ZAP by Checkmarx Scanning Report

Sites: https://tracking-protection.cdn.mozilla.net http://cdnjs.cloudflare.com https://shavar.services.mozilla.com http://localhost:3000

Generated on Fri, 6 Feb 2026 03:45:16

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	5
Low	6
Informational	4

Insights

Level	Reason	Site	Description	Statistic
Low	Warning		ZAP warnings logged - see the zap.log file for details	3
Info	Informational	http://cdnjs.cloudflare.com	Percentage of responses with status code 2xx	100 %
Info	Informational	http://cdnjs.cloudflare.com	Percentage of endpoints with content type application/javascript	66 %
Info	Informational	http://cdnjs.cloudflare.com	Percentage of endpoints with content type text/css	33 %
			Percentage of endpoints	

Info	Informational	http://cdnjs.cloudflare.com	with method GET	100 %
Info	Informational	http://cdnjs.cloudflare.com	Count of total endpoints	3
Info	Informational	http://cdnjs.cloudflare.com	Percentage of slow responses	16 %
Info	Informational	http://localhost:3000	Percentage of responses with status code 1xx	1 %
Info	Informational	http://localhost:3000	Percentage of responses with status code 2xx	64 %
Info	Informational	http://localhost:3000	Percentage of responses with status code 3xx	8 %
Info	Exceeded Low	http://localhost:3000	Percentage of responses with status code 4xx	24 %
Info	Informational	http://localhost:3000	Percentage of responses with status code 5xx	2 %
Info	Informational	http://localhost:3000	Percentage of endpoints with content type application/javascript	5 %
Info	Informational	http://localhost:3000	Percentage of endpoints with content type application/json	7 %
Info	Informational	http://localhost:3000	Percentage of endpoints with content type application/octet-stream	5 %
			Percentage of endpoints	

Info	Informational	http://localhost:3000	with content type font /woff	1 %
Info	Informational	http://localhost:3000	Percentage of endpoints with content type font /woff2	1 %
Info	Informational	http://localhost:3000	Percentage of endpoints with content type image /jpeg	12 %
Info	Informational	http://localhost:3000	Percentage of endpoints with content type image /png	2 %
Info	Informational	http://localhost:3000	Percentage of endpoints with content type image /x-icon	1 %
Info	Informational	http://localhost:3000	Percentage of endpoints with content type text /css	1 %
Info	Informational	http://localhost:3000	Percentage of endpoints with content type text /html	58 %
Info	Informational	http://localhost:3000	Percentage of endpoints with content type text /markdown	3 %
Info	Informational	http://localhost:3000	Percentage of endpoints with content type text /plain	3 %
			Percentage of endpoints	

Info	Informational	http://localhost:3000	with method GET	99 %
Info	Informational	http://localhost:3000	Percentage of endpoints with method POST	1 %
Info	Informational	http://localhost:3000	Count of total endpoints	100
Info	Informational	http://localhost:3000	Percentage of slow responses	4 %
Info	Informational	https://shavar.services.mozilla.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://shavar.services.mozilla.com	Percentage of endpoints with content type application/octet-stream	100 %
Info	Informational	https://shavar.services.mozilla.com	Percentage of endpoints with method POST	100 %
Info	Informational	https://shavar.services.mozilla.com	Count of total endpoints	1
Info	Informational	https://shavar.services.mozilla.com	Percentage of slow responses	100 %
Info	Informational	https://tracking-protection.cdn.mozilla.net	Percentage of responses with status code 2xx	100 %
Info	Informational	https://tracking-protection.cdn.mozilla.net	Percentage of endpoints with content type application/octet-stream	100 %
Info	Informational	https://tracking-protection.cdn.mozilla.net	Percentage of endpoints with method GET	100 %

Info	Informational	https://tracking-protection.cdn.mozilla.net	Count of total endpoints	1
Info	Informational	https://tracking-protection.cdn.mozilla.net	Percentage of slow responses	100 %

