ZAP Scanning Report

Site: http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080

Generated on Sun, 13 Apr 2025 07:45:57

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	4
Informational	1
False Positives:	0

Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

Alerts

Name	Risk Level	Number of Instances
Application Error Disclosure	Low	1
Information Disclosure - Debug Error Messages	Low	1
Insufficient Site Isolation Against Spectre Vulnerability	Low	2
Unexpected Content-Type was returned	Low	7
Non-Storable Content	Informational	9

Alert Detail

Low	Application Error Disclosure
Description	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/pay_api/api/v1/payments/webhook
Method	POST

Parameter	
Attack	
Evidence	HTTP/1.1 500
Other Info	
Instances	1
Solution	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Reference	
CWE Id	550
WASC Id	13
Plugin Id	90022

Low	**Information Disclosure - Debug Error Messages**
Description	The response appeared to contain common error messages returned by platforms such as ASP.NET, and Web-servers such as IIS and Apache. You can configure the list of common debug messages.
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/pay_api/api/v1/payments/webhook
Method	POST
Parameter	
Attack	
Evidence	Internal Server Error
Other Info	
Instances	1
Solution	Disable debugging messages before pushing to production.
Reference	
CWE Id	1295
WASC Id	13
Plugin Id	10023

Low	**Insufficient Site Isolation Against Spectre Vulnerability**
Description	Cross-Origin-Resource-Policy header is an opt-in header designed to counter side-channels attacks like Spectre. Resource should be specifically set as shareable amongst different origins.
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/pay_api/api-docs
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/pay_api/api/v1/payments/ServiceStatus
Method	GET

Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
Instances	2
Solution	Ensure that the application/web server sets the Cross-Origin-Resource-Policy header appropriately, and that it sets the Cross-Origin-Resource-Policy header to 'same-origin' for all web pages. 'same-site' is considered as less secured and should be avoided. If resources must be shared, set the header to 'cross-origin'. If possible, ensure that the end user uses a standards-compliant and modern web browser that supports the Cross-Origin-Resource-Policy header (https://caniuse.com/mdn-http_headers_cross-origin-resource-policy).
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Cross-Origin_Resource_Policy
CWE Id	693
WASC Id	14
Plugin Id	90004

Low	**Unexpected Content-Type was returned**
Description	A Content-Type of text/html was returned by the server. This is not one of the types expected to be returned by an API. Raised by the 'Alert on Unexpected Content Types' script
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080
Method	GET
Parameter	
Attack	
Evidence	text/html
Other Info	
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/
Method	GET
Parameter	
Attack	
Evidence	text/html
Other Info	
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/5820472884515476146
Method	GET
Parameter	
Attack	
Evidence	text/html

Other Info	
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/computeMetadata/v1/
Method	POST
Parameter	
Attack	
Evidence	text/html
Other Info	
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/latest/meta-data/
Method	POST
Parameter	
Attack	
Evidence	text/html
Other Info	
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/metadata/instance
Method	POST
Parameter	
Attack	
Evidence	text/html
Other Info	
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/opc/v1/instance/
Method	POST
Parameter	
Attack	
Evidence	text/html
Other Info	
Instances	7
Solution	
Reference	
CWE Id	
WASC Id	
Plugin Id	100001

Informational	Non-Storable Content
Description	The response contents are not storable by caching components such as proxy servers. If the response does not contain sensitive, personal or user-specific information, it may benefit from being stored and cached, to improve performance.
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/pay_api/api-docs
Method	GET

Parameter	
Attack	
Evidence	no-store
Other Info	
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/pay_api/api/v1/payments/ServiceStatus
Method	GET
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/pay_api/api/v1/payments/CreatePaymentIntent
Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/pay_api/api/v1/payments/CreatePaymentIntentByNewCard
Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/pay_api/api/v1/payments/CreateSetupIntent
Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/pay_api/api/v1/payments/DeletePaymentMethod
Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/pay_api/api/v1/payments/FetchCustomerCards

Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/pay_api/api/v1/payments/Refund
Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/pay_api/api/v1/payments/webhook
Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
Instances	9
Solution	The content may be marked as storable by ensuring that the following conditions are satisfied: The request method must be understood by the cache and defined as being cacheable ("GET", "HEAD", and "POST" are currently defined as cacheable) The response status code must be understood by the cache (one of the 1XX, 2XX, 3XX, 4XX, or 5XX response classes are generally understood) The "no-store" cache directive must not appear in the request or response header fields For caching by "shared" caches such as "proxy" caches, the "private" response directive must not appear in the response For caching by "shared" caches such as "proxy" caches, the "Authorization" header field must not appear in the request, unless the response explicitly allows it (using one of the "must-revalidate", "public", or "s-maxage" Cache-Control response directives) In addition to the conditions above, at least one of the following conditions must also be satisfied by the response: It must contain an "Expires" header field It must contain a "max-age" response directive For "shared" caches such as "proxy" caches, it must contain a "s-maxage" response directive It must contain a "Cache Control Extension" that allows it to be cached It must have a status code that is defined as cacheable by default (200, 203, 204, 206, 300, 301, 404, 405, 410, 414, 501).
Reference	https://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html

CWE Id	524
WASC Id	13
Plugin Id	10049

Sequence Details

With the associated active scan results.