BAFL-Scan-Report

Generated with ZAP on Sun 13 Nov 2022, at 14:30:53

Contents

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- `https://www.bankalfalah.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 (20.0%)	1 (5.0%)	1 (5.0%)	6 (30.0%)
	Low	0 (0.0%)	2 (10.0%)	7 (35.0%)	1 (5.0%)	10 (50.0%)
	Informational	0 (0.0%)	0 (0.0%)	1 (5.0%)	3 (15.0%)	4 (20.0%)
	Total	0 (0.0%)	6 (30.0%)	9 (45.0%)	5 (25.0%)	20 (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.bankalfalah.com	0 (0)	6 (6)	10 (16)	4 (20)

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	1134 (5,670.0%)
CSP: Wildcard Directive	Medium	350 (1,750.0%)
CSP: script-src unsafe-inline	Medium	350 (1,750.0%)
CSP: style-src unsafe-inline	Medium	350 (1,750.0%)
Content Security Policy (CSP) Header Not Set	Medium	2 (10.0%)
Total		20

Alert type	Risk	Count
Vulnerable JS Library	Medium	1 (5.0%)
Cookie No HttpOnly Flag	Low	4 (20.0%)
Cookie Without Secure Flag	Low	2 (10.0%)
Cookie with SameSite Attribute None	Low	2 (10.0%)
Cookie without SameSite Attribute	Low	352 (1,760.0%)
Cross-Domain JavaScript Source File Inclusion	Low	1582 (7,910.0%)
Information Disclosure - Debug Error Messages	Low	2 (10.0%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	2 (10.0%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	2 (10.0%)
Strict-Transport-Security Header Not Set	Low	2 (10.0%)
Timestamp Disclosure - Unix	Low	340 (1,700.0%)
Charset Mismatch	Informational	1 (5.0%)
Total		20

Alert type	Risk	Count
Information Disclosure - Suspicious Comments	Informational	595 (2,975.0%)
Modern Web Application	Informational	345 (1,725.0%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	5 (25.0%)
Total		20

Alerts

Risk=Medium, Confidence=High (4)

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

CSP: Wildcard Directive (1)

▶ GET https://www.bankalfalah.com

CSP: script-src unsafe-inline (1)

▶ GET https://www.bankalfalah.com

CSP: style-src unsafe-inline (1)

▶ GET https://www.bankalfalah.com

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

▶ GET https://www.bankalfalah.com/?_wp_http_referer=%2F%3F_wp_http_referer%3D%252Finvestor-relations%252Fcorporate-social-responsibility-reports%252F%26filter%3Dinfo%26s%3DZAP%26search_form_sitem%3Dff39415525&filter=info&s=ZAP&search_form_sitem=ff39415525

Risk=Medium, Confidence=Medium (1)

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

Vulnerable JS Library (1)

▶ GET https://www.bankalfalah.com/wp-content/themes/alfalah-theme/js/bootstrap.min.js

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.bankalfalah.com

Risk=Low, Confidence=High (2)

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

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

▶ GET https://www.bankalfalah.com/?_wp_http_referer=%2F%3F_wp_http_referer%3D%252Finvestor-relations%252Fcorporate-social-responsibility-reports%252F%26filter%3Dinfo%26s%3DZAP%26search_form_sitem%3Dff39415525&filter=info&s=ZAP&search_form_sitem=ff39415525

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.bankalfalah.com/?_wp_http_referer=%2F%3F_wp_http_referer%3D%252Finvestor-relations%252Fcorporate-social-responsibility-reports%252F%26filter%3Dinfo%26s%3DZAP%26search_form_sitem%3Dff39415525&filter=info&s=ZAP&search_form_site=4ef9a23d59

Risk=Low, Confidence=Medium (7)

https://www.bankalfalah.com (7)

Cookie No HttpOnly Flag (1)

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

Cookie Without Secure Flag (1)

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

Cookie with SameSite Attribute None (1)

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

Cookie without SameSite Attribute (1)

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

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.bankalfalah.com

Information Disclosure - Debug Error Messages (1)

▶ GET https://www.bankalfalah.com/personal-banking/loans/roshan-apna-ghar/

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

▶ GET https://www.bankalfalah.com/notice/click-here-to-watch-the-ceos-annual-review-message/

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

▶ GET https://www.bankalfalah.com

Risk=Informational, Confidence=Medium (1)

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

Modern Web Application (1)

▶ GET https://www.bankalfalah.com

Risk=Informational, Confidence=Low (3)

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

Charset Mismatch (1)

▶ GET https://www.bankalfalah.com/api/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fwww.bankalfalah.com%2F

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.bankalfalah.com

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

▶ `GET https://www.bankalfalah.com/?_wp_http_referer=%2F&s=ZAP&search_form_site=4ef9a23d59`

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+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/

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829
Reference	https://github.com/twbs/bootstrap/issues/28236 https://github.com/twbs/bootstrap/issues/20184 https://github.com/advisories/GHSA-4p24-vmcr-4gqj

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 with SameSite Attribute None

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

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

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

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

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 - 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)

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