ZAP Scanning Report

Site: http://soulmenu.api:8080

Generated on Sat, 7 Sep 2024 17:15:57

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	0
Informational	2
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
A Client Error response code was returned by the server	Informational	7
Non-Storable Content	Informational	1

Alert Detail

Informational	A Client Error response code was returned by the server
Description	A response code of 400 was returned by the server. This may indicate that the application is failing to handle unexpected input correctly. Raised by the 'Alert on HTTP Response Code Error' script
URL	http://soulmenu.api:8080
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 404
Other Info	
URL	http://soulmenu.api:8080/
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 404
Other Info	
URL	http://soulmenu.api:8080/7648618595035420219
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 404
Other Info	
URL	http://soulmenu.api:8080/actuator/health
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 404
Other Info	
URL	http://soulmenu.api:8080/itemMenu
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 400
Other Info	
URL	http://soulmenu.api:8080/itemMenu/
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 400
Other Info	
URL	http://soulmenu.api:8080/latest/meta-data/
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 404
Other Info	
Instances	7
Solution	
Reference	
CWE Id	388
WASC Id	20
Plugin Id	100000

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://soulmenu.api:8080/itemMenu
Method	GET
Parameter	
Attack	
Evidence	400
Other Info	
Instances	1
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