ZAP Scanning Report

Sites: http://cdnjs.cloudflare.com http://localhost:3000

Generated on Thu, 6 Mar 2025 14:12:36

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

Risk Level	Number of Alerts
High	2
Medium	5
Low	4
Informational	4

Alerts

Name	Risk Level	Number of Instances
Cloud Metadata Potentially Exposed	High	1
SQL Injection - SQLite	High	1
Content Security Policy (CSP) Header Not Set	Medium	50
Cross-Domain Misconfiguration	Medium	55
Missing Anti-clickjacking Header	Medium	38
Session ID in URL Rewrite	Medium	141
Vulnerable JS Library	Medium	1
Cross-Domain JavaScript Source File Inclusion	Low	6
Private IP Disclosure	Low	1
Timestamp Disclosure - Unix	Low	5
X-Content-Type-Options Header Missing	Low	141
Information Disclosure - Suspicious Comments	Informational	4
Modern Web Application	Informational	4
Retrieved from Cache	Informational	24
User Agent Fuzzer	Informational	150

Alert Detail

High	Cloud Metadata Potentially Exposed
Description	The Cloud Metadata Attack attempts to abuse a misconfigured NGINX server in order to access the instance metadata maintained by cloud service providers such as AWS, GCP and Azure.

	All of these providers provide metadata via an internal unroutable IP address '169.254.169.254' - this can be exposed by incorrectly configured NGINX servers and accessed by using this IP address in the Host header field.
URL	http://localhost:3000/latest/meta-data/?EIO=4&transport=polling&t=PLhM2rl&sid=cmLHL2b8fysJd-YgAAA2
Method	POST
Attack	169.254.169.254
Evidence	
Other Info	Based on the successful response status code cloud metadata may have been returned in the response. Check the response data to see if any cloud metadata has been returned. The meta data returned can include information that would allow an attacker to completely compromise the system.
Instances	1
Solution	Do not trust any user data in NGINX configs. In this case it is probably the use of the $host variable which is set from the 'Host' header and can be controlled by an attacker.
Reference	https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/
CWE Id	
WASC Id	
Plugin Id	90034

High	**SQL Injection - SQLite**
Description	SQL injection may be possible.
URL	http://localhost:3000/rest/products/search?q=%27%28
Method	GET
Attack	'(
Evidence	SQLITE_ERROR
Other Info	RDBMS [SQLite] likely, given error message regular expression [SQLITE_ERROR] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised
Instances	1
Solution	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 '?' 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
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/.%5C..
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/coupons_2013.md.bak

Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/eastere.gg
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/encrypt.pyc
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/package.json.bak
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/quarantine
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/suspicious_errors.yml
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL-ih&sid=0SzjROnLTe1Uty3_AAAi
Method	POST

Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL-j-&sid=rQUfHvV_JhNoo8OaAAAj
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL-zt&sid=IRCZUeZsH9CgSMVEAAAl
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL_0N&sid=nmp2oA_-ssaRKvJhAAAm
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL_qJ&sid=Ek-S78emcX4YaM5FAAAq
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLp-a&sid=h12TvocwMf1zFlpWAAAE
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLpRM&sid=_6_9r-Q6FvBVV53JAAAC
Method	POST
Attack	
Evidence	
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PLhLr7c&sid=z_e2XLWQ7yYu4deJAAAG
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLseM&sid=ww77rV-o7FEPzuKBAAAI
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLtb5&sid=tWA_bkTaIcqrCfnZAAAK
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLtmm&sid=P54F40OqcygZM7rCAAAL
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLu_0&sid=mQyGP0_Ehjbeb3rOAAAQ
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLums&sid=szVkFNFY7BG9xnNFAAAO
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLurI&sid=KmcdNMHdAYoD7_RTAAAP
Method	POST
Attack	
Evidence	

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLwRL&sid=1CYSQn62MrDa4YQZAAAU
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLxaT&sid=KY5AlRQBKEQJHYb_AAAW
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLxre&sid=LFel27BXAgj3lVTLAAAX
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLyoq&sid=05w-ElbfMS-EBDd9AAAa
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLz43&sid=D0q7FjV1YbihPoPZAAAb
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLzEd&sid=f9HwJKyImsChn-GKAAAd
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLzFZ&sid=39xuD3Abuw-piyz2AAAe
Method	POST

Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Af&sid=hGKF0Km_pvfsJ64CAAAs
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Cl&sid=cp4fTSfWwEjAXVzPAAAu
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Cl&sid=x5t1cMFQKR0BN1YfAAAt
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0f1&sid=x5t1cMFQKR0BN1YfAAAt
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Zn&sid=hGKF0Km_pvfsJ64CAAAs
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM1Ce&sid=7HrtSvbIveh-VF7mAAAy
Method	POST
Attack	
Evidence	
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PLhM2F2&sid=VM4jP53aPPpcqMtWAAA0
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2Fz&sid=gS_I1nHwFgohCKDHAAA1
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2GB&sid=cmLHL2b8fysJd-YgAAA2
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2rl&sid=cmLHL2b8fysJd-YgAAA2
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM3L7&sid=26VoZSs-I52Lb6uBAAA5
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM3XB&sid=wCK99aunRRamgoChAAA7
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM4pL&sid=tKQ5aVoFDSjODCUQAABA
Method	POST
Attack	
Evidence	

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM4VQ&sid=tDStjPfTQ0QSJS-oAAA-
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM5-A&sid=zzh_5PKYIOr3BNP7AABC
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM6UZ&sid=okKlIRbDBvHtygq9AABE
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8IH&sid=gSgb1pCv77PedBXuAABG
Method	POST
Attack	
Evidence	
Other Info	
Instances	50
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://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
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
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
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/
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/api/Challenges/?name=Score%20Board
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/api/Quantitys/
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/i18n/en.json
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
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/images/hackingInstructor.png
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/images/JuiceShop_Logo.png
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/images/products/apple_juice.jpg
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/images/products/apple_pressings.jpg
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/images/products/artwork2.jpg
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/images/products/banana_juice.jpg
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/images/products/carrot_juice.jpeg
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/images/products/eggfruit_juice.jpg
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/images/products/fruit_press.jpg
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/images/products/green_smoothie.jpg
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/images/products/lemon_juice.jpg
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/images/products/melon_bike.jpeg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
	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

