FirstWomenBank-Scan-Report

Generated with ZAP on Sat 3 Dec 2022, at 16:12:52

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.fwbl.com.pk`

(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 (6.2%)	0 (0.0%)	0 (0.0%)	1 (6.2%)
	Medium	0 (0.0%)	1 (6.2%)	2 (12.5%)	1 (6.2%)	4 (25.0%)
	Low	0 (0.0%)	0 (0.0%)	4 (25.0%)	1 (6.2%)	5 (31.2%)
	Informational	0 (0.0%)	1 (6.2%)	2 (12.5%)	3 (18.8%)	6 (37.5%)
	Total	0 (0.0%)	3 (18.8%)	8 (50.0%)	5 (31.2%)	16 (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	http://www.fwbl.com.pk	1 (1)	4 (5)	5 (10)	6 (16)

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	32 (200.0%)
Absence of Anti-CSRF Tokens	Medium	282 (1,762.5%)
Content Security Policy (CSP) Header Not Set	Medium	287 (1,793.8%)
Total		16

Alert type	Risk	Count
Missing Anti-clickjacking Header	Medium	252 (1,575.0%)
Vulnerable JS Library	Medium	3 (18.8%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	24 (150.0%)
Cross-Domain JavaScript Source File Inclusion	Low	565 (3,531.2%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	942 (5,887.5%)
Timestamp Disclosure - Unix	Low	63 (393.8%)
X-Content-Type-Options Header Missing	Low	947 (5,918.8%)
Charset Mismatch	Informational	118 (737.5%)
Content Security Policy (CSP) Report-Only Header Found	Informational	5 (31.2%)
Information Disclosure - Suspicious Comments	Informational	604 (3,775.0%)
Modern Web Application	Informational	37 (231.2%)
Retrieved from Cache	Informational	43 (268.8%)
Total		16

Alert type	Risk	Count
User Controllable HTML Element Attribute (Potential XSS)	Informational	1 (6.2%)
Total		16

Alerts

Risk=High, Confidence=High (1)

http://www.fwbl.com.pk (1)

PII Disclosure (1)

▶ GET http://www.fwbl.com.pk/wp-content/uploads/2012/prJun12.pdf

Risk=Medium, Confidence=High (1)

http://www.fwbl.com.pk (1)

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

▶ GET http://www.fwbl.com.pk/?doing_wp_cron=1670063663.3282430171966552734375

Risk=Medium, Confidence=Medium (2)

http://www.fwbl.com.pk (2)

Missing Anti-clickjacking Header (1)

▶ GET http://www.fwbl.com.pk/?doing_wp_cron=1670063663.3282430171966552734375

Vulnerable JS Library (1)

▶ GET http://www.fwbl.com.pk/wp-content/themes/fwb3/assets/js/jquery.tools.min.js

Risk=Medium, Confidence=Low (1)

http://www.fwbl.com.pk (1)

Absence of Anti-CSRF Tokens (1)

▶ GET http://www.fwbl.com.pk/?doing_wp_cron=1670063663.3282430171966552734375

Risk=Low, Confidence=Medium (4)

http://www.fwbl.com.pk (4)

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

▶ GET http://www.fwbl.com.pk/wp-content/themes/fwb3/assets/css/mainstyle.css

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET http://www.fwbl.com.pk/?doing_wp_cron=1670063663.3282430171966552734375

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

▶ GET http://www.fwbl.com.pk/?doing_wp_cron=1670063663.3282430171966552734375

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

▶ GET http://www.fwbl.com.pk/sitemap.xml

Risk=Low, Confidence=Low (1)

http://www.fwbl.com.pk (1)

Timestamp Disclosure - Unix (1)

▶ GET http://www.fwbl.com.pk/?doing_wp_cron=1670063663.3282430171966552734375

Risk=Informational, Confidence=High (1)

http://www.fwbl.com.pk (1)

Content Security Policy (CSP) Report-Only Header Found (1)

▶ GET http://www.fwbl.com.pk/ms-sakina-alam/

Risk=Informational, Confidence=Medium (2)

http://www.fwbl.com.pk (2)

Modern Web Application (1)

▶ GET http://www.fwbl.com.pk/?doing_wp_cron=1670063663.3282430171966552734375

Retrieved from Cache (1)

▶ GET http://www.fwbl.com.pk/wp-content/plugins/jquery-accordion/jquery/themes/base/ui.all.css

Risk=Informational, Confidence=Low (3)

http://www.fwbl.com.pk (3)

Charset Mismatch (1)

▶ GET http://www.fwbl.com.pk/wp-json/oembed/1.0/embed?format=xml&url=http%3A%2F%2Fwww.fwbl.com.pk%2Fbranch-network%2F

Information Disclosure - Suspicious Comments (1)

▶ GET http://www.fwbl.com.pk/?doing_wp_cron=1670063663.3282430171966552734375

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

▶ GET http://www.fwbl.com.pk/?s=Search...

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/

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

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

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

Cross-Domain JavaScript Source File Inclusion

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

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

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

Content Security Policy (CSP) Report-Only Header Found

Source	raised by a passive scanner (Content Security Policy (CSP) Header Not Set)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP2/ ▪ https://w3c.github.io/webappsec-csp/ ▪ http://caniuse.com/#feat=contentsecuritypolicy ▪ http://content-security-policy.com/

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)

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