ZAP by Checkmarx Scanning Report

Generated with ZAP on uto 16 pro 2025, at 19:13:31

ZAP Version: 2.17.0

ZAP by Checkmarx

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://xpaywalletcdn-prod.azureedge.net
- https://edge-mobile-static.azureedge.net
- https://edge-cloud-resource-static.azureedge.net
- https://edge-consumer-static.azureedge.net
- https://edgeassetservice.azureedge.net
- https://www.bing.com
- https://telem-edge.smartscreen.microsoft.com
- https://data-edge.smartscreen.microsoft.com
- http://localhost:4000
- https://nav-edge.smartscreen.microsoft.com
- https://www.googleapis.com
- https://edge.microsoft.com
- http://edge.microsoft.com
- https://plausible.io
- https://msedgedriver.microsoft.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 %)	2 (12,5 %)	1 (6,2 %)	0 (0,0 %)	3 (18,8 %)
	Low	0 (0,0 %)	3 (18,8 %)	6 (37,5 %)	1 (6,2 %)	10 (62,5 %)
	Informational	0 (0,0 %)	0 (0,0 %)	1 (6,2 %)	2 (12,5 %)	3 (18,8 %)

	Confidence				
	User Confirmed	High	Medium	Low	Total
Total	0 (0,0 %)	5 (31,2 %)	8 (50,0 %)	3 (18,8 %)	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	https://www.bing.com	0 (0)	0 (0)	5 (5)	2 (7)
	http://localhost:4000	0 (0)	2 (2)	0 (2)	0 (2)
	https://edge.microsoft.com	0 (0)	0 (0)	2 (2)	1 (3)
	https://plausible.io	0 (0)	1 (1)	1 (2)	0 (2)
	https://msedgedriver.microsoft.com	0 (0)	0 (0)	2 (2)	0 (2)

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
CSP: Wildcard Directive	Medium	1 (6,2 %)
CSP: style-src unsafe-inline	Medium	1 (6,2 %)
Cross-Domain Misconfiguration	Medium	5 (31,2 %)
Cookie No HttpOnly Flag	Low	1 (6,2 %)
Cookie Without Secure Flag	Low	3 (18,8 %)
Cookie with SameSite Attribute None	Low	1 (6,2 %)
Cookie without SameSite Attribute	Low	3 (18,8 %)
Private IP Disclosure	Low	1 (6,2 %)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	1 (6,2 %)
Strict-Transport-Security Disabled	Low	1 (6,2 %)
Total		16

Alert type	Risk	Count
Strict-Transport-Security Header Not Set	Low	25 (156,2 %)
Timestamp Disclosure - Unix	Low	7 (43,8 %)
X-Content-Type-Options Header Missing	Low	21 (131,2 %)
Loosely Scoped Cookie	Informational	1 (6,2 %)
Re-examine Cache-control Directives	Informational	8 (50,0 %)
Session Management Response Identified	Informational	1 (6,2 %)
Total		16

Insights

This table shows information that is likely to be very relevant to you, but which is not related to vulnerabilities, or potentially even related to the application in question.

Level	Reason	Site	Description	Statistic
Info	Informational	http://edge.microsoft.com	Percentage of responses with status code 4xx	100 %
Info	Informational	http://edge.microsoft.com	Percentage of endpoints with method GET	100 %

Level	Reason	Site	Description	Statistic
Info	Informational	http://edge.microsoft.com	Count of total endpoints	1
Info	Informational	http://localhost:4000	Percentage of responses with status code 2xx	100 %
Info	Informational	http://localhost:4000	Percentage of endpoints with content type text/html	100 %
Info	Informational	http://localhost:4000	Percentage of endpoints with method GET	100 %
Info	Informational	http://localhost:4000	Count of total endpoints	1
Info	Informational	https://data-edge.smartscreen.microsoft.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://data-edge.smartscreen.microsoft.com	Percentage of endpoints with content type application/octet-stream	100 %
Info	Informational	https://data-edge.smartscree	Percentage of endpoints with method POST	100 %

