segundo-relatorio

Site: https://cyqar4usf1.execute-api.us-east-1.amazonaws.com

Generated on Mon, 22 Jul 2024 23:09:24

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	2
Informational	2

Alerts

Name	Risk Level	Number of Instances
Strict-Transport-Security Header Not Set	Low	5
X-Content-Type-Options Header Missing	Low	3
Re-examine Cache-control Directives	Informational	3
Session Management Response Identified	Informational	4

Alert Detail

Low	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://cyqar4usf1.execute-api.us-east-1.amazonaws.com/api/order/c5b32001-300d-4ccc-98b4-682bdc20b033
Method	GET
Attack	
Evidence	
Other Info	
URL	https://cyqar4usf1.execute-api.us-east-1.amazonaws.com/api/products
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://cyqar4usf1.execute-api.us-east-1.amazonaws.com/api/order
Method	POST
Attack	
Evidence	
Other Info	
URL	https://cyqar4usf1.execute-api.us-east-1.amazonaws.com/api/order/c5b32001-300d-4ccc-98b4-682bdc20b033/pay
Method	POST
Attack	
Evidence	
Other Info	
URL	https://cyqar4usf1.execute-api.us-east-1.amazonaws.com/api/order/callback
Method	POST
Attack	
Evidence	
Other Info	
Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
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
CWE Id	319
WASC Id	15
Plugin Id	10035

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://cyqar4usf1.execute-api.us-east-1.amazonaws.com/api/order/c5b32001-300d-4ccc-98b4-682bdc20b033
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://cyqar4usf1.execute-api.us-east-1.amazonaws.com/api/products

Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://cyqar4usf1.execute-api.us-east-1.amazonaws.com/api/order
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	3
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
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
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	**Re-examine Cache-control Directives**
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://cyqar4usf1.execute-api.us-east-1.amazonaws.com/api/order/c5b32001-300d-4ccc-98b4-682bdc20b033
Method	GET
Attack	
Evidence	
Other Info	
URL	https://cyqar4usf1.execute-api.us-east-1.amazonaws.com/api/products
Method	GET
Attack	
Evidence	
Other Info	
URL	https://cyqar4usf1.execute-api.us-east-1.amazonaws.com/api/order
Method	POST
Attack	

Evidence	
Other Info	
Instances	3
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
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/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informational	**Session Management Response Identified**
Description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	https://cyqar4usf1.execute-api.us-east-1.amazonaws.com/api
Method	GET
Attack	
Evidence	D494496647D28D409A2F09C0865DEA3C
Other Info	cookie:JSESSIONID
URL	https://cyqar4usf1.execute-api.us-east-1.amazonaws.com/api/order/c5b32001-300d-4ccc-98b4-682bdc20b033
Method	GET
Attack	
Evidence	D494496647D28D409A2F09C0865DEA3C
Other Info	cookie:JSESSIONID
URL	https://cyqar4usf1.execute-api.us-east-1.amazonaws.com/api/order
Method	POST
Attack	
Evidence	D494496647D28D409A2F09C0865DEA3C
Other Info	cookie:JSESSIONID
URL	https://cyqar4usf1.execute-api.us-east-1.amazonaws.com/api/order/callback
Method	POST
Attack	
Evidence	D494496647D28D409A2F09C0865DEA3C
Other Info	cookie:JSESSIONID
Instances	4
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.

Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
CWE Id	
WASC Id	
Plugin Id	10112