Other Info	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/images/products/permafrost.jpg
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/images/products/user_day_ticket.png
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/font-mfizz.woff
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/ftp
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/ftp/
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/ftp/.%5C..
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/ftp/acquisitions.md
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/ftp/announcement_encrypted.md
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/ftp/coupons_2013.md.bak
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/ftp/eastere.gg
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/ftp/encrypt.pyc
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/ftp/incident-support.kdbx
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/ftp/legal.md
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/ftp/package.json.bak
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/ftp/quarantine
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/ftp/quarantine/juicy_malware_linux_amd_64.url

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/ftp/quarantine/juicy_malware_linux_arm_64.url
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/ftp/quarantine/juicy_malware_macos_64.url
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/ftp/quarantine/juicy_malware_windows_64.exe.url
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/ftp/suspicious_errors.yml
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/main.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/MaterialIcons-Regular.woff2
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/polyfills.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/rest/admin/application-configuration
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/rest/admin/application-version
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/rest/captcha/
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/rest/languages
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/rest/products/search?q=
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/rest/user/whoami
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
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
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
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/styles.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://localhost:3000/vendor.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.
Instances	55
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 include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL-

URL	ih&sid=0SzjROnLTe1Uty3_AAAi
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL-j-&sid=rQUfHvV_JhNoo8OaAAAj
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL-zt&sid=IRCZUeZsH9CgSMVEAAAl
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL_0N&sid=nmp2oA_-ssaRKvJhAAAm
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL_qJ&sid=Ek-S78emcX4YaM5FAAAq
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLp-a&sid=h12TvocwMf1zFlpWAAAE
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLpRM&sid=_6_9r-Q6FvBVV53JAAAC
Method	POST
Attack	
Evidence	

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLr7c&sid=z_e2XLWQ7yYu4deJAAAG
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLseM&sid=ww77rV-o7FEPzuKBAAAI
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLtb5&sid=tWA_bkTaIcqrCfnZAAAK
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLtmm&sid=P54F40OqcygZM7rCAAAL
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLu_0&sid=mQyGP0_Ehjbeb3rOAAAQ
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLums&sid=szVkFNFY7BG9xnNFAAAO
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLurI&sid=KmcdNMHdAYoD7_RTAAAP
Method	POST

Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLwRL&sid=1CYSQn62MrDa4YQZAAAU
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLxaT&sid=KY5AlRQBKEQJHYb_AAAW
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLxre&sid=LFel27BXAgj3lVTLAAAX
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLyoq&sid=05w-ElbfMS-EBDd9AAAa
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLz43&sid=D0q7FjV1YbihPoPZAAAb
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLzEd&sid=f9HwJKyImsChn-GKAAAd
Method	POST
Attack	
Evidence	
Other Info	
	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLzFZ&sid=39xuD3Abuw-

URL	piyz2AAAe
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Af&sid=hGKF0Km_pvfsJ64CAAAs
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Cl&sid=cp4fTSfWwEjAXVzPAAAu
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Cl&sid=x5t1cMFQKR0BN1YfAAAt
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0f1&sid=x5t1cMFQKR0BN1YfAAAt
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Zn&sid=hGKF0Km_pvfsJ64CAAAs
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM1Ce&sid=7HrtSvbIveh-VF7mAAAy
Method	POST
Attack	
Evidence	

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2F2&sid=VM4jP53aPPpcqMtWAAA0
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2Fz&sid=gS_I1nHwFgohCKDHAAA1
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2GB&sid=cmLHL2b8fysJd-YgAAA2
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2rl&sid=cmLHL2b8fysJd-YgAAA2
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM3L7&sid=26VoZSs-I52Lb6uBAAA5
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM3XB&sid=wCK99aunRRamgoChAAA7
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM4pL&sid=tKQ5aVoFDSjODCUQAABA
Method	POST

Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM4VQ&sid=tDStjPfTQ0QSJS-oAAA-
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM5-A&sid=zzh_5PKYIOr3BNP7AABC
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM6UZ&sid=okKlIRbDBvHtygq9AABE
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8IH&sid=gSgb1pCv77PedBXuAABG
Method	POST
Attack	
Evidence	
Other Info	
Instances	38
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

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=PLhL-ii&sid=0SzjROnLTe1Uty3_AAAi
Method	GET
Attack	
Evidence	0SzjROnLTe1Uty3_AAAi
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL-k0&sid=rQUfHvV_JhNoo8OaAAAj
Method	GET
Attack	
Evidence	rQUfHvV_JhNoo8OaAAAj
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL-zx&sid=IRCZUeZsH9CgSMVEAAAl
Method	GET
Attack	
Evidence	IRCZUeZsH9CgSMVEAAAl
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL_0P&sid=nmp2oA_-ssaRKvJhAAAm
Method	GET
Attack	
Evidence	nmp2oA_-ssaRKvJhAAAm
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL_0q&sid=0SzjROnLTe1Uty3_AAAi
Method	GET
Attack	
Evidence	0SzjROnLTe1Uty3_AAAi
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL_Pw&sid=IRCZUeZsH9CgSMVEAAAl
Method	GET
Attack	
Evidence	IRCZUeZsH9CgSMVEAAAl
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL_QB&sid=rQUfHvV_JhNoo8OaAAAj
Method	GET
Attack	
Evidence	rQUfHvV_JhNoo8OaAAAj

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL_qL&sid=Ek-S78emcX4YaM5FAAAq
Method	GET
Attack	
Evidence	Ek-S78emcX4YaM5FAAAq
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL_Wq&sid=nmp2oA_-ssaRKvJhAAAm
Method	GET
Attack	
Evidence	nmp2oA_-ssaRKvJhAAAm
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLp-b&sid=h12TvocwMf1zFlpWAAAE
Method	GET
Attack	
Evidence	h12TvocwMf1zFlpWAAAE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLp_d&sid=h12TvocwMf1zFlpWAAAE
Method	GET
Attack	
Evidence	h12TvocwMf1zFlpWAAAE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLpRN&sid=_6_9r-Q6FvBVV53JAAAC
Method	GET
Attack	
Evidence	_6_9r-Q6FvBVV53JAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLpWe&sid=_6_9r-Q6FvBVV53JAAAC
Method	GET
Attack	
Evidence	_6_9r-Q6FvBVV53JAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLr7e&sid=z_e2XLWQ7yYu4deJAAAG
Method	GET

