



# ZAP Scanning Report

Site: <http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080>

Generated on Sun, 13 Apr 2025 07:34:00

ZAP Version: 2.16.1

ZAP by [Checkmarx](#)

## Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	4
Informational	3
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
<a href="#">Application Error Disclosure</a>	Medium	1
<a href="#">Application Error Disclosure</a>	Low	5
<a href="#">Information Disclosure - Debug Error Messages</a>	Low	6
<a href="#">Insufficient Site Isolation Against Spectre Vulnerability</a>	Low	12
<a href="#">Unexpected Content-Type was returned</a>	Low	7
<a href="#">Authentication Request Identified</a>	Informational	2
<a href="#">Information Disclosure - Sensitive Information in URL</a>	Informational	2
<a href="#">Non-Storable Content</a>	Informational	14

## Alert Detail

Medium	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	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qz_gen_api/api/v1/validator/Validate">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qz_gen_api/api/v1/validator/Validate</a>
Method	POST
Parameter	
Attack	
Evidence	Internal Server Error
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	<a href="#">550</a>
WASC Id	13
Plugin Id	<a href="#">90022</a>

<b>Low</b>	<b>Application Error Disclosure</b>
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	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qz_gen_api/api/v1/auth/Register">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qz_gen_api/api/v1/auth/Register</a>
Method	POST
Parameter	
Attack	
Evidence	HTTP/1.1 500
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qz_gen_api/api/v1/auth/SendOtp">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qz_gen_api/api/v1/auth/SendOtp</a>
Method	POST
Parameter	
Attack	
Evidence	HTTP/1.1 500
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qz_gen_api/api/v1/otp/SendOtp">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qz_gen_api/api/v1/otp/SendOtp</a>
Method	POST
Parameter	
Attack	
Evidence	HTTP/1.1 500
Other Info	

URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/payments/webhook">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/payments/webhook</a>
Method	POST
Parameter	
Attack	
Evidence	HTTP/1.1 500
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/users/ChangePassword">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/users/ChangePassword</a>
Method	POST
Parameter	
Attack	
Evidence	HTTP/1.1 500
Other Info	
Instances	5
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	<a href="#">550</a>
WASC Id	13
Plugin Id	<a href="#">90022</a>

<b>Low</b>	<b>Information Disclosure - Debug Error Messages</b>
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	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/auth/Register">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/auth/Register</a>
Method	POST
Parameter	
Attack	
Evidence	Internal Server Error
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/auth/SendOtp">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/auth/SendOtp</a>
Method	POST
Parameter	
Attack	
Evidence	Internal Server Error
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/otp/SendOtp">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/otp/SendOtp</a>
Method	POST

Parameter	
Attack	
Evidence	Internal Server Error
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/payments/webhook">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/payments/webhook</a>
Method	POST
Parameter	
Attack	
Evidence	Internal Server Error
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/users/ChangePassword">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/users/ChangePassword</a>
Method	POST
Parameter	
Attack	
Evidence	Internal Server Error
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/validator/Validate">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/validator/Validate</a>
Method	POST
Parameter	
Attack	
Evidence	Internal Server Error
Other Info	
Instances	6
Solution	Disable debugging messages before pushing to production.
Reference	
CWE Id	<a href="#">1295</a>
WASC Id	13
Plugin Id	<a href="#">10023</a>

<b>Low</b>	<b>Insufficient Site Isolation Against Spectre Vulnerability</b>
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	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api-docs">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api-docs</a>
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	

Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/message/loadTest">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/message/loadTest</a>
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/tickets/ServiceStatus">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/tickets/ServiceStatus</a>
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/tickets/Test">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/tickets/Test</a>
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/users/AllUsers">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/users/AllUsers</a>
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/users/GetUsers">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/users/GetUsers</a>
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/auth/RefreshToken">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/auth/RefreshToken</a>
Method	POST
Parameter	Cross-Origin-Resource-Policy
Attack	

Evidence	
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/auth/ValidateOtp">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/auth/ValidateOtp</a>
Method	POST
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/message/send">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/message/send</a>
Method	POST
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/otp/ValidateOtp">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/otp/ValidateOtp</a>
Method	POST
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/users/Logout">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/users/Logout</a>
Method	POST
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/validator/Validate">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/validator/Validate</a>
Method	POST
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
Instances	12
Solution	<p>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.</p> <p>'same-site' is considered as less secured and should be avoided.</p>

	<p>If resources must be shared, set the header to 'cross-origin'.</p> <p>If possible, ensure that the end user uses a standards-compliant and modern web browser that supports the Cross-Origin-Resource-Policy header (<a href="https://caniuse.com/mdn-http_headers_cross-origin-resource-policy">https://caniuse.com/mdn-http_headers_cross-origin-resource-policy</a>).</p>
Reference	<a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Cross-Origin_Resource_Policy">https://developer.mozilla.org/en-US/docs/Web/HTTP/Cross-Origin_Resource_Policy</a>
CWE Id	<a href="#">693</a>
WASC Id	14
Plugin Id	<a href="#">90004</a>

