ZAP Scanning Report

Sites: https://host.docker.internal:8080 http://host.docker.internal:8080

Generated on Mon, 28 Jul 2025 01:24:39

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	0
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
HTTP Only Site	Medium	1
Non-Storable Content	Informational	4

Alert Detail

Medium	HTTP Only Site
Description	The site is only served under HTTP and not HTTPS.
URL	http://host.docker.internal:8080
Method	GET
Parameter	
Attack	
Evidence	
Other Info	Failed to connect. ZAP attempted to connect via: https://host.docker.internal:8080

Instances	1
Solution	Configure your web or application server to use SSL (https).
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html https://letsencrypt.org/
CWE Id	311
WASC Id	4
Plugin Id	10106

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://host.docker.internal:8080
Method	GET
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	http://host.docker.internal:8080/
Method	GET
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	http://host.docker.internal:8080/robots.txt
Method	GET
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	http://host.docker.internal:8080/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	no-store
Other Info	
Instances	4
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.