Attack	
Evidence	z_e2XLWQ7yYu4deJAAAG
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLrZA&sid=z_e2XLWQ7yYu4deJAAAG
Method	GET
Attack	
Evidence	z_e2XLWQ7yYu4deJAAAG
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLsi8&sid=ww77rV-o7FEPzuKBAAAI
Method	GET
Attack	
Evidence	ww77rV-o7FEPzuKBAAAI
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLt-j&sid=tWA_bkTaIcqrCfnZAAAK
Method	GET
Attack	
Evidence	tWA_bkTaIcqrCfnZAAAK
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLt4W&sid=ww77rV-o7FEPzuKBAAAI
Method	GET
Attack	
Evidence	ww77rV-o7FEPzuKBAAAI
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLt_C&sid=P54F40OqcygZM7rCAAAL
Method	GET
Attack	
Evidence	P54F40OqcygZM7rCAAAL
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLtb6&sid=tWA_bkTaIcqrCfnZAAAK
Method	GET
Attack	
Evidence	tWA_bkTaIcqrCfnZAAAK
Other Info	

URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLtmo&sid=P54F40OqcygZM7rCAAAL
Method	GET
Attack	
Evidence	P54F40OqcygZM7rCAAAL
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLu_3&sid=mQyGP0_Ehjbeb3rOAAAQ
Method	GET
Attack	
Evidence	mQyGP0_Ehjbeb3rOAAAQ
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLu_8&sid=szVkFNFY7BG9xnNFAAAO
Method	GET
Attack	
Evidence	szVkFNFY7BG9xnNFAAAO
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLu_u&sid=KmcdNMHdAYoD7_RTAAAP
Method	GET
Attack	
Evidence	KmcdNMHdAYoD7_RTAAAP
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLumu&sid=szVkFNFY7BG9xnNFAAAO
Method	GET
Attack	
Evidence	szVkFNFY7BG9xnNFAAAO
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLurJ&sid=KmcdNMHdAYoD7_RTAAAP
Method	GET
Attack	
Evidence	KmcdNMHdAYoD7_RTAAAP
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLvRr&sid=mQyGP0_Ehjbeb3rOAAAQ
Method	GET
Attack	
Evidence	mQyGP0_Ehjbeb3rOAAAQ

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLwhs&sid=1CYSQn62MrDa4YQZAAAU
Method	GET
Attack	
Evidence	1CYSQn62MrDa4YQZAAAU
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLwRO&sid=1CYSQn62MrDa4YQZAAAU
Method	GET
Attack	
Evidence	1CYSQn62MrDa4YQZAAAU
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLxaW&sid=KY5AlRQBKEQJHYb_AAAW
Method	GET
Attack	
Evidence	KY5AlRQBKEQJHYb_AAAW
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLxjJ&sid=KY5AlRQBKEQJHYb_AAAW
Method	GET
Attack	
Evidence	KY5AlRQBKEQJHYb_AAAW
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLxsU&sid=LFel27BXAgj3lVTLAAAX
Method	GET
Attack	
Evidence	LFel27BXAgj3lVTLAAAX
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLyos&sid=05w-ElbfMS-EBDd9AAAa
Method	GET
Attack	
Evidence	05w-ElbfMS-EBDd9AAAa
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLyS-&sid=LFel27BXAgj3lVTLAAAX
Method	GET

Attack	
Evidence	LFel27BXAgj3lVTLAAAX
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLz47&sid=D0q7FjV1YbihPoPZAAAb
Method	GET
Attack	
Evidence	D0q7FjV1YbihPoPZAAAb
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLz4N&sid=05w-ElbfMS-EBDd9AAAa
Method	GET
Attack	
Evidence	05w-ElbfMS-EBDd9AAAa
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLzEf&sid=f9HwJKyImsChn-GKAAAd
Method	GET
Attack	
Evidence	f9HwJKyImsChn-GKAAAd
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLzFb&sid=39xuD3Abuw-piyz2AAAe
Method	GET
Attack	
Evidence	39xuD3Abuw-piyz2AAAe
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLzGe&sid=D0q7FjV1YbihPoPZAAAb
Method	GET
Attack	
Evidence	D0q7FjV1YbihPoPZAAAb
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLzur&sid=f9HwJKyImsChn-GKAAAd
Method	GET
Attack	
Evidence	f9HwJKyImsChn-GKAAAd
Other Info	

URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLzw3&sid=39xuD3Abuw-piyz2AAAe
Method	GET
Attack	
Evidence	39xuD3Abuw-piyz2AAAe
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM09E&sid=Ek-S78emcX4YaM5FAAAq
Method	GET
Attack	
Evidence	Ek-S78emcX4YaM5FAAAq
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Ah&sid=hGKF0Km_pvfsJ64CAAAs
Method	GET
Attack	
Evidence	hGKF0Km_pvfsJ64CAAAs
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Cn&sid=cp4fTSfWwEjAXVzPAAAu
Method	GET
Attack	
Evidence	cp4fTSfWwEjAXVzPAAAu
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Cn&sid=x5t1cMFQKR0BN1YfAAAt
Method	GET
Attack	
Evidence	x5t1cMFQKR0BN1YfAAAt
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0hG&sid=cp4fTSfWwEjAXVzPAAAu
Method	GET
Attack	
Evidence	cp4fTSfWwEjAXVzPAAAu
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Y9&sid=hGKF0Km_pvfsJ64CAAAs
Method	GET
Attack	
Evidence	hGKF0Km_pvfsJ64CAAAs

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM1ar&sid=7HrtSvbIveh-VF7mAAAy
Method	GET
Attack	
Evidence	7HrtSvbIveh-VF7mAAAy
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM1C-&sid=7HrtSvbIveh-VF7mAAAy
Method	GET
Attack	
Evidence	7HrtSvbIveh-VF7mAAAy
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2F6&sid=VM4jP53aPPpcqMtWAAA0
Method	GET
Attack	
Evidence	VM4jP53aPPpcqMtWAAA0
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2F_&sid=gS_I1nHwFgohCKDHAAA1
Method	GET
Attack	
Evidence	gS_I1nHwFgohCKDHAAA1
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2GD&sid=cmLHL2b8fysJd-YgAAA2
Method	GET
Attack	
Evidence	cmLHL2b8fysJd-YgAAA2
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM3L9&sid=26VoZSs-I52Lb6uBAAA5
Method	GET
Attack	
Evidence	26VoZSs-I52Lb6uBAAA5
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM3OF&sid=VM4jP53aPPpcqMtWAAA0
Method	GET