<b>Low</b>	<b>Unexpected Content-Type was returned</b>
Description	<p>A Content-Type of text/html was returned by the server.</p> <p>This is not one of the types expected to be returned by an API.</p> <p>Raised by the 'Alert on Unexpected Content Types' script</p>
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080</a>
Method	GET
Parameter	
Attack	
Evidence	text/html
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/</a>
Method	GET
Parameter	
Attack	
Evidence	text/html
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/2836467806891330054">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/2836467806891330054</a>
Method	GET
Parameter	
Attack	
Evidence	text/html
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/computeMetadata/v1/">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/computeMetadata/v1/</a>
Method	POST
Parameter	
Attack	
Evidence	text/html
Other Info	

URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/latest/meta-data/">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/latest/meta-data/</a>
Method	POST
Parameter	
Attack	
Evidence	text/html
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/metadata/instance">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/metadata/instance</a>
Method	POST
Parameter	
Attack	
Evidence	text/html
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/opc/v1/instance/">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/opc/v1/instance/</a>
Method	POST
Parameter	
Attack	
Evidence	text/html
Other Info	
Instances	7
Solution	
Reference	
CWE Id	
WASC Id	
Plugin Id	<a href="#">100001</a>

Informational	Authentication Request Identified
Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qz_gen_api/api/v1/auth/Authenticate">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qz_gen_api/api/v1/auth/Authenticate</a>
Method	POST
Parameter	email
Attack	
Evidence	password
Other Info	userParam=email userValue=zaproxy@example.com passwordParam=password
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qz_gen_api/api/v1/users/ChangePassword">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qz_gen_api/api/v1/users/ChangePassword</a>
Method	POST



Parameter	email
Attack	
Evidence	confirmationPassword
Other Info	userParam=email userValue=zaproxy@example.com passwordParam=confirmationPassword
Instances	2
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	<a href="https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-reg-id/">https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-reg-id/</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">10111</a>

Informational	Information Disclosure - Sensitive Information in URL
Description	The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies. You can configure the list of strings for this check to add or remove values specific to your environment.
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/tickets/GetRefundTickets?email=zaproxy@example.com">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/tickets/GetRefundTickets?email=zaproxy@example.com</a>
Method	GET
Parameter	email
Attack	
Evidence	zaproxy@example.com
Other Info	The URL contains email address(es).
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/tickets/GetTickets?email=zaproxy@example.com">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/tickets/GetTickets?email=zaproxy@example.com</a>
Method	GET
Parameter	email
Attack	
Evidence	zaproxy@example.com
Other Info	The URL contains email address(es).
Instances	2
Solution	Do not pass sensitive information in URIs.
Reference	
CWE Id	<a href="#">598</a>
WASC Id	13
Plugin Id	<a href="#">10024</a>

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	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api-docs">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api-docs</a>
Method	GET

Parameter	
Attack	
Evidence	no-store
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/auth/ValidateOtp">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/auth/ValidateOtp</a>
Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/message/send">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/message/send</a>
Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/otp/SendOtp">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/otp/SendOtp</a>
Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/otp/ValidateOtp">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/otp/ValidateOtp</a>
Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/payments/CreatePaymentIntentByNewCard">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/payments/CreatePaymentIntentByNewCard</a>
Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/payments/FetchCustomerCards">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/payments/FetchCustomerCards</a>

Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/payments/Refund">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/payments/Refund</a>
Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/payments/webhook">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/payments/webhook</a>
Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/tickets/PurchaseTicket">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/tickets/PurchaseTicket</a>
Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/tickets/RefundTicket">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/tickets/RefundTicket</a>
Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/users/ChangePassword">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/users/ChangePassword</a>
Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	

URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/users/Logout">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/users/Logout</a>
Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	<a href="http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/validator/Validate">http://ad51f7dfa2b1d42dd8606642668f7db1-2123440888.ap-southeast-1.elb.amazonaws.com:8080/qr_gen_api/api/v1/validator/Validate</a>
Method	POST
Parameter	
Attack	
Evidence	no-store
Other Info	
Instances	14
Solution	<p>The content may be marked as storable by ensuring that the following conditions are satisfied:</p> <p>The request method must be understood by the cache and defined as being cacheable ("GET", "HEAD", and "POST" are currently defined as cacheable)</p> <p>The response status code must be understood by the cache (one of the 1XX, 2XX, 3XX, 4XX, or 5XX response classes are generally understood)</p> <p>The "no-store" cache directive must not appear in the request or response header fields</p> <p>For caching by "shared" caches such as "proxy" caches, the "private" response directive must not appear in the response</p> <p>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)</p> <p>In addition to the conditions above, at least one of the following conditions must also be satisfied by the response:</p> <p>It must contain an "Expires" header field</p> <p>It must contain a "max-age" response directive</p> <p>For "shared" caches such as "proxy" caches, it must contain a "s-maxage" response directive</p> <p>It must contain a "Cache Control Extension" that allows it to be cached</p> <p>It must have a status code that is defined as cacheable by default (200, 203, 204, 206, 300, 301, 404, 405, 410, 414, 501).</p>
Reference	<a href="https://datatracker.ietf.org/doc/html/rfc7234">https://datatracker.ietf.org/doc/html/rfc7234</a> <a href="https://datatracker.ietf.org/doc/html/rfc7231">https://datatracker.ietf.org/doc/html/rfc7231</a> <a href="https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html">https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html</a>
CWE Id	<a href="#">524</a>
WASC Id	13
Plugin Id	<a href="#">10049</a>

## Sequence Details

With the associated active scan results.

