KASBBank-Scan-Report

Generated with ZAP on Tue 6 Dec 2022, at 19:26:28

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://web.archive.org`
- `https://web.archive.org`
- `https://kasb.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 (4.3%)	0 (0.0%)	0 (0.0%)	1 (4.3%)
	Medium	0 (0.0%)	4 (17.4%)	3 (13.0%)	1 (4.3%)	8 (34.8%)
	Low	0 (0.0%)	2 (8.7%)	5 (21.7%)	1 (4.3%)	8 (34.8%)
	Informational	0 (0.0%)	0 (0.0%)	2 (8.7%)	4 (17.4%)	6 (26.1%)
	Total	0 (0.0%)	7 (30.4%)	10 (43.5%)	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://web.archive.org	0 (0)	4 (4)	2 (6)	2 (8)
	https://kasb.com	1 (1)	4 (5)	6 (11)	4 (15)

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	5 (21.7%)
Absence of Anti-CSRF Tokens	Medium	934 (4,060.9%)
Total		23

Alert type	Risk	Count
CSP: Wildcard Directive	Medium	81 (352.2%)
CSP: script-src unsafe-inline	Medium	81 (352.2%)
CSP: style-src unsafe-inline	Medium	81 (352.2%)
Content Security Policy (CSP) Header Not Set	Medium	2125 (9,239.1%)
Missing Anti-clickjacking Header	Medium	577 (2,508.7%)
Secure Pages Include Mixed Content (Including Scripts)	Medium	1556 (6,765.2%)
Vulnerable JS Library	Medium	1 (4.3%)
Cookie No HttpOnly Flag	Low	1824 (7,930.4%)
Cross-Domain JavaScript Source File Inclusion	Low	3052 (13,269.6%)
Information Disclosure - Debug Error Messages	Low	4 (17.4%)
Secure Pages Include Mixed Content	Low	1 (4.3%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	901 (3,917.4%)
Total		23

Alert type	Risk	Count
Strict-Transport-Security Header Not Set	Low	2904 (12,626.1%)
Timestamp Disclosure - Unix	Low	7477 (32,508.7%)
X-Content-Type-Options Header Missing	Low	1232 (5,356.5%)
Charset Mismatch	Informational	65 (282.6%)
Information Disclosure - Sensitive Information in URL	Informational	14 (60.9%)
Information Disclosure - Suspicious Comments	Informational	3404 (14,800.0%)
Modern Web Application	Informational	652 (2,834.8%)
Re-examine Cache-control Directives	Informational	954 (4,147.8%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	18 (78.3%)
Total		23

Alerts

Risk=High, Confidence=High (1)

https://kasb.com (1)

PII Disclosure (1)

▶ GET https://kasb.com/wp-content/plugins/elementor-pro/assets/js/elements-handlers.min.js?ver=3.5.2

Risk=Medium, Confidence=High (4)

https://web.archive.org (3)

CSP: Wildcard Directive (1)

▶ GET https://web.archive.org/web/20111118144437/http://www.kasb.com/bank/deposit_accounts.aspx?expandable=0&subexpandable=0

CSP: script-src unsafe-inline (1)

▶ GET https://web.archive.org/web/20111118144437/http://www.kasb.com/bank/deposit_accounts.aspx?expandable=0&subexpandable=0

CSP: style-src unsafe-inline (1)

▶ GET https://web.archive.org/web/20111118144437/http://www.kasb.com/bank/deposit_accounts.aspx?expandable=0&subexpandable=0

https://kasb.com (1)

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

▶ GET https://kasb.com/

Risk=Medium, Confidence=Medium (3)

https://web.archive.org (1)

Vulnerable JS Library (1)

▶ GET https://web.archive.org/web/20110713135441js_/http:/www.kasb.com/common/js/jquery.min.js

https://kasb.com (2)

Missing Anti-clickjacking Header (1)

▶ GET https://kasb.com/

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

▶ POST https://kasb.com/

Risk=Medium, Confidence=Low (1)

https://kasb.com (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://kasb.com/

Risk=Low, Confidence=High (2)

https://web.archive.org (1)

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

▶ GET https://web.archive.org/robots.txt

https://kasb.com (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://kasb.com/robots.txt

Risk=Low, Confidence=Medium (5)

https://web.archive.org (1)

Secure Pages Include Mixed Content (1)

▶ GET
https://web.archive.org/web/20220718064930/http:/sitemap.xml/

https://kasb.com (4)

Cookie No HttpOnly Flag (1)

▶ GET https://kasb.com/sitemap.xml

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://kasb.com/

Information Disclosure - Debug Error Messages (1)

▶ GET https://kasb.com/blog/tag/17-may/feed/

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

▶ GET https://kasb.com/robots.txt

Risk=Low, Confidence=Low (1)

https://kasb.com (1)

Timestamp Disclosure - Unix (1)

▶ GET https://kasb.com/sitemap.xml

Risk=Informational, Confidence=Medium (2)

https://web.archive.org (1)

Information Disclosure - Sensitive Information in URL (1)

▶ GET https://web.archive.org/web/20091127104838/http:/www.kasb.com:80/bank/deposit_accounts.aspx?amp;subexpandable=0&email=foo-bar%40example.com&expandable=0&first_name=ZAP&last_name=ZAP

https://kasb.com (1)

Modern Web Application (1)

▶ GET https://kasb.com/

Risk=Informational, Confidence=Low (4)

https://web.archive.org (1)

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

▶ POST https://web.archive.org/web/20111118144437/http:/www.kasb.com/bank/deposit_accounts.aspx?expandable=0&subexpandable=0

https://kasb.com (3)

Charset Mismatch (1)

▶ GET https://kasb.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fkasb.com%2F

Information Disclosure - Suspicious Comments (1)

▶ GET https://kasb.com/

Re-examine Cache-control Directives (1)

▶ GET https://kasb.com/robots.txt

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

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/

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 ▪ http://research.insecurelabs.org/jquery/test/ ▪ https://bugs.jquery.com/ticket/9521 ▪ 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://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b ▪ https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ ▪ https://nvd.nist.gov/vuln/detail/CVE-2011-4969

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

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 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

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

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 - Sensitive Information in URL

Source	raised by a passive scanner (Information Disclosure - Sensitive Information in URL)
CWE ID	200
WASC ID	13

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