ZAP Scanning Report

Site: http://172.16.10.100:3000

Generated on Thu, 18 May 2023 17:11:02

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	4
Informational	4
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	11
Cross-Domain Misconfiguration	Medium	11
Cross-Domain JavaScript Source File Inclusion	Low	10
Dangerous JS Functions	Low	2
Deprecated Feature Policy Header Set	Low	12
Timestamp Disclosure - Unix	Low	1
Information Disclosure - Suspicious Comments	Informational	2
Modern Web Application	Informational	11
Storable and Cacheable Content	Informational	2
Storable but Non-Cacheable Content	Informational	10

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, audioand video files.
URL	http://172.16.10.100:3000/
Method	GET

Parameter	
Attack	
Evidence	
URL	http://172.16.10.100:3000/ftp
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.16.10.100:3000/ftp/coupons_2013.md.bak
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.16.10.100:3000/ftp/eastere.gg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.16.10.100:3000/ftp/encrypt.pyc
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.16.10.100:3000/ftp/package.json.bak
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.16.10.100:3000/ftp/suspicious_errors.yml
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.16.10.100:3000/home/node_modules/express/lib/router/index.js:280:10
Method	GET

Parameter	
Attack	
Evidence	
URL	http://172.16.10.100:3000/home/node_modules/express/lib/router/index.js:328:13
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.16.10.100:3000/home/node_modules/express/lib/router/index.js:365:14
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.16.10.100:3000/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
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 http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://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://172.16.10.100:3000/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *

URL	http://172.16.10.100:3000/assets/public/favicon_js.ico
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://172.16.10.100:3000/ftp
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://172.16.10.100:3000/ftp/acquisitions.md
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://172.16.10.100:3000/main.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://172.16.10.100:3000/polyfills.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://172.16.10.100:3000/robots.txt
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://172.16.10.100:3000/runtime.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://172.16.10.100:3000/sitemap.xml

Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://172.16.10.100:3000/styles.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://172.16.10.100:3000/vendor.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Instances	11
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 allowthe 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://172.16.10.100:3000/
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>
URL	http://172.16.10.100:3000/
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>
URL	http://172.16.10.100:3000/home/node_modules/express/lib/router/index.js:280:10

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>
URL	http://172.16.10.100:3000/home/node_modules/express/lib/router/index.js:280:10
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>
URL	http://172.16.10.100:3000/home/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>
URL	http://172.16.10.100:3000/home/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>
URL	http://172.16.10.100:3000/home/node_modules/express/lib/router/index.js:365:14
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>
URL	http://172.16.10.100:3000/home/node_modules/express/lib/router/index.js:365:14
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>
URL	http://172.16.10.100:3000/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>

URL	http://172.16.10.100:3000/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>
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://172.16.10.100:3000/main.js
Method	GET
Parameter	
Attack	
Evidence	bypassSecurityTrustHtml
URL	http://172.16.10.100:3000/vendor.js
Method	GET
Parameter	
Attack	
Evidence	bypassSecurityTrustHtml
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://172.16.10.100:3000/
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy

URL	http://172.16.10.100:3000/ftp
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
URL	http://172.16.10.100:3000/ftp/coupons_2013.md.bak
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
URL	http://172.16.10.100:3000/ftp/eastere.gg
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
URL	http://172.16.10.100:3000/ftp/encrypt.pyc
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
URL	http://172.16.10.100:3000/ftp/package.json.bak
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
URL	http://172.16.10.100:3000/ftp/suspicious_errors.yml
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
URL	http://172.16.10.100:3000/main.js
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
URL	http://172.16.10.100:3000/polyfills.js

Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
URL	http://172.16.10.100:3000/runtime.js
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
URL	http://172.16.10.100:3000/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
URL	http://172.16.10.100:3000/vendor.js
Method	GET
Parameter	
Attack	
Evidence	Feature-Policy
Instances	12
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header instead of the Feature-Policyheader.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy https://scotthelme.co.uk/goodbye-feature-policy-and-hello-permissions-policy/
CWE Id	16
WASC Id	15
Plugin Id	10063

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server - Unix
URL	http://172.16.10.100:3000/main.js
Method	GET
Parameter	
Attack	
Evidence	1734944650
Instances	1
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage

CWE Id	200
WASC Id	13
Plugin Id	10096

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	http://172.16.10.100:3000/main.js
Method	GET
Parameter	
Attack	
Evidence	query
URL	http://172.16.10.100:3000/vendor.js
Method	GET
Parameter	
Attack	
Evidence	query
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	200
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://172.16.10.100:3000/
Method	GET
Parameter	
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"> </script>
URL	http://172.16.10.100:3000/home/build/routes/fileServer.js:16:13
Method	GET
Parameter	
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"> </script>
URL	http://172.16.10.100:3000/home/build/routes/fileServer.js:32:18

Method	GET
Parameter	
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://172.16.10.100:3000/home/node_modules/express/lib/router/index.js:280:10
Method	GET
Parameter	
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://172.16.10.100:3000/home/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>
URL	http://172.16.10.100:3000/home/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>
URL	http://172.16.10.100:3000/home/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>
URL	http://172.16.10.100:3000/home/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>
URL	http://172.16.10.100:3000/home/node_modules/express/lib/router/styles.css
Method	GET
Parameter	
Attack	

Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://172.16.10.100:3000/home/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>
URL	http://172.16.10.100:3000/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Instances	11
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 somecases, 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://172.16.10.100:3000/ftp
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.16.10.100:3000/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Instances	2

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://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)
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 validatingthe request upstream, in response to similar requests from other users.
URL	http://172.16.10.100:3000/
Method	GET
Parameter	
Attack	
Evidence	max-age=0
URL	http://172.16.10.100:3000/assets/public/favicon_js.ico
Method	GET
Parameter	
Attack	
Evidence	max-age=0
URL	http://172.16.10.100:3000/ftp/acquisitions.md
Method	GET
Parameter	
Attack	
Evidence	max-age=0
URL	http://172.16.10.100:3000/ftp/legal.md
Method	GET
Parameter	
Attack	
Evidence	max-age=0
URL	http://172.16.10.100:3000/main.js

Method	GET
Parameter	
Attack	
Evidence	max-age=0
URL	http://172.16.10.100:3000/polyfills.js
Method	GET
Parameter	
Attack	
Evidence	max-age=0
URL	http://172.16.10.100:3000/runtime.js
Method	GET
Parameter	
Attack	
Evidence	max-age=0
URL	http://172.16.10.100:3000/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	max-age=0
URL	http://172.16.10.100:3000/styles.css
Method	GET
Parameter	
Attack	
Evidence	max-age=0
URL	http://172.16.10.100:3000/vendor.js
Method	GET
Parameter	
Attack	
Evidence	max-age=0
Instances	10
Solution	
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)
CWE Id	524
WASC Id	13
Plugin Id	10049