

Faysalbank-Scan-Report

Generated with  ZAP on Wed 23 Nov 2022, at 17:49:20

Contents

- [About this report](#)
 - [Report parameters](#)
- [Summaries](#)
 - [Alert counts by risk and confidence](#)
 - [Alert counts by site and risk](#)
 - [Alert counts by alert type](#)
- [Alerts](#)
 - [Risk=High, Confidence=High \(1\)](#)
 - [Risk=High, Confidence=Medium \(1\)](#)
 - [Risk=Medium, Confidence=High \(1\)](#)
 - [Risk=Medium, Confidence=Medium \(2\)](#)
 - [Risk=Medium, Confidence=Low \(1\)](#)
 - [Risk=Low, Confidence=High \(1\)](#)
 - [Risk=Low, Confidence=Medium \(8\)](#)

- [Risk=Low, Confidence=Low \(1\)](#)
- [Risk=Informational, Confidence=Medium \(4\)](#)
- [Risk=Informational, Confidence=Low \(4\)](#)
- [Appendix](#)
 - [Alert types](#)

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.faysalbank.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				
Risk		User Confirmed	High	Medium	Low	Total
	High	0 (0.0%)	1 (4.2%)	1 (4.2%)	0 (0.0%)	2 (8.3%)
	Medium	0 (0.0%)	1 (4.2%)	2 (8.3%)	1 (4.2%)	4 (16.7%)
	Low	0 (0.0%)	1 (4.2%)	8 (33.3%)	1 (4.2%)	10 (41.7%)
	Informational	0 (0.0%)	0 (0.0%)	4 (16.7%)	4 (16.7%)	8 (33.3%)
	1					
Total		0 (0.0%)	3 (12.5%)	15 (62.5%)	6 (25.0%)	24 (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.)

Site	Risk			Informational
	High (= High)	Medium (>= Medium)	Low (>= Low)	(>= Informational)
https://www.faysalbank.com	2 (2)	4 (6)	10 (16)	8 (24)

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 (4.2%)
PII Disclosure	High	69 (287.5%)
Absence of Anti-CSRF Tokens	Medium	2364 (9,850.0%)
Total		24

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	3577 (14,904.2%)
Missing Anti-clickjacking Header	Medium	705 (2,937.5%)
Vulnerable JS Library	Medium	3 (12.5%)
Application Error Disclosure	Low	186 (775.0%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	535 (2,229.2%)
Cookie No HttpOnly Flag	Low	1262 (5,258.3%)
Cookie Without Secure Flag	Low	1262 (5,258.3%)
Cookie without SameSite Attribute	Low	1262 (5,258.3%)
Cross-Domain JavaScript Source File Inclusion	Low	2548 (10,616.7%)
Secure Pages Include Mixed Content	Low	28 (116.7%)
Strict-Transport-Security Header Not Set	Low	8 (33.3%)
Timestamp Disclosure - Unix	Low	31 (129.2%)
Total		24

Alert type	Risk	Count
X-Content-Type-Options Header Missing	Low	2197 (9,154.2%)
Charset Mismatch	Informational	100 (416.7%)
Content-Type Header Missing	Informational	3 (12.5%)
Information Disclosure - Sensitive Information in URL	Informational	1 (4.2%)
Information Disclosure - Suspicious Comments	Informational	1969 (8,204.2%)
Modern Web Application	Informational	1277 (5,320.8%)
Re-examine Cache-control Directives	Informational	419 (1,745.8%)
Retrieved from Cache	Informational	467 (1,945.8%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	462 (1,925.0%)
Total		24

Alerts

Risk=High, Confidence=High (1)

<https://www.faysalbank.com> (1)

PII Disclosure (1)

► GET <https://www.faysalbank.com/wp-content/uploads/2021/06/Faysal-Islami-Current-Account-PKR.pdf>

Risk=High, Confidence=Medium (1)

<https://www.faysalbank.com> (1)

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

► GET <https://www.faysalbank.com/wp-content/uploads/2022/11/Islamic-Personal-Finance-Legal-Agreement-Terms-Conditions.pdf>

Risk=Medium, Confidence=High (1)

<https://www.faysalbank.com> (1)

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

► GET <https://www.faysalbank.com/en/personal/loans/lending/faysal-flexi-credit/>

Risk=Medium, Confidence=Medium (2)

<https://www.faysalbank.com> (2)

Missing Anti-clickjacking Header (1)

► GET https://www.faysalbank.com

Vulnerable JS Library (1)

► GET https://www.faysalbank.com/wp-includes/js/jquery/ui/core.min.js?ver=1.12.1

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

► GET https://www.faysalbank.com

Risk=Low, Confidence=High (1)

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

Strict-Transport-Security Header Not Set (1)

► GET https://www.faysalbank.com/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js

Risk=Low, Confidence=Medium (8)

https://www.faysalbank.com (8)

Application Error Disclosure (1)

► GET https://www.faysalbank.com/en/about-us/

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

► GET https://www.faysalbank.com/author/admin/

Cookie No HttpOnly Flag (1)

► GET https://www.faysalbank.com/sitemap.xml

Cookie Without Secure Flag (1)

► GET https://www.faysalbank.com/sitemap.xml

Cookie without SameSite Attribute (1)

► GET https://www.faysalbank.com/sitemap.xml

Cross-Domain JavaScript Source File Inclusion (1)

► GET https://www.faysalbank.com

Secure Pages Include Mixed Content (1)

► GET https://www.faysalbank.com/priority/faysal-priority-centers-2/

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

► GET https://www.faysalbank.com/robots.txt

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

► GET https://www.faysalbank.com/wp-content/uploads/2018/12/STATMENT-OF-CHANGES-Urdu.pdf

Risk=Informational, Confidence=Medium (4)

<https://www.faysalbank.com> (4)

Content-Type Header Missing (1)

► GET <https://www.faysalbank.com/vid/fbl1.m4v>

Information Disclosure - Sensitive Information in URL (1)

► GET <https://www.faysalbank.com/wp-login.php?itsec-hb-token=fblcms18>

Modern Web Application (1)

► GET <https://www.faysalbank.com>

Retrieved from Cache (1)

► GET <https://www.faysalbank.com/robots.txt>

Risk=Informational, Confidence=Low (4)

<https://www.faysalbank.com> (4)

Charset Mismatch (1)

► GET <https://www.faysalbank.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fwww.faysalbank.com%2F>

Information Disclosure - Suspicious Comments (1)

► GET <https://www.faysalbank.com>

Re-examine Cache-control Directives (1)

► GET <https://www.faysalbank.com/robots.txt>

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

► GET https://www.faysalbank.com/en/personal/loans/?apply=view&inpage_id=9848

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	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ 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>

Application Error Disclosure

Source	raised by a passive scanner (Application Error Disclosure)
CWE ID	200
WASC ID	13

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

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	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection

Content-Type Header Missing

Source	raised by a passive scanner (Content-Type Header Missing)
CWE ID	345
WASC ID	12
Reference	<ul style="list-style-type: none">http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx

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	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ 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>