Attack	
Evidence	VM4jP53aPPpcqMtWAAA0
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM3P2&sid=gS_I1nHwFgohCKDHAAA1
Method	GET
Attack	
Evidence	gS_I1nHwFgohCKDHAAA1
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM3q_&sid=wCK99aunRRamgoChAAA7
Method	GET
Attack	
Evidence	wCK99aunRRamgoChAAA7
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM3XE&sid=wCK99aunRRamgoChAAA7
Method	GET
Attack	
Evidence	wCK99aunRRamgoChAAA7
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM3Xk&sid=26VoZSs-I52Lb6uBAAA5
Method	GET
Attack	
Evidence	26VoZSs-I52Lb6uBAAA5
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM4mO&sid=tDStjPfTQ0QSJS-oAAA-
Method	GET
Attack	
Evidence	tDStjPfTQ0QSJS-oAAA-
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM4pM&sid=tKQ5aVoFDSjODCUQAABA
Method	GET
Attack	
Evidence	tKQ5aVoFDSjODCUQAABA
Other Info	

URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM4VU&sid=tDStjPfTQ0QSJS-oAAA-
Method	GET
Attack	
Evidence	tDStjPfTQ0QSJS-oAAA-
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM5-B&sid=zzh_5PKYIOr3BNP7AABC
Method	GET
Attack	
Evidence	zzh_5PKYIOr3BNP7AABC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM5BF&sid=tKQ5aVoFDSjODCUQAABA
Method	GET
Attack	
Evidence	tKQ5aVoFDSjODCUQAABA
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM63j&sid=zzh_5PKYIOr3BNP7AABC
Method	GET
Attack	
Evidence	zzh_5PKYIOr3BNP7AABC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM6gV&sid=okKlIRbDBvHtygq9AABE
Method	GET
Attack	
Evidence	okKlIRbDBvHtygq9AABE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM6Ub&sid=okKlIRbDBvHtygq9AABE
Method	GET
Attack	
Evidence	okKlIRbDBvHtygq9AABE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8II&sid=gSgb1pCv77PedBXuAABG
Method	GET
Attack	
Evidence	gSgb1pCv77PedBXuAABG

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8JU&sid=gSgb1pCv77PedBXuAABG
Method	GET
Attack	
Evidence	gSgb1pCv77PedBXuAABG
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=05w-ElbfMS-EBDd9AAAa
Method	GET
Attack	
Evidence	05w-ElbfMS-EBDd9AAAa
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=0SzjROnLTe1Uty3_AAAi
Method	GET
Attack	
Evidence	0SzjROnLTe1Uty3_AAAi
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=1CYSQn62MrDa4YQZAAAU
Method	GET
Attack	
Evidence	1CYSQn62MrDa4YQZAAAU
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=26VoZSs-I52Lb6uBAAA5
Method	GET
Attack	
Evidence	26VoZSs-I52Lb6uBAAA5
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=39xuD3Abuw-piyz2AAAe
Method	GET
Attack	
Evidence	39xuD3Abuw-piyz2AAAe
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=7HrtSvbIveh-VF7mAAAy
Method	GET
Attack	
Evidence	7HrtSvbIveh-VF7mAAAy

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=_6_9r-Q6FvBVV53JAAAC
Method	GET
Attack	
Evidence	_6_9r-Q6FvBVV53JAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=cmLHL2b8fysJd-YgAAA2
Method	GET
Attack	
Evidence	cmLHL2b8fysJd-YgAAA2
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=cp4fTSfWwEjAXVzPAAAu
Method	GET
Attack	
Evidence	cp4fTSfWwEjAXVzPAAAu
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=D0q7FjV1YbihPoPZAAAb
Method	GET
Attack	
Evidence	D0q7FjV1YbihPoPZAAAb
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=Ek-S78emcX4YaM5FAAAq
Method	GET
Attack	
Evidence	Ek-S78emcX4YaM5FAAAq
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=f9HwJKyImsChn-GKAAAd
Method	GET
Attack	
Evidence	f9HwJKyImsChn-GKAAAd
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=gS_I1nHwFgohCKDHAAA1
Method	GET
Attack	

Evidence	gS_I1nHwFgohCKDHAAA1
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=gSgb1pCv77PedBXuAABG
Method	GET
Attack	
Evidence	gSgb1pCv77PedBXuAABG
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=h12TvocwMf1zFlpWAAAE
Method	GET
Attack	
Evidence	h12TvocwMf1zFlpWAAAE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=hGKF0Km_pvfsJ64CAAAs
Method	GET
Attack	
Evidence	hGKF0Km_pvfsJ64CAAAs
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=IRCZUeZsH9CgSMVEAAAl
Method	GET
Attack	
Evidence	IRCZUeZsH9CgSMVEAAAl
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=KmcdNMHdAYoD7_RTAAAP
Method	GET
Attack	
Evidence	KmcdNMHdAYoD7_RTAAAP
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=KY5AlRQBKEQJHYb_AAAW
Method	GET
Attack	
Evidence	KY5AlRQBKEQJHYb_AAAW
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=LFel27BXAgj3lVTLAAAX
Method	GET

Attack	
Evidence	LFel27BXAgj3lVTLAAAX
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=mQyGP0_Ehjbeb3rOAAAQ
Method	GET
Attack	
Evidence	mQyGP0_Ehjbeb3rOAAAQ
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=nmp2oA_-ssaRKvJhAAAm
Method	GET
Attack	
Evidence	nmp2oA_-ssaRKvJhAAAm
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=okKlIRbDBvHtygq9AABE
Method	GET
Attack	
Evidence	okKlIRbDBvHtygq9AABE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=P54F40OqcygZM7rCAAAL
Method	GET
Attack	
Evidence	P54F40OqcygZM7rCAAAL
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=rQUfHvV_JhNoo8OaAAAj
Method	GET
Attack	
Evidence	rQUfHvV_JhNoo8OaAAAj
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=szVkFNFY7BG9xnNFAAAO
Method	GET
Attack	
Evidence	szVkFNFY7BG9xnNFAAAO
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=tDStjPfTQ0QSJS-oAAA-

