, at 17:58:53

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.icbc.com.cn
- https://www.icbc.com.cn

(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 (4.3%)	0 (0.0%)	0 (0.0%)	1 (4.3%)
	Medium	0 (0.0%)	1 (4.3%)	5 (21.7%)	1 (4.3%)	7 (30.4%)
	Low	0 (0.0%)	2 (8.7%)	6 (26.1%)	1 (4.3%)	9 (39.1%)
	Informational	0 (0.0%)	0 (0.0%)	2 (8.7%)	4 (17.4%)	6 (26.1%)
	Total	0 (0.0%)	4 (17.4%)	13 (56.5%)	6 (26.1%)	23 (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.icbc.com.cn	1 (1)	7 (8)	9 (17)	6 (23)

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	17 (73.9%)
Absence of Anti-CSRF Tokens	Medium	2262 (9,834.8%)
Content Security Policy (CSP) Header Not Set	Medium	3888 (16,904.3%)
Cross-Domain Misconfiguration	Medium	88 (382.6%)
Total		23

Alert type	Risk	Count
Potential IP Addresses Found in the Viewstate	Medium	2236 (9,721.7%)
Secure Pages Include Mixed Content (Including Scripts)	Medium	124 (539.1%)
Vulnerable JS Library	Medium	20 (87.0%)
X-Frame-Options Setting Malformed	Medium	2724 (11,843.5%)
Cookie without SameSite Attribute	Low	2 (8.7%)
Cross-Domain JavaScript Source File Inclusion	Low	4 (17.4%)
Information Disclosure - Debug Error Messages	Low	1 (4.3%)
Secure Pages Include Mixed Content	Low	1257 (5,465.2%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	26 (113.0%)
Strict-Transport-Security Header Not Set	Low	4807 (20,900.0%)
Timestamp Disclosure - Unix	Low	13 (56.5%)
X-AspNet-Version Response Header	Low	26 (113.0%)
Total		23

Alert type	Risk	Count
X-Content-Type-Options Header Missing	Low	3947 (17,160.9%)
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	1 (4.3%)
Information Disclosure - Suspicious Comments	Informational	930 (4,043.5%)
Modern Web Application	Informational	2523 (10,969.6%)
Re-examine Cache-control Directives	Informational	2543 (11,056.5%)
Retrieved from Cache	Informational	46 (200.0%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	10 (43.5%)
Total		23

Alerts

Risk=High, Confidence=High (1)

https://www.icbc.com.cn (1)

PII Disclosure (1)

▶ GET
https://www.icbc.com.cn/ICBC/%E9%87%91%E8%9E%8D%E4%BF%A1%E6%81%AF

/%E5%AD%98%E8%B4%B7%E6%AC%BE%E5%88%A9%E7%8E%87%E8%A1%A8/%E4%BA%BA%E6%B0%91%E5%B8%81%E8%B4%B7%E6%AC%BE%E5%88%A9%E7%8E%87%E8%A1%A8/default.htm

Risk=Medium, Confidence=High (1)

https://www.icbc.com.cn (1)

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

▶ GET https://www.icbc.com.cn/robots.txt

Risk=Medium, Confidence=Medium (5)

https://www.icbc.com.cn (5)

Cross-Domain Misconfiguration (1)

▶ GET https://www.icbc.com.cn/Portal_Resources/css/page/main.css

Potential IP Addresses Found in the Viewstate (1)

▶ GET https://www.icbc.com.cn/column/1438058343720960888.html

Secure Pages Include Mixed Content (Including Scripts) (1)

▶ GET https://www.icbc.com.cn/ICBC/%E7%89%A1%E4%B8%B9%E5%8D%A1/%E8%B4%B4%E5%BF%83%E6%9C%8D%E5%8A%A1/default.htm

Vulnerable JS Library (1)

▶ GET https://www.icbc.com.cn/Portal_Resources/Common/jquery/jquery-ui-1.9.2.autocomplete.js

X-Frame-Options Setting Malformed (1)

▶ GET https://www.icbc.com.cn/icbc/en/

Risk=Medium, Confidence=Low (1)

https://www.icbc.com.cn (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.icbc.com.cn/column/1438058343720960888.html