Alerts

Name	Risk Level	Number of Instances
SQL Injection	High	1
Content Security Policy (CSP) Header Not Set	Medium	Systemic
Cross-Domain Misconfiguration	Medium	Systemic
Missing Anti-clickjacking Header	Medium	1
Session ID in URL Rewrite	Medium	Systemic
Vulnerable JS Library	Medium	1
Cross-Domain JavaScript Source File Inclusion	Low	Systemic
Private IP Disclosure	Low	1
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	1
Strict-Transport-Security Header Not Set	Low	1
Timestamp Disclosure - Unix	Low	Systemic
X-Content-Type-Options Header Missing	Low	5
Information Disclosure - Suspicious Comments	Informational	4
Modern Web Application	Informational	Systemic
Retrieved from Cache	Informational	Systemic
User Agent Fuzzer	Informational	Systemic

Alert Detail

High	SQL Injection
Description	SQL injection may be possible.
URL	http://localhost:3000/rest/products/search?q=%27%28
Node Name	http://localhost:3000/rest/products/search (q)
Method	GET
Attack	'(
Evidence	HTTP/1.1 500 Internal Server Error
Other Info	
Instances	1
	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'

Solution	If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	40018

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://localhost:3000
Node Name	http://localhost:3000
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/
Node Name	http://localhost:3000/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp
Node Name	http://localhost:3000/ftp

Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/coupons_2013.md.bak
Node Name	http://localhost:3000/ftp/coupons_2013.md.bak
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/sitemap.xml
Node Name	http://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	Systemic
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/HTTP/Guides/CSP 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://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Node Name	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Method	GET
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://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Node Name	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Method	GET
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://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Node Name	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
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://localhost:3000
Node Name	http://localhost:3000
Method	GET
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://localhost:3000/assets/public/favicon_js.ico
Node Name	http://localhost:3000/assets/public/favicon_js.ico
Method	GET
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://localhost:3000/robots.txt

Node Name	http://localhost:3000/robots.txt
Method	GET
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://localhost:3000/runtime.js
Node Name	http://localhost:3000/runtime.js
Method	GET
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://localhost:3000/sitemap.xml
Node Name	http://localhost:3000/sitemap.xml
Method	GET
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	Systemic
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?category=HTML5&subcategory=Overly%20Permissive%20CORS%20Policy
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.
	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=Pmo4hi-

URL	&sid=6bKKjYkNtQEXCyQ9AAAI
Node Name	http://localhost:3000/socket.io/ (EIO,sid,t,transport)(40)
Method	POST
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/Reference/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Medium	Session ID in URL Rewrite
Description	URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site referer header. In addition, the session ID might be stored in browser history or server logs.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=Pmo4hj6&sid=6bKKjYkNtQEXCyQ9AAAI
Node Name	http://localhost:3000/socket.io/ (EIO,sid,t,transport)
Method	GET
Attack	
Evidence	6bKKjYkNtQEXCyQ9AAAI
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=Pmo4ils&sid=ZisMQvHDfd-IMkuqAAAK
Node Name	http://localhost:3000/socket.io/ (EIO,sid,t,transport)
Method	GET
Attack	
Evidence	ZisMQvHDfd-IMkuqAAAK
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=6bKKjYkNtQEXCyQ9AAAI
Node Name	http://localhost:3000/socket.io/ (EIO,sid,transport)
Method	GET
Attack	

Evidence	6bKKjYkNtQEXCyQ9AAAI
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=Pmo4hi-&sid=6bKKjYkNtQEXCyQ9AAAI
Node Name	http://localhost:3000/socket.io/ (EIO,sid,t,transport)(40)
Method	POST
Attack	
Evidence	6bKKjYkNtQEXCyQ9AAAI
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=Pmo4ilm&sid=ZisMQvHDfd-IMkuqAAAK
Node Name	http://localhost:3000/socket.io/ (EIO,sid,t,transport)(40)
Method	POST
Attack	
Evidence	ZisMQvHDfd-IMkuqAAAK
Other Info	
Instances	Systemic
Solution	For secure content, put session ID in a cookie. To be even more secure consider using a combination of cookie and URL rewrite.
Reference	https://seclists.org/webappsec/2002/q4/111
CWE Id	598
WASC Id	13
Plugin Id	3