Method	GET
Attack	
Evidence	tDStjPfTQ0QSJS-oAAA-
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=tKQ5aVoFDSjODCUQAABA
Method	GET
Attack	
Evidence	tKQ5aVoFDSjODCUQAABA
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=tWA_bkTaIcqrCfnZAAAK
Method	GET
Attack	
Evidence	tWA_bkTaIcqrCfnZAAAK
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=VM4jP53aPPpcqMtWAAA0
Method	GET
Attack	
Evidence	VM4jP53aPPpcqMtWAAA0
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=wCK99aunRRamgoChAAA7
Method	GET
Attack	
Evidence	wCK99aunRRamgoChAAA7
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=ww77rV-o7FEPzuKBAAAI
Method	GET
Attack	
Evidence	ww77rV-o7FEPzuKBAAAI
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=x5t1cMFQKR0BN1YfAAAt
Method	GET
Attack	
Evidence	x5t1cMFQKR0BN1YfAAAt
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=websocket&sid=z_e2XLWQ7yYu4deJAAAG
Method	GET
Attack	
Evidence	z_e2XLWQ7yYu4deJAAAG
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=zzh_5PKYIOr3BNP7AABC
Method	GET
Attack	
Evidence	zzh_5PKYIOr3BNP7AABC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL-ih&sid=0SzjROnLTe1Uty3_AAAi
Method	POST
Attack	
Evidence	0SzjROnLTe1Uty3_AAAi
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL-j-&sid=rQUfHvV_JhNoo8OaAAAj
Method	POST
Attack	
Evidence	rQUfHvV_JhNoo8OaAAAj
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL-zt&sid=IRCZUeZsH9CgSMVEAAAl
Method	POST
Attack	
Evidence	IRCZUeZsH9CgSMVEAAAl
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL_0N&sid=nmp2oA_-ssaRKvJhAAAm
Method	POST
Attack	
Evidence	nmp2oA_-ssaRKvJhAAAm
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL_qJ&sid=Ek-S78emcX4YaM5FAAAq
Method	POST
Attack	
Evidence	Ek-S78emcX4YaM5FAAAq

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLp-a&sid=h12TvocwMf1zFlpWAAAE
Method	POST
Attack	
Evidence	h12TvocwMf1zFlpWAAAE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLpRM&sid=_6_9r-Q6FvBVV53JAAAC
Method	POST
Attack	
Evidence	_6_9r-Q6FvBVV53JAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLr7c&sid=z_e2XLWQ7yYu4deJAAAG
Method	POST
Attack	
Evidence	z_e2XLWQ7yYu4deJAAAG
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLseM&sid=ww77rV-o7FEPzuKBAAAI
Method	POST
Attack	
Evidence	ww77rV-o7FEPzuKBAAAI
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLtb5&sid=tWA_bkTaIcqrCfnZAAAK
Method	POST
Attack	
Evidence	tWA_bkTaIcqrCfnZAAAK
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLtmm&sid=P54F40OqcygZM7rCAAAL
Method	POST
Attack	
Evidence	P54F40OqcygZM7rCAAAL
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLu_0&sid=mQyGP0_Ehjbeb3rOAAAQ
Method	POST

Attack	
Evidence	mQyGP0_Ehjbeb3rOAAAQ
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLums&sid=szVkFNFY7BG9xnNFAAAO
Method	POST
Attack	
Evidence	szVkFNFY7BG9xnNFAAAO
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLurI&sid=KmcdNMHdAYoD7_RTAAAP
Method	POST
Attack	
Evidence	KmcdNMHdAYoD7_RTAAAP
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLwRL&sid=1CYSQn62MrDa4YQZAAAU
Method	POST
Attack	
Evidence	1CYSQn62MrDa4YQZAAAU
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLxaT&sid=KY5AlRQBKEQJHYb_AAAW
Method	POST
Attack	
Evidence	KY5AlRQBKEQJHYb_AAAW
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLxre&sid=LFel27BXAgj3lVTLAAAX
Method	POST
Attack	
Evidence	LFel27BXAgj3lVTLAAAX
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLyoq&sid=05w-ElbfMS-EBDd9AAAa
Method	POST
Attack	
Evidence	05w-ElbfMS-EBDd9AAAa
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PLhLz43&sid=D0q7FjV1YbihPoPZAAAb
Method	POST
Attack	
Evidence	D0q7FjV1YbihPoPZAAAb
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLzEd&sid=f9HwJKyImsChn-GKAAAd
Method	POST
Attack	
Evidence	f9HwJKyImsChn-GKAAAd
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLzFZ&sid=39xuD3Abuw-piyz2AAAe
Method	POST
Attack	
Evidence	39xuD3Abuw-piyz2AAAe
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Af&sid=hGKF0Km_pvfsJ64CAAAs
Method	POST
Attack	
Evidence	hGKF0Km_pvfsJ64CAAAs
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Cl&sid=cp4fTSfWwEjAXVzPAAAu
Method	POST
Attack	
Evidence	cp4fTSfWwEjAXVzPAAAu
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Cl&sid=x5t1cMFQKR0BN1YfAAAt
Method	POST
Attack	
Evidence	x5t1cMFQKR0BN1YfAAAt
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0f1&sid=x5t1cMFQKR0BN1YfAAAt
Method	POST
Attack	
Evidence	x5t1cMFQKR0BN1YfAAAt

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Zn&sid=hGKF0Km_pvfsJ64CAAAs
Method	POST
Attack	
Evidence	hGKF0Km_pvfsJ64CAAAs
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM1Ce&sid=7HrtSvbIveh-VF7mAAAy
Method	POST
Attack	
Evidence	7HrtSvbIveh-VF7mAAAy
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2F2&sid=VM4jP53aPPpcqMtWAAA0
Method	POST
Attack	
Evidence	VM4jP53aPPpcqMtWAAA0
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2Fz&sid=gS_I1nHwFgohCKDHAAA1
Method	POST
Attack	
Evidence	gS_I1nHwFgohCKDHAAA1
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2GB&sid=cmLHL2b8fysJd-YgAAA2
Method	POST
Attack	
Evidence	cmLHL2b8fysJd-YgAAA2
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2rl&sid=cmLHL2b8fysJd-YgAAA2
Method	POST
Attack	
Evidence	cmLHL2b8fysJd-YgAAA2
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM3L7&sid=26VoZSs-I52Lb6uBAAA5
Method	POST