Level	Reason	Site	Description	Statistic
		n.microsoft.com		
Info	Informational	https://data-edge.smartscreen.microsoft.com	Count of total endpoints	2
Info	Informational	https://data-edge.smartscreen.microsoft.com	Percentage of slow responses	100 %
Info	Informational	https://edge-cloud-resource-static.azureedge.net	Percentage of responses with status code 2xx	100 %
Info	Informational	https://edge-cloud-resource-static.azureedge.net	Percentage of endpoints with content type application/json	100 %
Info	Informational	https://edge-cloud-resource-static.az	Percentage of endpoints with method GET	66 %

Level	Reason	Site	Description	Statistic
		ureedge.net		
Info	Informational	https://edge-cloud-resource-static.azureedge.net	Percentage of endpoints with method HEAD	33 %
Info	Informational	https://edge-cloud-resource-static.azureedge.net	Count of total endpoints	3
Info	Informational	https://edge-consumer-static.azureedge.net	Percentage of responses with status code 2xx	100 %
Info	Informational	https://edge-consumer-static.azureedge.net	Percentage of endpoints with content type application/json	100 %
Info	Informational	https://edge-consumer-	Percentage of endpoints with method GET	100 %

Level	Reason	Site	Description	Statistic
		static.azureedge.net		
Info	Informational	https://edge-consumer-static.azureedge.net	Count of total endpoints	1
Info	Informational	https://edge-consumer-static.azureedge.net	Percentage of slow responses	100 %
Info	Informational	https://edge-mobile-static.azureedge.net	Percentage of responses with status code 2xx	100 %
Info	Informational	https://edge-mobile-static.azureedge.net	Percentage of endpoints with content type application/json	100 %
Info	Informational	https://edge-mobile-static.azureedge.net	Percentage of endpoints with method GET	100 %

Level	Reason	Site	Description	Statistic
Info	Informational	https://edge-mobile-static.azureedge.net	Count of total endpoints	1
Info	Informational	https://edge-mobile-static.azureedge.net	Percentage of slow responses	100 %
Info	Informational	https://edge.microsoft.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://edge.microsoft.com	Percentage of endpoints with content type application/json	100 %
Info	Informational	https://edge.microsoft.com	Percentage of endpoints with method GET	50 %
Info	Informational	https://edge.microsoft.com	Percentage of endpoints with method POST	50 %
Info	Informational	https://edge.microsoft.com	Count of total endpoints	6
Info	Informational	https://edge.mi	Percentage of slow responses	4 %

Level	Reason	Site	Description	Statistic
		crosoft.com		
Info	Informational	https://edgeassetservice.azureedge.net	Percentage of responses with status code 2xx	100 %
Info	Informational	https://edgeassetservice.azureedge.net	Percentage of endpoints with content type application/octet-stream	100 %
Info	Informational	https://edgeassetservice.azureedge.net	Percentage of endpoints with method GET	100 %
Info	Informational	https://edgeassetservice.azureedge.net	Count of total endpoints	5
Info	Informational	https://edgeassetservice.azureedge.net	Percentage of slow responses	100 %
Info	Informational	https://msedgedriver.microsoft.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://msedge	Percentage of endpoints with	50 %

Level	Reason	Site	Description	Statistic
		driver.microsoft.com	content type application/octet-stream	
Info	Informational	https://msedgedriver.microsoft.com	Percentage of endpoints with content type application/x-zip-compressed	50 %
Info	Informational	https://msedgedriver.microsoft.com	Percentage of endpoints with method GET	100 %
Info	Informational	https://msedgedriver.microsoft.com	Count of total endpoints	2
Info	Informational	https://msedgedriver.microsoft.com	Percentage of slow responses	100 %
Info	Informational	https://nav-edge.smartscreen.microsoft.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://nav-edge.smartscreen.microsoft.com	Percentage of endpoints with content type application/json	100 %