Medium	**Vulnerable JS Library**
Description	The identified library appears to be vulnerable.
URL	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Node Name	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	/2.2.4/jquery.min.js
Other Info	The identified library jquery, version 2.2.4 is vulnerable. CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://github.com/jquery/jquery.com/issues/162 https://bugs.jquery.com/ticket/11974 https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
Instances	1
Solution	Upgrade to the latest version of the affected library.
Reference	https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

CWE Id	1395
WASC Id	
Plugin Id	10003

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

Other Info	
Instances	Systemic
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](829)
WASC Id	15
Plugin Id	[10017](10017)

Low	Private IP Disclosure
Description	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
URL	http://localhost:3000/rest/admin/application-configuration
Node Name	http://localhost:3000/rest/admin/application-configuration
Method	GET
Attack	
Evidence	192.168.99.100:3000
Other Info	192.168.99.100:3000 192.168.99.100:4200
Instances	1
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP /PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.
Reference	https://datatracker.ietf.org/doc/html/rfc1918
CWE Id	[497](497)
WASC Id	13
Plugin Id	[2](2)

Low	Server Leaks Version Information via "Server" HTTP Response Header Field
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	https://tracking-protection.cdn.mozilla.net/ads-track-digest256/128.0/1754651396
Node Name	https://tracking-protection.cdn.mozilla.net/ads-track-digest256/128.0/1754651396
Method	GET
Attack	
Evidence	AmazonS3
Other Info	
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	[497](497)

WASC Id	13
Plugin Id	10036

Low	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://tracking-protection.cdn.mozilla.net/ads-track-digest256/128.0/1754651396
Node Name	https://tracking-protection.cdn.mozilla.net/ads-track-digest256/128.0/1754651396
Method	GET
Attack	
Evidence	
Other Info	
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

Low	Timestamp Disclosure - Unix
Description	A timestamp was disclosed by the application/web server. - Unix
URL	http://localhost:3000
Node Name	http://localhost:3000
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000
Node Name	http://localhost:3000
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000

Node Name	http://localhost:3000
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/sitemap.xml
Node Name	http://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/sitemap.xml
Node Name	http://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://tracking-protection.cdn.mozilla.net/ads-track-digest256/128.0/1754651396
Node Name	https://tracking-protection.cdn.mozilla.net/ads-track-digest256/128.0/1754651396
Method	GET
Attack	
Evidence	1754651396
Other Info	1754651396, which evaluates to: 2025-08-08 07:09:56.
URL	https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=128.10&pver=2.2
Node Name	https://shavar.services.mozilla.com/downloads (appver,client,pver)(ads-track-digest256;social-track-digest...)
Method	POST
Attack	
Evidence	1718977977
Other Info	1718977977, which evaluates to: 2024-06-21 09:52:57.
URL	https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=128.10&pver=2.2
Node Name	https://shavar.services.mozilla.com/downloads (appver,client,pver)(ads-track-digest256;social-track-digest...)
Method	POST
Attack	

