ZAP Scanning Report

Site: http://host.docker.internal:3000

Generated on Sun, 20 Jul 2025 00:21:04

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	5
Informational	4
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
CSP: Failure to Define Directive with No Fallback	Medium	2
Content Security Policy (CSP) Header Not Set	Medium	1
Cross-Domain Misconfiguration	Medium	5
Missing Anti-clickjacking Header	Medium	1
Insufficient Site Isolation Against Spectre Vulnerability	Low	2
Permissions Policy Header Not Set	Low	4
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	5
Timestamp Disclosure - Unix	Low	20
X-Content-Type-Options Header Missing	Low	3
Information Disclosure - Suspicious Comments	Informational	1
Modern Web Application	Informational	1
Storable and Cacheable Content	Informational	4

Storable but Non-Cacheable Content	Informational	1

Alert Detail

Medium	**CSP: Failure to Define Directive with No Fallback**
Description	The Content Security Policy fails to define one of the directives that has no fallback. Missing/ excluding them is the same as allowing anything.
URL	http://host.docker.internal:3000/robots.txt
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://host.docker.internal:3000/sitemap.xml
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
Instances	2
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**Content Security Policy (CSP) Header Not Set**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	http://host.docker.internal:3000

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Cross-Domain Misconfiguration**
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
URL	http://host.docker.internal:3000
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://host.docker.internal:3000/logo.png
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some

	other form of security, such as IP address white-listing.
URL	http://host.docker.internal:3000/robots.txt
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://host.docker.internal:3000/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Instances	5
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
CWE Id	264
WASC Id	14

Plugin Id	10098

Medium **Missing Anti-clickjacking Header**

Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	http://host.docker.internal:3000
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
Instances	1
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Low **Insufficient Site Isolation Against Spectre Vulnerability**

Description	Cross-Origin-Embedder-Policy header is a response header that prevents a document from loading any cross-origin resources that don't explicitly grant the document permission (using CORP or CORS).
URL	http://host.docker.internal:3000
Method	GET
Parameter	Cross-Origin-Embedder-Policy
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000
Method	GET
Parameter	Cross-Origin-Opener-Policy
Attack	
Evidence	
Other Info	

Instances	2
Solution	Ensure that the application/web server sets the Cross-Origin-Embedder-Policy header appropriately, and that it sets the Cross-Origin-Embedder-Policy header to 'require-corp' for documents. If possible, ensure that the end user uses a standards-compliant and modern web browser that supports the Cross-Origin-Embedder-Policy header (https://caniuse.com/mdn-http_headers_cross-origin-embedder-policy).
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cross-Origin-Embedder-Policy
CWE Id	693
WASC Id	14
Plugin Id	90004

Low **Permissions Policy Header Not Set**

Description	Permissions Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Permissions Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
URL	http://host.docker.internal:3000
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
Instances	4
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Permissions-Policy https://developer.chrome.com/blog/feature-policy/ https://scotthelme.co.uk/a-new-security-header-feature-policy/ https://w3c.github.io/webappsec-feature-policy/ https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	693
WASC Id	15
Plugin Id	10063

Low	**Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
URL	http://host.docker.internal:3000
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://host.docker.internal:3000/logo.png
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://host.docker.internal:3000/robots.txt
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Express
Other Info	

URL	http://host.docker.internal:3000/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Express
Other Info	
Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	497
WASC Id	13
Plugin Id	10037

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	1444681467
Other Info	1444681467, which evaluates to: 2015-10-12 20:24:27.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	1473231341
Other Info	1473231341, which evaluates to: 2016-09-07 06:55:41.

URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	1502002290
Other Info	1502002290, which evaluates to: 2017-08-06 06:51:30.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	1530992060
Other Info	1530992060, which evaluates to: 2018-07-07 19:34:20.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	1560198380
Other Info	1560198380, which evaluates to: 2019-06-10 20:26:20.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	1700485571
Other Info	1700485571, which evaluates to: 2023-11-20 13:06:11.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	1732584193
Other Info	1732584193, which evaluates to: 2024-11-26 01:23:13.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	

Evidence	1732584194
Other Info	1732584194, which evaluates to: 2024-11-26 01:23:14.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	1735328473
Other Info	1735328473, which evaluates to: 2024-12-27 19:41:13.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	1770035416
Other Info	1770035416, which evaluates to: 2026-02-02 12:30:16.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	1804603682
Other Info	1804603682, which evaluates to: 2027-03-09 14:48:02.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	1836589329
Other Info	1836589329, which evaluates to: 2028-03-13 19:42:09.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	1839030562
Other Info	1839030562, which evaluates to: 2028-04-11 01:49:22.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET

Parameter	
Attack	
Evidence	1873313359
Other Info	1873313359, which evaluates to: 2029-05-12 20:49:19.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	1894986606
Other Info	1894986606, which evaluates to: 2030-01-18 17:10:06.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	1926607734
Other Info	1926607734, which evaluates to: 2031-01-19 16:48:54.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	1958414417
Other Info	1958414417, which evaluates to: 2032-01-22 20:00:17.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	1990404162
Other Info	1990404162, which evaluates to: 2033-01-27 02:02:42.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	2022574463
Other Info	2022574463, which evaluates to: 2034-02-03 10:14:23.

URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	2054922799
Other Info	2054922799, which evaluates to: 2035-02-12 19:53:19.
Instances	20
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
Plugin Id	10096

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	http://host.docker.internal:3000
Method	GET
Parameter	x-content-type-options
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	http://host.docker.internal:3000/logo.png
Method	GET
Parameter	x-content-type-options
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	http://host.docker.internal:3000/static/js/bundle.js
Method	GET

Parameter	x-content-type-options
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	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker.
URL	http://host.docker.internal:3000/static/js/bundle.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "// We will warn the user (as this is likely a mistake) and assume they cannot be refreshed.", see evidence field for the suspicious comment/snippet.
Instances	1
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615
WASC Id	13
Plugin Id	10027

Informational	**Modern Web Application**
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	http://host.docker.internal:3000

Method	GET
Parameter	
Attack	
Evidence	<script defer src="/static/js/bundle.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	1
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

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://host.docker.internal:3000
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.
URL	http://host.docker.internal:3000/robots.txt
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.
URL	http://host.docker.internal:3000/sitemap.xml
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.
URL	http://host.docker.internal:3000/static/js/bundle.js
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	4
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

Informational	**Storable but Non-Cacheable Content**
Description	The response contents are storable by caching components such as proxy servers, but will not be retrieved directly from the cache, without validating the request upstream, in response to similar requests from other users.
URL	http://host.docker.internal:3000/logo.png
Method	GET
Parameter	
Attack	
Evidence	max-age=0
Other Info	
Instances	1
Solution	

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.