AJKBank-Scan-Report

Generated with ZAP on Sun 4 Dec 2022, at 21:04:31

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.bankajk.com
- https://www.bankajk.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%)	1 (4.8%)	1 (4.8%)	0 (0.0%)	2 (9.5%)
	Medium	0 (0.0%)	1 (4.8%)	5 (23.8%)	1 (4.8%)	7 (33.3%)
	Low	0 (0.0%)	1 (4.8%)	6 (28.6%)	0 (0.0%)	7 (33.3%)
	Informational	0 (0.0%)	0 (0.0%)	3 (14.3%)	2 (9.5%)	5 (23.8%)
	Total	0 (0.0%)	3 (14.3%)	15 (71.4%)	3 (14.3%)	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.bankajk.com	2 (2)	7 (9)	7 (16)	5 (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	1 (4.8%)
PII Disclosure	High	8 (38.1%)
Absence of Anti-CSRF Tokens	Medium	32 (152.4%)
Content Security Policy (CSP) Header Not Set	Medium	164 (781.0%)
Total		21

Alert type	Risk	Count
HTTPS to HTTP Insecure Transition in Form Post	Medium	30 (142.9%)
Missing Anti-clickjacking Header	Medium	113 (538.1%)
Secure Pages Include Mixed Content (Including Scripts)	Medium	1 (4.8%)
Vulnerable JS Library	Medium	3 (14.3%)
X-Frame-Options Defined via META (Non-compliant with Spec)	Medium	97 (461.9%)
Cookie No HttpOnly Flag	Low	1 (4.8%)
Cookie Without Secure Flag	Low	1 (4.8%)
Cookie without SameSite Attribute	Low	1 (4.8%)
Cross-Domain JavaScript Source File Inclusion	Low	33 (157.1%)
Secure Pages Include Mixed Content	Low	29 (138.1%)
Strict-Transport-Security Header Not Set	Low	609 (2,900.0%)
X-Content-Type-Options Header Missing	Low	560 (2,666.7%)
Total		21

Alert type	Risk	Count
Content-Type Header Missing	Informational	1 (4.8%)
Information Disclosure - Suspicious Comments	Informational	254 (1,209.5%)
Modern Web Application	Informational	50 (238.1%)
Re-examine Cache-control Directives	Informational	113 (538.1%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	5 (23.8%)
Total		21

Alerts

Risk=High, Confidence=High (1)

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

PII Disclosure (1)

▶ GET https://www.bankajk.com/downloads/Officer%20Litigation%20(Final)Ammended%20Oct%2020.pdf

Risk=High, Confidence=Medium (1)

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

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

▶ GET https://www.bankajk.com/downloads/Pre-Qualification%20Notice%20for%20life%20and%20General%20Insurance%20Companies.pdf

Risk=Medium, Confidence=High (1)

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

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

▶ GET https://www.bankajk.com/nogooglebot/

Risk=Medium, Confidence=Medium (5)

https://www.bankajk.com (5)

HTTPS to HTTP Insecure Transition in Form Post (1)

▶ GET https://www.bankajk.com/

Missing Anti-clickjacking Header (1)

▶ GET https://www.bankajk.com/

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

▶ GET https://www.bankajk.com/bod.php

Vulnerable JS Library (1)

▶ GET https://www.bankajk.com/js/jquery.min.js

X-Frame-Options Defined via META (Non-compliant with Spec) (1)

▶ GET https://www.bankajk.com/

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.bankajk.com/

Risk=Low, Confidence=High (1)

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

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.bankajk.com/nogooglebot/

Risk=Low, Confidence=Medium (6)

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

Cookie No HttpOnly Flag (1)

▶ GET https://www.bankajk.com/contact/contact.php

Cookie Without Secure Flag (1)

▶ GET https://www.bankajk.com/contact/contact.php

Cookie without SameSite Attribute (1)

▶ GET https://www.bankajk.com/contact/contact.php

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.bankajk.com/

Secure Pages Include Mixed Content (1)

▶ GET https://www.bankajk.com/

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

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

Risk=Informational, Confidence=Medium (3)

https://www.bankajk.com (3)

Content-Type Header Missing (1)

▶ GET https://www.bankajk.com/css/style.scss

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.bankajk.com/

Modern Web Application (1)

▶ GET https://www.bankajk.com/

Risk=Informational, Confidence=Low (2)

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

Re-examine Cache-control Directives (1)

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

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

▶ POST https://www.bankajk.com/contact/contact.php

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/

HTTPS to HTTP Insecure Transition in Form Post

Source	raised by a passive scanner (HTTPS to HTTP Insecure Transition in Form Post)
CWE ID	319
WASC ID	15

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

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://nvd.nist.gov/vuln/detail/CVE-2012-6708
- https://github.com/jquery/jquery/issues/2432
- http://research.insecurelabs.org/jquery/test/
- http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/
- http://bugs.jquery.com/ticket/11290
- 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/

X-Frame-Options Defined via META (Non-compliant with Spec)

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	- https://tools.ietf.org/html/rfc7034#section-4

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

Cross-Domain JavaScript Source File Inclusion

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

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

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

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

Content-Type Header Missing

Source	raised by a passive scanner (Content-Type Header Missing)
CWE ID	345
WASC ID	12
Reference	▪ http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx

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/

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