Attack	
Evidence	26VoZSs-I52Lb6uBAAA5
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM3XB&sid=wCK99aunRRamgoChAAA7
Method	POST
Attack	
Evidence	wCK99aunRRamgoChAAA7
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM4pL&sid=tKQ5aVoFDSjODCUQAABA
Method	POST
Attack	
Evidence	tKQ5aVoFDSjODCUQAABA
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM4VQ&sid=tDStjPfTQ0QSJS-oAAA-
Method	POST
Attack	
Evidence	tDStjPfTQ0QSJS-oAAA-
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM5-A&sid=zzh_5PKYIOr3BNP7AABC
Method	POST
Attack	
Evidence	zzh_5PKYIOr3BNP7AABC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM6UZ&sid=okKlIRbDBvHtygq9AABE
Method	POST
Attack	
Evidence	okKlIRbDBvHtygq9AABE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8IH&sid=gSgb1pCv77PedBXuAABG
Method	POST
Attack	
Evidence	gSgb1pCv77PedBXuAABG
Other Info	
Instances	141

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	200
WASC Id	13
Plugin Id	3

Medium	**Vulnerable JS Library**
Description	The identified library jquery, version 2.2.4 is vulnerable.
URL	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	CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358
Instances	1
Solution	Please upgrade to the latest version of jquery.
Reference	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/
CWE Id	829
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
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
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/
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/
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/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
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
Instances	6
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	**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
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://tools.ietf.org/html/rfc1918
CWE Id	200

WASC Id	13
Plugin Id	2

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server - Unix
URL	http://localhost:3000/main.js
Method	GET
Attack	
Evidence	1734944650
Other Info	1734944650, which evaluates to: 2024-12-23 11:04:10
URL	http://localhost:3000/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1969196030
Other Info	1969196030, which evaluates to: 2032-05-26 16:53:50
URL	http://localhost:3000/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1970691216
Other Info	1970691216, which evaluates to: 2032-06-13 00:13:36
URL	http://localhost:3000/rest/products/search?q=
Method	GET
Attack	
Evidence	1969196030
Other Info	1969196030, which evaluates to: 2032-05-26 16:53:50
URL	http://localhost:3000/rest/products/search?q=
Method	GET
Attack	
Evidence	1970691216
Other Info	1970691216, which evaluates to: 2032-06-13 00:13:36
Instances	5
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	200
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=PLhL-ao
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=PLhL-f4
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=PLhL-hB
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=PLhL-ii&sid=0SzjROnLTe1Uty3_AAAi
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=PLhL-k0&sid=rQUfHvV_JhNoo8OaAAAj
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=PLhL-ZC
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=PLhL-zx&sid=IRCZUeZsH9CgSMVEAAAI
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=PLhL_0P&sid=nmp2oA_-ssaRKvJhAAAm
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=PLhL_0q&sid=0SzjROnLTe1Uty3_AAAi
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=PLhL_iW
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=PLhL_Pw&sid=IRCZUeZsH9CgSMVEAAAI
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=PLhL_QB&sid=rQUfHvV_JhNoo8OaAAAj
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=PLhL_qL&sid=Ek-S78emcX4YaM5FAAAq
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=PLhL_ud
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=PLhL_Wq&sid=nmp2oA_-ssaRKvJhAAAm
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=PLhLp-b&sid=h12TvocwMf1zFlpWAAAE
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=PLhLp8d
Method	GET
Attack	
Evidence	
Other	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

Info	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=PLhLp_d&sid=h12TvocwMf1zFlpWAAAE
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=PLhLpRN&sid=_6_9r-Q6FvBVV53JAAAC
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=PLhLpWe&sid=_6_9r-Q6FvBVV53JAAAC
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=PLhLpwo
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=PLhLq-s
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=PLhLr7e&sid=z_e2XLWQ7yYu4deJAAAG
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=PLhLrZA&sid=z_e2XLWQ7yYu4deJAAAG
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=PLhLsi8&sid=ww77rV-o7FEPzuKBAAAI
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=PLhLsUw
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=PLhLt-j&sid=tWA_bkTaIcqrCfnZAAAK
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=PLhLt4W&sid=ww77rV-o7FEPzuKBAAAI
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=PLhLt_C&sid=P54F40OqcygZM7rCAAAL
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=PLhLtb6&sid=tWA_bkTaIcqrCfnZAAAK
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=PLhLtmo&sid=P54F40OqcygZM7rCAAAL
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=PLhLtRd
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=PLhLtT-
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=PLhLu_3&sid=mQyGP0_Ehjbeb3rOAAAQ
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.
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PLhLu_8&sid=szVkFNFY7BG9xnNFAAAO
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=PLhLu_u&sid=KmcdNMHdAYoD7_RTAAAP
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=PLhLukj
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=PLhLumu&sid=szVkFNFY7BG9xnNFAAAO
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=PLhLurJ&sid=KmcdNMHdAYoD7_RTAAAP
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=PLhLuXS
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=PLhLuY9
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=PLhLvRr&sid=mQyGP0_Ehjbeb3rOAAAQ
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=PLhLwGt
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=PLhLwhs&sid=1CYSQn62MrDa4YQZAAAU
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=PLhLwRO&sid=1CYSQn62MrDa4YQZAAAU
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=PLhLxaW&sid=KY5AlRQBKEQJHYb_AAAW
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=PLhLxjJ&sid=KY5AlRQBKEQJHYb_AAAW
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=PLhLxOX
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=PLhLxsU&sid=LFel27BXAgj3lVTLAAAX
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=PLhLxSX
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=PLhLyce
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=PLhLyl2
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=PLhLyos&sid=05w-ElbfMS-EBDd9AAAa
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=PLhLyqE
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=PLhLyS-&sid=LFel27BXAgj3lVTLAAAX
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=PLhLyyL
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=PLhLz47&sid=D0q7FjV1YbihPoPZAAAb
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=PLhLz4N&sid=05w-ElbfMS-EBDd9AAAa

