ZAP Scanning Report

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

Generated on Thu, 17 Jul 2025 11:57:13

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	5
Informational	5
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
Content Security Policy (CSP) Header Not Set	Medium	11
Cross-Domain Misconfiguration	Medium	13
Cross-Domain JavaScript Source File Inclusion	Low	10
Dangerous JS Functions	Low	2
Deprecated Feature Policy Header Set	Low	11
Insufficient Site Isolation Against Spectre Vulnerability	Low	10
Timestamp Disclosure - Unix	Low	9
Information Disclosure - Suspicious Comments	Informational	2
Modern Web Application	Informational	11
Non-Storable Content	Informational	2
Storable and Cacheable Content	Informational	1
Storable but Non-Cacheable Content	Informational	8

Alert Detail

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	
URL	http://host.docker.internal:3000/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/ftp
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/ftp/coupons_2013.md.bak
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/ftp/eastere.gg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/ftp/encrypt.pyc
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/ftp/package-lock.json.bak
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/ftp/package.json.bak
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/ftp/suspicious_errors.yml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/juice-shop/build/routes/fileServer.js:59:18
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	11
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/
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/assets/public/favicon_js.ico
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/ftp
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/ftp/coupons_2013.md.bak
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/ftp/eastere.gg
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/main.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.
URL	http://host.docker.internal:3000/polyfills.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.
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/runtime.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.
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/styles.css
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/vendor.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	13
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

Low	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	http://host.docker.internal:3000
Method	GET
Parameter	//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	
URL	http://host.docker.internal:3000
Method	GET
Parameter	//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://host.docker.internal:3000/
Method	GET
Parameter	//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	
URL	http://host.docker.internal:3000/
Method	GET
Parameter	//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js

Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://host.docker.internal:3000/juice-shop/build/routes/fileServer.js:59:18
Method	GET
Parameter	//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	
URL	http://host.docker.internal:3000/juice-shop/build/routes/fileServer.js:59:18
Method	GET
Parameter	//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://host.docker.internal:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
Method	GET
Parameter	//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	
URL	http://host.docker.internal:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
Method	GET
Parameter	//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://host.docker.internal:3000/sitemap.xml
Method	GET
Parameter	//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	
URL	http://host.docker.internal:3000/sitemap.xml
Method	GET
Parameter	//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	

Instances	10
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

Low	**Dangerous JS Functions**
Description	A dangerous JS function seems to be in use that would leave the site vulnerable.
URL	http://host.docker.internal:3000/main.js
Method	GET
Parameter	
Attack	
Evidence	bypassSecurityTrustHtml(
Other Info	
URL	http://host.docker.internal:3000/vendor.js
Method	GET
Parameter	
Attack	
Evidence	bypassSecurityTrustHtml(
Other Info	
Instances	2
Solution	See the references for security advice on the use of these functions.
Reference	https://angular.io/guide/security
CWE Id	749
WASC Id	
Plugin Id	10110

Low	**Deprecated Feature Policy Header Set**
Description	The header has now been renamed to Permissions-Policy.
URL	http://host.docker.internal:3000
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
Other Info	
URL	http://host.docker.internal:3000/
Method	GET
Parameter	
Attack	

Evidence	Feature-Policy
Other Info	
URL	http://host.docker.internal:3000/ftp
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
Other Info	
URL	http://host.docker.internal:3000/ftp/coupons_2013.md.bak
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
Other Info	
URL	http://host.docker.internal:3000/ftp/eastere.gg
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
Other Info	
URL	http://host.docker.internal:3000/ftp/encrypt.pyc
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
Other Info	
URL	http://host.docker.internal:3000/ftp/package-lock.json.bak
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
Other Info	
URL	http://host.docker.internal:3000/main.js
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
Other Info	
URL	http://host.docker.internal:3000/polyfills.js

Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
Other Info	
URL	http://host.docker.internal:3000/runtime.js
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
Other Info	
URL	http://host.docker.internal:3000/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
Other Info	
Instances	11
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header instead of the Feature-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Permissions-Policy https://scotthelme.co.uk/goodbye-feature-policy-and-hello-permissions-policy/
CWE Id	16
WASC Id	15
Plugin Id	10063

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-Embedder-Policy
Attack	
Evidence	