Level	Reason	Site	Description	Statistic
Info	Informational	https://nav-edge.smartscreen.microsoft.com	Percentage of endpoints with method POST	100 %
Info	Informational	https://nav-edge.smartscreen.microsoft.com	Count of total endpoints	1
Info	Informational	https://nav-edge.smartscreen.microsoft.com	Percentage of slow responses	100 %
Info	Informational	https://plausible.io	Percentage of responses with status code 2xx	100 %
Info	Informational	https://plausible.io	Percentage of endpoints with content type text/plain	100 %
Info	Informational	https://plausible.io	Percentage of endpoints with method POST	100 %
Info	Informational	https://plausible.io	Count of total endpoints	1
Info	Informational	https://plausible.io	Percentage of slow responses	100 %

Level	Reason	Site	Description	Statistic
Info	Informational	https://telem-edge.smartscreen.microsoft.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://telem-edge.smartscreen.microsoft.com	Percentage of endpoints with method POST	100 %
Info	Informational	https://telem-edge.smartscreen.microsoft.com	Count of total endpoints	1
Info	Informational	https://telem-edge.smartscreen.microsoft.com	Percentage of slow responses	100 %
Info	Informational	https://www.bing.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://www.bing.com	Percentage of endpoints with content type application/json	100 %
Info	Informational	https://www.bing.com	Percentage of endpoints with method GET	100 %

Level	Reason	Site	Description	Statistic
Info	Informational	https://www.bing.com	Count of total endpoints	2
Info	Informational	https://www.bing.com	Percentage of slow responses	100 %
Info	Informational	https://www.googleapis.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://www.googleapis.com	Percentage of endpoints with content type application/json	100 %
Info	Informational	https://www.googleapis.com	Percentage of endpoints with method POST	100 %
Info	Informational	https://www.googleapis.com	Count of total endpoints	1
Info	Informational	https://www.googleapis.com	Percentage of slow responses	100 %
Info	Informational	https://xpaywalletcdn-prod.azureedge.net	Percentage of responses with status code 2xx	100 %

Level	Reason	Site	Description	Statistic
Info	Informational	https://xpaywalletcdn-prod.azureedge.net	Percentage of endpoints with content type text/plain	100 %
Info	Informational	https://xpaywalletcdn-prod.azureedge.net	Percentage of endpoints with method GET	100 %
Info	Informational	https://xpaywalletcdn-prod.azureedge.net	Count of total endpoints	1
Info	Informational	https://xpaywalletcdn-prod.azureedge.net	Percentage of slow responses	50 %

Alerts

Risk=Medium, Confidence=High (2)

http://localhost:4000 (2)

CSP: Wildcard Directive (1)

▶ GET http://localhost:4000/

CSP: style-src unsafe-inline (1)

▶ GET http://localhost:4000/

Risk=Medium, Confidence=Medium (1)

https://plausible.io (1)

Cross-Domain Misconfiguration (1)

▶ POST https://plausible.io/api/event

Risk=Low, Confidence=High (3)

https://edge.microsoft.com (1)

Strict-Transport-Security Disabled (1)

▶ GET
https://edge.microsoft.com/abusiveadblocking/api/v1/blocklist

https://plausible.io (1)

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

▶ POST https://plausible.io/api/event

https://msedgedriver.microsoft.com (1)

Strict-Transport-Security Header Not Set (1)

▶ GET
https://msedgedriver.microsoft.com/LATEST_RELEASE_143_WINDOWS

Risk=Low, Confidence=Medium (6)

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

Cookie No HttpOnly Flag (1)

▶ GET
https://www.bing.com/api/shopping/v1/user/shoppingsettings?EnabledServiceFeaturesv2=edgeServerUX.shopping.msEdgeShoppingCashbackDismissTimeout2s

Cookie Without Secure Flag (1)

▶ GET
https://www.bing.com/api/shopping/v1/user/shoppingsettings?EnabledServiceFeaturesv2=edgeServerUX.shopping.msEdgeShoppingCashbackDismissTimeout2s

Cookie with SameSite Attribute None (1)