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=PLhLzEf&sid=f9HwJKyImsChn-GKAAAd
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=PLhLzFb&sid=39xuD3Abuw-piyz2AAAe
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=PLhLzGe&sid=D0q7FjV1YbihPoPZAAAb
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=PLhLzur&sid=f9HwJKyImsChn-GKAAAd
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=PLhLzw3&sid=39xuD3Abuw-piyz2AAAe
Method	GET
Attack	
Evidence	
Other	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

Info	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=PLhM01t
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=PLhM02p
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=PLhM09E&sid=Ek-S78emcX4YaM5FAAAq
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=PLhM0Ah&sid=hGKF0Km_pvfsJ64CAAAs
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=PLhM0Cn&sid=cp4fTSfWwEjAXVzPAAAu
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=PLhM0Cn&sid=x5t1cMFQKR0BN1YfAAAt
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=PLhM0hG&sid=cp4fTSfWwEjAXVzPAAAu
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=PLhM0Y9&sid=hGKF0Km_pvfsJ64CAAAs
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=PLhM157
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=PLhM1ar&sid=7HrtSvbIveh-VF7mAAAy
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=PLhM1C-&sid=7HrtSvbIveh-VF7mAAAy
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=PLhM1JM
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=PLhM1Ki
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=PLhM1L1
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=PLhM2Cl
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=PLhM2F6&sid=VM4jP53aPPpcqMtWAAA0
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=PLhM2F_&sid=gS_I1nHwFgohCKDHAAA1
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=PLhM2GD&sid=cmLHL2b8fysJd-YgAAA2

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=PLhM2ZP
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=PLhM3L9&sid=26VoZSs-I52Lb6uBAAA5
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=PLhM3OF&sid=VM4jP53aPPpcqMtWAAA0
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=PLhM3P2&sid=gS_I1nHwFgohCKDHAAA1
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=PLhM3q_&sid=wCK99aunRRamgoChAAA7
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=PLhM3XE&sid=wCK99aunRRamgoChAAA7
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=PLhM3Xk&sid=26VoZSs-I52Lb6uBAAA5
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=PLhM4BL
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=PLhM4mO&sid=tDStjPfTQ0QSJS-oAAA-
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=PLhM4pM&sid=tKQ5aVoFDSjODCUQAABA
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=PLhM4VU&sid=tDStjPfTQ0QSJS-oAAA-
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=PLhM4ZS
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=PLhM5-B&sid=zzh_5PKYIOr3BNP7AABC
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=PLhM5BF&sid=tKQ5aVoFDSjODCUQAABA
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=PLhM5mQ
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=PLhM63j&sid=zzh_5PKYIOr3BNP7AABC
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=PLhM6F_
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=PLhM6gV&sid=okKlIRbDBvHtygq9AABE
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=PLhM6Ub&sid=okKlIRbDBvHtygq9AABE
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=PLhM8A4
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=PLhM8II&sid=gSgb1pCv77PedBXuAABG
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=PLhM8JU&sid=gSgb1pCv77PedBXuAABG
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=PLhL-ih&sid=0SzjROnLTe1Uty3_AAAi

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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL-j-&sid=rQUfHvV_JhNoo8OaAAAj
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL-zt&sid=IRCZUeZsH9CgSMVEAAAl
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL_0N&sid=nmp2oA_-ssaRKvJhAAAm
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhL_qJ&sid=Ek-S78emcX4YaM5FAAAq
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLp-a&sid=h12TvocwMf1zFlpWAAAE
Method	POST
Attack	
Evidence	
Other	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

Info	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=PLhLpRM&sid=_6_9r-Q6FvBVV53JAAAC
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLr7c&sid=z_e2XLWQ7yYu4deJAAAG
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLseM&sid=ww77rV-o7FEPzuKBAAAI
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLtb5&sid=tWA_bkTaIcqrCfnZAAAK
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLtmm&sid=P54F40OqcygZM7rCAAAL
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLu_0&sid=mQyGP0_Ehjbeb3rOAAAQ
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLums&sid=szVkFNFY7BG9xnNFAAAO
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLurI&sid=KmcdNMHdAYoD7_RTAAAP
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLwRL&sid=1CYSQn62MrDa4YQZAAAU
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLxaT&sid=KY5AlRQBKEQJHYb_AAAW
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLxre&sid=LFel27BXAgj3lVTLAAAX
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.
	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLyoq&sid=05w-ElbfMS-

URL	EBDd9AAAa
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLz43&sid=D0q7FjV1YbihPoPZAAAb
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLzEd&sid=f9HwJKyImsChn-GKAAAd
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhLzFZ&sid=39xuD3Abuw-piyz2AAAe
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Af&sid=hGKF0Km_pvfsJ64CAAAs
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Cl&sid=cp4fTSfWwEjAXVzPAAAu
Method	POST
Attack	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	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=PLhM0Cl&sid=x5t1cMFQKR0BN1YfAAAt
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0f1&sid=x5t1cMFQKR0BN1YfAAAt
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM0Zn&sid=hGKF0Km_pvfsJ64CAAAs
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM1Ce&sid=7HrtSvbIveh-VF7mAAAy
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2F2&sid=VM4jP53aPPpcqMtWAAA0
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2Fz&sid=gS_I1nHwFgohCKDHAAA1
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2GB&sid=cmLHL2b8fysJd-YgAAA2
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2rl&sid=cmLHL2b8fysJd-YgAAA2
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM3L7&sid=26VoZSs-I52Lb6uBAAA5
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM3XB&sid=wCK99aunRRamgoChAAA7
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM4pL&sid=tKQ5aVoFDSjODCUQAABA
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM4VQ&sid=tDStjPfTQ0QSJS-oAAA-
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM5-A&sid=zzh_5PKYIOr3BNP7AABC
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM6UZ&sid=okKlIRbDBvHtygq9AABE
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	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8IH&sid=gSgb1pCv77PedBXuAABG
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	141
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. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	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 2 times, the first in the element starting with: "}catch(e){}O.set(a,b,c)}else c=void 0;return c}n.extend({hasData:function(a){return O.hasData(a)||N.hasData(a)},data:function(a,", see evidence field for the suspicious comment/snippet.
URL	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.docu", see evidence field for the suspicious comment/snippet.
URL	http://localhost:3000/main.js
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: ""use strict";(self.webpackChunkfrontend=self.webpackChunkfrontend||[]).push([[179],{4550:(tt,K,c)=>{c.d(K,{e:()=>s});var S=c(234", see evidence field for the suspicious comment/snippet.
URL	http://localhost:3000/vendor.js
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "(self.webpackChunkfrontend=self.webpackChunkfrontend||[]).push([[736],{9187:(Mt,te,u)=>{"use strict";u.d(te,{Xy:()=>J,ne:()=>Be,", 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	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://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/
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/ftp/
Method	GET
Attack	
Evidence	ftp
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	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	4
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
Method	GET
Attack	
Evidence	Age: 14
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
Method	GET
Attack	