Other Info	
URL	http://host.docker.internal:3000/ftp
Method	GET
Parameter	Cross-Origin-Embedder-Policy
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/juice-shop/build/routes/fileServer.js:59:18
Method	GET
Parameter	Cross-Origin-Embedder-Policy
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/sitemap.xml
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	
URL	http://host.docker.internal:3000/
Method	GET
Parameter	Cross-Origin-Opener-Policy
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/ftp
Method	GET
Parameter	Cross-Origin-Opener-Policy
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/juice-shop/build/routes/fileServer.js:59:18
Method	GET

Parameter	Cross-Origin-Opener-Policy
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/sitemap.xml
Method	GET
Parameter	Cross-Origin-Opener-Policy
Attack	
Evidence	
Other Info	
Instances	10
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	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	http://host.docker.internal:3000
Method	GET
Parameter	
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 20:10:37.
URL	http://host.docker.internal:3000
Method	GET
Parameter	
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 19:35:49.
URL	http://host.docker.internal:3000
Method	GET
Parameter	
Attack	
Evidence	2038834951

Other Info	2038834951, which evaluates to: 2034-08-10 15:02:31.
URL	http://host.docker.internal:3000/
Method	GET
Parameter	
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 20:10:37.
URL	http://host.docker.internal:3000/
Method	GET
Parameter	
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 19:35:49.
URL	http://host.docker.internal:3000/
Method	GET
Parameter	
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 15:02:31.
URL	http://host.docker.internal:3000/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 20:10:37.
URL	http://host.docker.internal:3000/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 19:35:49.
URL	http://host.docker.internal:3000/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 15:02:31.
Instances	9

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

Informational **Information Disclosure - Suspicious Comments**

Description	The response appears to contain suspicious comments which may help an attacker.
URL	http://host.docker.internal:3000/main.js
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//owasp.org' target='_blank'>Open Worldwide Application Security Project (OWASP) and is developed and maintained by voluntee", see evidence field for the suspicious comment/snippet.
URL	http://host.docker.internal:3000/vendor.js
Method	GET
Parameter	
Attack	
Evidence	Query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//www.w3.org/2000/svg" viewBox="0 0 512 512"><path d="M0 256C0 397.4 114.6 512 256 512s256-114.6 256-256S397.4 0 256 0S0 114.6 0", see evidence field for the suspicious comment/snippet.
Instances	2
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 src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.

URL	http://host.docker.internal:3000/
Method	GET
Parameter	
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://host.docker.internal:3000/juice-shop/build/routes/fileServer.js:59:18
Method	GET
Parameter	
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://host.docker.internal:3000/juice-shop/node_modules/express/lib/router/index.js:286:9
Method	GET
Parameter	
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://host.docker.internal:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
Method	GET
Parameter	
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://host.docker.internal:3000/juice-shop/node_modules/express/lib/router/index.js:365:14
Method	GET
Parameter	
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://host.docker.internal:3000/juice-shop/node_modules/express/lib/router/index.js:376:14
Method	GET
Parameter	
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.

URL	http://host.docker.internal:3000/juice-shop/node_modules/express/lib/router/index.js:421:3
Method	GET
Parameter	
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://host.docker.internal:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5
Method	GET
Parameter	
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://host.docker.internal:3000/juice-shop/node_modules/serve-index/index.js:145:39
Method	GET
Parameter	
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://host.docker.internal:3000/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.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	11
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

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:3000/ftp/coupons_2013.md.bak
Method	GET
Parameter	

Attack	
Evidence	403
Other Info	
URL	http://host.docker.internal:3000/ftp/eastere.gg
Method	GET
Parameter	
Attack	
Evidence	403
Other Info	
Instances	2
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

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/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.
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

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
Method	GET
Parameter	
Attack	
Evidence	max-age=0
Other Info	
URL	http://host.docker.internal:3000/
Method	GET
Parameter	
Attack	
Evidence	max-age=0
Other Info	
URL	http://host.docker.internal:3000/assets/public/favicon_js.ico

Method	GET
Parameter	
Attack	
Evidence	max-age=0
Other Info	
URL	http://host.docker.internal:3000/main.js
Method	GET
Parameter	
Attack	
Evidence	max-age=0
Other Info	
URL	http://host.docker.internal:3000/polyfills.js
Method	GET
Parameter	
Attack	
Evidence	max-age=0
Other Info	
URL	http://host.docker.internal:3000/runtime.js
Method	GET
Parameter	
Attack	
Evidence	max-age=0
Other Info	
URL	http://host.docker.internal:3000/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	max-age=0
Other Info	
URL	http://host.docker.internal:3000/styles.css
Method	GET
Parameter	
Attack	
Evidence	max-age=0
Other Info	
Instances	8
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.