Risk=Low, Confidence=High (2)

https://www.icbc.com.cn (2)

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.icbc.com.cn/robots.txt

X-AspNet-Version Response Header (1)

▶ GET
https://www.icbc.com.cn/ICBCCOLLEGE/client/page/PageShow.aspx

Risk=Low, Confidence=Medium (6)

https://www.icbc.com.cn (6)

Cookie without SameSite Attribute (1)

▶ GET
https://www.icbc.com.cn/ICBCCOLLEGE/client/page/PageShow.aspx

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.icbc.com.cn/ICBC/%E9%87%91%E8%9E%8D%E4%BF%A1%E6%81%AF/%E8%A1%8C%E6%83%85%E6%95%B0%E6%8D%AE/%E9%9B%86%E5%90%88%E8%AE%A1%E5%88%92%E5%87%80%E5%80%BC/

Information Disclosure - Debug Error Messages (1)

▶ GET https://www.icbc.com.cn/ICBC/EN/PersonalFinance/PersonalLoan/PaymentMethodandService/

Secure Pages Include Mixed Content (1)

▶ GET https://www.icbc.com.cn/icbc/en/

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

▶ GET https://www.icbc.com.cn/ICBCCOLLEGE/client/page/PageShow.aspx

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

▶ GET https://www.icbc.com.cn/column/1438058343720960888.html

Risk=Low, Confidence=Low (1)

https://www.icbc.com.cn (1)

Timestamp Disclosure - Unix (1)

▶ GET https://www.icbc.com.cn/ICBC/%E9%87%91%E8%9E%8D%E4%BF%A1%E6%81%AF/%E5%AD%98%E8%B4%B7%E6%AC%BE%E5%88%A9%E7%8E%87%E8%A1%A8/%E4%BA%BA%E6%B0%91%E5%B8%81%E8%B4%B7%E6%AC%BE%E5%88%A9%E7%8E%87%E8%A1%A8/default.htm

Risk=Informational, Confidence=Medium (2)

https://www.icbc.com.cn (2)

Modern Web Application (1)

▶ GET https://www.icbc.com.cn/robots.txt

Retrieved from Cache (1)

▶ GET
https://www.icbc.com.cn/Portal_Resources/js/util/polyfill.js

Risk=Informational, Confidence=Low (4)

https://www.icbc.com.cn (4)

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

▶ GET
https://www.icbc.com.cn/ICBCCollege/client/page/CatalogDetail.aspx?CatelogID=633717554914092671&flagParent=false

Information Disclosure - Suspicious Comments (1)

▶ GET
https://www.icbc.com.cn/ICBC/%E4%B8%AA%E4%BA%BA%E9%87%91%E8%9E%8D/default.htm

Re-examine Cache-control Directives (1)

▶ GET https://www.icbc.com.cn/column/1438058343720960888.html

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

```
▶ GET https://www.icbc.com.cn/deposit/personal/index.html?type=0
```

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/

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

Potential IP Addresses Found in the Viewstate

Source	raised by a passive scanner (Viewstate)
CWE ID	642
WASC ID	14

Secure Pages Include Mixed Content (Including Scripts)

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

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829
Reference	▪ https://bugs.jqueryui.com/ticket/15284 ▪ https://nvd.nist.gov/vuln/detail/CVE-2022-31160

- https://github.com/jquery/jquery-ui/security/advisories/GHSA-h6gj-6jjq-h8g9
- https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327
- https://nvd.nist.gov/vuln/detail/CVE-2021-41184
- https://nvd.nist.gov/vuln/detail/CVE-2021-41183
- https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc
- https://nvd.nist.gov/vuln/detail/CVE-2021-41182

X-Frame-Options Setting Malformed

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	• https://tools.ietf.org/html/rfc7034#section-2.1

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-AspNet-Version Response Header

Source	raised by a passive scanner (X-AspNet-Version Response Header)
CWE ID	933
WASC ID	14
Reference	- https://www.troyhunt.com/shhh-dont-let-your-response-headers/ - https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/

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

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