ZAP Scanning Report

Site: http://hermescontrol.api:8080

Generated on Sat, 7 Sep 2024 18:45:48

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
Storable and Cacheable Content	Informational	1

Alert Detail

Informational	A Client Error response code was returned by the server
Description	A response code of 404 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://hermescontrol.api:8080
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 404
Other Info	
URL	http://hermescontrol.api:8080/
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 404
Other Info	
URL	http://hermescontrol.api:8080/6957005391044271914
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 404
Other Info	
URL	http://hermescontrol.api:8080/actuator/health
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 404
Other Info	
URL	http://hermescontrol.api:8080/latest/meta-data/
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 404
Other Info	
URL	http://hermescontrol.api:8080/order
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 404
Other Info	
URL	http://hermescontrol.api:8080/order/
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	Storable and Cacheable Content
Description	The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to similar requests from other users. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where "shared" caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	http://hermescontrol.api:8080/order
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
Instances	1
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
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