Evidence	Age: 23
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
Method	GET
Attack	
Evidence	Age: 30
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
Method	GET
Attack	
Evidence	Age: 40
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
Method	GET
Attack	
Evidence	Age: 48
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
Method	GET
Attack	
Evidence	Age: 57
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
Method	GET
Attack	
Evidence	Age: 70
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
Method	GET
Attack	
Evidence	Age: 8
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
Method	GET
Attack	
Evidence	Age: 14

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
Method	GET
Attack	
Evidence	Age: 23
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
Method	GET
Attack	
Evidence	Age: 30
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
Method	GET
Attack	
Evidence	Age: 40
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
Method	GET
Attack	
Evidence	Age: 48
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
Method	GET
Attack	
Evidence	Age: 57
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
Method	GET
Attack	
Evidence	Age: 70
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
Method	GET
Attack	
Evidence	Age: 8
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
Method	GET
Attack	
Evidence	Age: 14
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
Method	GET
Attack	
Evidence	Age: 23
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
Method	GET
Attack	
Evidence	Age: 30
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
Method	GET
Attack	
Evidence	Age: 40
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
Method	GET
Attack	
Evidence	Age: 48
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
Method	GET
Attack	
Evidence	Age: 57
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
Method	GET
Attack	
Evidence	Age: 70
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
Method	GET

Attack	
Evidence	Age: 8
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	24
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 https://www.rfc-editor.org/rfc/rfc9110.html
CWE Id	
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/assets
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko

Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18

Attack	(KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36

Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

Evidence	
Other Info	
URL	http://localhost:3000/assets/public
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/assets/public
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/assets/public
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/assets/public
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/assets/public
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	

Other Info	
URL	http://localhost:3000/assets/public
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost:3000/assets/public
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/assets/public
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	

Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	

Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other	

Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other	

Info	
URL	http://localhost:3000/rest/captcha
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	

URL	http://localhost:3000/rest/captcha
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	

URL	http://localhost:3000/rest/captcha/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha/
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha/
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha/

Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha/
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/rest/captcha/
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/rest/languages
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/rest/languages
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/rest/languages
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/rest/languages
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/rest/languages

Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/rest/languages
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8A4
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8A4
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=PLhM8A4
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=PLhM8A4
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8A4
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8A4
Method	GET

Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8A4
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8A4
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8A4
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8A4
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8A4
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8A4
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8JU&sid=gSgb1pCv77PedBXuAABG
Method	GET

Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8JU&sid=gSgb1pCv77PedBXuAABG
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=PLhM8JU&sid=gSgb1pCv77PedBXuAABG
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=PLhM8JU&sid=gSgb1pCv77PedBXuAABG
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8JU&sid=gSgb1pCv77PedBXuAABG
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8JU&sid=gSgb1pCv77PedBXuAABG
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8JU&sid=gSgb1pCv77PedBXuAABG
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other	

Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8JU&sid=gSgb1pCv77PedBXuAABG
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8JU&sid=gSgb1pCv77PedBXuAABG
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8JU&sid=gSgb1pCv77PedBXuAABG
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8JU&sid=gSgb1pCv77PedBXuAABG
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8JU&sid=gSgb1pCv77PedBXuAABG
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=_6_9r-Q6FvBVV53JAAAC
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=_6_9r-Q6FvBVV53JAAAC
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=websocket&sid=_6_9r-Q6FvBVV53JAAAC
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=_6_9r-Q6FvBVV53JAAAC
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=_6_9r-Q6FvBVV53JAAAC
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=_6_9r-Q6FvBVV53JAAAC
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=_6_9r-Q6FvBVV53JAAAC
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=_6_9r-Q6FvBVV53JAAAC
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other	

Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=_6_9r-Q6FvBVV53JAAAC
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=_6_9r-Q6FvBVV53JAAAC
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=_6_9r-Q6FvBVV53JAAAC
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=_6_9r-Q6FvBVV53JAAAC
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2rl&sid=cmLHL2b8fysJd-YgAAA2
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2rl&sid=cmLHL2b8fysJd-YgAAA2
Method	POST
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=PLhM2rl&sid=cmLHL2b8fysJd-YgAAA2
Method	POST

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=PLhM2rl&sid=cmLHL2b8fysJd-YgAAA2
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2rl&sid=cmLHL2b8fysJd-YgAAA2
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2rl&sid=cmLHL2b8fysJd-YgAAA2
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2rl&sid=cmLHL2b8fysJd-YgAAA2
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2rl&sid=cmLHL2b8fysJd-YgAAA2
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2rl&sid=cmLHL2b8fysJd-YgAAA2
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other	

Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2rl&sid=cmLHL2b8fysJd-YgAAA2
Method	POST
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2rl&sid=cmLHL2b8fysJd-YgAAA2
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM2rl&sid=cmLHL2b8fysJd-YgAAA2
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8IH&sid=gSgb1pCv77PedBXuAABG
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8IH&sid=gSgb1pCv77PedBXuAABG
Method	POST
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=PLhM8IH&sid=gSgb1pCv77PedBXuAABG
Method	POST
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=PLhM8IH&sid=gSgb1pCv77PedBXuAABG
Method	POST

Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8IH&sid=gSgb1pCv77PedBXuAABG
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8IH&sid=gSgb1pCv77PedBXuAABG
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8IH&sid=gSgb1pCv77PedBXuAABG
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8IH&sid=gSgb1pCv77PedBXuAABG
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8IH&sid=gSgb1pCv77PedBXuAABG
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8IH&sid=gSgb1pCv77PedBXuAABG
Method	POST
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8IH&sid=gSgb1pCv77PedBXuAABG
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PLhM8IH&sid=gSgb1pCv77PedBXuAABG
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	150
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104