▶ GET
https://www.bing.com/api/shopping/v1/user/shoppingsettings?EnabledServiceFeaturesv2=edgeServerUX.shopping.msEdgeShoppingCashbackDismissTimeout2s

Cookie without SameSite Attribute (1)

▶ GET
https://www.bing.com/api/shopping/v1/user/shoppingsettings?EnabledServiceFeaturesv2=edgeServerUX.shopping.msEdgeShoppingCashbackDismissTimeout2s

https://edge.microsoft.com (1)

Private IP Disclosure (1)

▶ POST
https://edge.microsoft.com/componentupdater/api/v1/update?cup2key=7:mzFdMxvyEDnoJR9zMCkHUwWPMX07VSFtJawelspks9Y&cup2hreq=217970704ac5c3489294a21dde554e6e2ee5203f41c8e8692e88335ebd3555e4

https://msedgedriver.microsoft.com (1)

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

▶ GET
https://msedgedriver.microsoft.com/LATEST_RELEASE_143_WINDOWS

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

▶ GET
https://www.bing.com/api/shopping/v1/user/shoppingsettings?EnabledServiceFeaturesv2=edgeServerUX.shopping.msEdgeShoppingCashbackDismissTimeout2s

Risk=Informational, Confidence=Medium (1)

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

Session Management Response Identified (1)

▶ GET
https://www.bing.com/api/shopping/v1/user/shoppingsettings?EnabledServiceFeaturesv2=edgeServerUX.shopping.msEdgeShoppingCashbackDismissTimeout2s

Risk=Informational, Confidence=Low (2)

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

Loosely Scoped Cookie (1)

▶ GET
https://www.bing.com/api/shopping/v1/user/shoppingsettings?EnabledServiceFeaturesv2=edgeServerUX.shopping.msEdgeShoppingCashbackDismissTimeout2s

https://edge.microsoft.com (1)

Re-examine Cache-control Directives (1)

▶ GET
https://edge.microsoft.com/entityextractiontemplates/api/v1/assets/find-assets?name=arbitration_priority_list&version=36.*.*&channel=stable&key=d414dd4f9db345fa8003e32adc81b362

Appendix

Alert Types

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

CSP: Wildcard Directive

Source	raised by a passive scanner (CSP)
CWE ID	693

WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://web.dev/articles/csp#resource-options

CSP: style-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://web.dev/articles/csp#resource-options

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?category=HTML5&subcategory=Overly%20Permissive%20CORS%20Policy

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://datatracker.ietf.org/doc/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://datatracker.ietf.org/doc/html/draft-ietf-httpbis-cookie-same-site

Private IP Disclosure

Source	raised by a passive scanner (Private IP Disclosure)
CWE ID	497
WASC ID	13
Reference	▪ https://datatracker.ietf.org/doc/html/rfc1918

Server Leaks Version Information via "Server" HTTP Response Header Field

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	497
WASC ID	13

Reference	▪ https://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) ▪ https://www.troyhunt.com/shhh-dont-let-your-response-headers/

Strict-Transport-Security Disabled

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15
Reference	▪ https://datatracker.ietf.org/doc/html/rfc6797#section-6.2

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

- https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
- https://caniuse.com/stricttransportsecurity
- https://datatracker.ietf.org/doc/html/rfc6797

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	497
WASC ID	13
Reference	- https://cwe.mitre.org/data/definitions/200.html

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	- https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) - https://owasp.org/www-community/Security_Headers

Loosely Scoped Cookie

Source	raised by a passive scanner (Loosely Scoped Cookie)
CWE ID	565
WASC ID	15
Reference	▪ https://datatracker.ietf.org/doc/html/rfc6265#section-4.1 ▪ 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 ▪ https://code.google.com/archive/p/browsersec/wikis/Part2.wiki

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/Reference/Headers/Cache-Control ▪ https://grayduck.mn/2021/09/13/cache-control-recommendations/

Session Management Response Identified

Source	raised by a passive scanner (Session Management Response Identified)
Reference	▪ https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id/