Evidence	1754651396
Other Info	1754651396, which evaluates to: 2025-08-08 07:09:56.
Instances	Systemic
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://localhost:3000/socket.io/?EIO=4&transport=polling&t=Pmo4hj6&sid=6bKKjYkNtQEXCyQ9AAAI
Node Name	http://localhost:3000/socket.io/ (EIO,sid,t,transport)
Method	GET
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://localhost:3000/socket.io/?EIO=4&transport=polling&t=Pmo4hXz
Node Name	http://localhost:3000/socket.io/ (EIO,t,transport)
Method	GET
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	https://tracking-protection.cdn.mozilla.net/ads-track-digest256/128.0/1754651396
Node Name	https://tracking-protection.cdn.mozilla.net/ads-track-digest256/128.0/1754651396
Method	GET
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://localhost:3000/socket.io/?EIO=4&transport=polling&t=Pmo4hi-&sid=6bKKjYkNtQEXCyQ9AAAI

Node Name	http://localhost:3000/socket.io/ (EIO,sid,t,transport)(40)
Method	POST
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	https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=128.10&pver=2.2
Node Name	https://shavar.services.mozilla.com/downloads (appver,client,pver)(ads-track-digest256;social-track-digest...)
Method	POST
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	5
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://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Node Name	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	Db
Other Info	The following pattern was used: \bDB\b and was detected in likely comment: "//,sb={},tb={},ub="*/".concat("*"),vb=d.createElement("a");vb.href=jb.href;function wb(a){return function(b,c){"string"!=typeof ", see evidence field for the suspicious comment/snippet.
URL	http://localhost:3000/main.js
Node Name	http://localhost:3000/main.js
Method	GET
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)</a> and is developed and maintained by voluntee", see evidence field for the suspicious comment/snippet.
URL	http://localhost:3000/tutorial.js
Node Name	http://localhost:3000/tutorial.js
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&amp;color=%23ff5500&amp;auto&lowbar;play=true&amp;h", see evidence field for the suspicious comment/snippet.
URL	http://localhost:3000/vendor.js
Node Name	http://localhost:3000/vendor.js
Method	GET
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	4
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	[615](615)
WASC Id	13
Plugin Id	[10027](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://localhost:3000
Node Name	http://localhost:3000
Method	GET
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://localhost:3000/
Node Name	http://localhost:3000/
Method	GET

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://localhost:3000/juice-shop/build/routes/fileServer.js:59:18
Node Name	http://localhost:3000/juice-shop/build/routes/fileServer.js:59:18
Method	GET
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://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
Node Name	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
Method	GET
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://localhost:3000/sitemap.xml
Node Name	http://localhost:3000/sitemap.xml
Method	GET
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	Systemic
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Retrieved from Cache**
Description	The content was retrieved from a shared cache. 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 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://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Node	

Name	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Method	GET
Attack	
Evidence	Age: 699874
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Node Name	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Method	GET
Attack	
Evidence	Age: 699889
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Node Name	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Method	GET
Attack	
Evidence	Age: 699874
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Node Name	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Method	GET
Attack	
Evidence	Age: 699889
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Node Name	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	Age: 1275461
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://tracking-protection.cdn.mozilla.net/ads-track-digest256/128.0/1754651396
Node Name	https://tracking-protection.cdn.mozilla.net/ads-track-digest256/128.0/1754651396
Method	GET
Attack	
Evidence	Age: 34402
Other	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in

Info	use.
Instances	Systemic
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.rfc-editor.org/rfc/rfc9110.html
CWE Id	525
WASC Id	
Plugin Id	10050

Informational	**User Agent Fuzzer**
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=Pmo52WI&sid=aUq7y67EUZI5ltAjAABI
Node Name	http://localhost:3000/socket.io/ (EIO,sid,t,transport)
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=aUq7y67EUZI5ltAjAABI
Node Name	http://localhost:3000/socket.io/ (EIO,sid,transport)
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=Pmo52LT
Node Name	http://localhost:3000/socket.io/ (EIO,t,transport)
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	

URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=Pmo52LT
Node Name	http://localhost:3000/socket.io/ (EIO,t,transport)
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=Pmo52Si&sid=aUq7y67EUZI5ltAjAABI
Node Name	http://localhost:3000/socket.io/ (EIO,sid,t,transport)(40)
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
Instances	Systemic
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104