ABL-Scan-Report

Generated with ZAP on Thu 10 Nov 2022, at 21:46:04

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.abl.com
- https://www.abl.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 (4.0%)	2 (8.0%)	0 (0.0%)	3 (12.0%)
	Medium	0 (0.0%)	1 (4.0%)	3 (12.0%)	1 (4.0%)	5 (20.0%)
	Low	0 (0.0%)	2 (8.0%)	7 (28.0%)	1 (4.0%)	10 (40.0%)
	Informational	0 (0.0%)	0 (0.0%)	3 (12.0%)	4 (16.0%)	7 (28.0%)
	Total	0 (0.0%)	4 (16.0%)	15 (60.0%)	6 (24.0%)	25 (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.abl.com	3 (3)	5 (8)	10 (18)	7 (25)

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
Big Redirect Detected (Potential Sensitive Information Leak)	High	1 (4.0%)
PII Disclosure	High	31 (124.0%)
Private IP Disclosure	High	1 (4.0%)
Total		25

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	17598 (70,392.0%)
Application Error Disclosure	Medium	1 (4.0%)
Content Security Policy (CSP) Header Not Set	Medium	5039 (20,156.0%)
Cross-Domain Misconfiguration	Medium	1603 (6,412.0%)
Vulnerable JS Library	Medium	3 (12.0%)
Application Error Disclosure	Low	526 (2,104.0%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	1 (4.0%)
CSP: X-Content-Security-Policy	Low	4896 (19,584.0%)
Cookie without SameSite Attribute	Low	4 (16.0%)
Cross-Domain JavaScript Source File Inclusion	Low	17202 (68,808.0%)
Private IP Disclosure	Low	2 (8.0%)
Secure Pages Include Mixed Content	Low	4 (16.0%)
Total		25

Alert type	Risk	Count
Strict-Transport-Security Header Not Set	Low	3657 (14,628.0%)
Timestamp Disclosure - Unix	Low	7993 (31,972.0%)
X-Content-Type-Options Header Missing	Low	6 (24.0%)
Charset Mismatch	Informational	573 (2,292.0%)
Information Disclosure - Sensitive Information in URL	Informational	4 (16.0%)
Information Disclosure - Suspicious Comments	Informational	10176 (40,704.0%)
Modern Web Application	Informational	5256 (21,024.0%)
Re-examine Cache-control Directives	Informational	83 (332.0%)
Retrieved from Cache	Informational	550 (2,200.0%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	4315 (17,260.0%)
Total		25

Alerts

Risk=High, Confidence=High (1)

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

PII Disclosure (1)

▶ GET https://www.abl.com/src/uploads/2019/04/Website-Compliance-Certificate-2019.pdf

Risk=High, Confidence=Medium (2)

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

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

▶ GET https://www.abl.com/?s

Private IP Disclosure (1)

▶ GET https://www.abl.com/src/uploads/2016/06/CNIC-Notice-Urdu.jpg

Risk=Medium, Confidence=High (1)

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

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

▶ GET https://www.abl.com/robots.txt

Risk=Medium, Confidence=Medium (3)

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

Application Error Disclosure (1)

▶ GET https://www.abl.com/download/financial_presentations_2/financial_presentations_2019/Investor-Presentation-For-The-Quarter-Ended-March-31-2019.pdf

Cross-Domain Misconfiguration (1)

▶ GET https://www.abl.com/wp-json/

Vulnerable JS Library (1)

▶ GET https://www.abl.com/wp-includes/js/jquery/ui/core.min.js

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.abl.com

Risk=Low, Confidence=High (2)

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

CSP: X-Content-Security-Policy (1)

▶ GET https://www.abl.com

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.abl.com/robots.txt

Risk=Low, Confidence=Medium (7)

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

Application Error Disclosure (1)

▶ GET https://www.abl.com/personal-banking/everyday-accounts/allied-express-account/account_open_form-2/

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

▶ GET https://www.abl.com/?lang=ur&s

Cookie without SameSite Attribute (1)

▶ GET https://www.abl.com/sitemap.xml

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.abl.com

Private IP Disclosure (1)

▶ GET https://www.abl.com/src/uploads/2016/06/Nov-20-urdu.jpg

Secure Pages Include Mixed Content (1)

▶ GET https://www.abl.com/personal-banking/theme-branches/women-banking/?lang=ur

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

▶ POST https://www.abl.com/cdn-cgi/challenge-platform/h/b/flow/ov1/0.582755073331258 8:1668093983:AsJy1VTyIz2LXpmY42CgJ0hALtt8ftMaO9evNUvTFbw/7680004b48b63bf5/27018d87135be01

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

▶ GET https://www.abl.com

Risk=Informational, Confidence=Medium (3)

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

Information Disclosure - Sensitive Information in URL (1)

▶ GET https://www.abl.com/?_wp_http_referer=%2Fdisclaimer%2Finfo%40abl.com&_wpnonce=810e4ba47d&s

Modern Web Application (1)

▶ GET https://www.abl.com

Retrieved from Cache (1)

▶ GET https://www.abl.com

Risk=Informational, Confidence=Low (4)

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

Charset Mismatch (1)

▶ GET https://www.abl.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fwww.abl.com%2Fservices%2Ffinancial-consumer-protection-framework%2F

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.abl.com

Re-examine Cache-control Directives (1)

▶ GET https://www.abl.com

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

▶ GET https://www.abl.com/?lang=ur

Appendix

Alert types

This section contains additional information on the types of alerts in the report.

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

PII Disclosure

Source	raised by a passive scanner (PII Disclosure)

CWE ID	359
WASC ID	13

Private IP Disclosure

Source	raised by a passive scanner (Private IP Disclosure)
CWE ID	200
WASC ID	13
Reference	▪ https://tools.ietf.org/html/rfc1918

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

Application Error Disclosure

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

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/

Cross-Domain Misconfiguration

Source	raised by a passive scanner (Cross-Domain Misconfiguration)
CWE ID	264

WASC ID 14

Reference
- https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Vulnerable JS Library

Source raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))

CWE ID 829

Reference
- 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

CSP: X-Content-Security-Policy

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

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

Private IP Disclosure

Source	raised by a passive scanner (Private IP Disclosure)
CWE ID	200
WASC ID	13
Reference	• https://tools.ietf.org/html/rfc1918

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

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/

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