ZAP Informes de Escaneo

Site: https://0beb-186-55-18-210.ngrok-free.app

Generated on Tue, 6 May 2025 16:29:58

ZAP Version: 2.16.1

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	8
Low	5

Alerts

Name	Risk Level	Number of Instances
CSP: Failure to Define Directive with No Fallback	Medium	1
CSP: script-src unsafe-inline	Medium	1
CSP: style-src unsafe-inline	Medium	1
Content Security Policy (CSP) Header Not Set	Medium	7
Cross-Domain Misconfiguration	Medium	36
Information Disclosure - JWT in Browser localStorage	Medium	3
Missing Anti-clickjacking Header	Medium	4
Session ID in URL Rewrite	Medium	13
Cross-Domain JavaScript Source File Inclusion	Low	5
Private IP Disclosure	Low	1
Strict-Transport-Security Header Not Set	Low	54
Timestamp Disclosure - Unix	Low	18
X-Content-Type-Options Header Missing	Low	13

Alert Detail

Medium	CSP: Failure to Define Directive with No Fallback
Description	The Content Security Policy fails to define one of the directives that has no fallback. Missing /excluding them is the same as allowing anything.
URL	https://0beb-186-55-18-210.ngrok-free.app/
Method	GET
Attack	
Evidence	default-src 'self' https://cdn.ngrok.com 'unsafe-eval' 'unsafe-inline'; img-src data: w3.org/svg /2000

Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	CSP: script-src unsafe-inline
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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	https://0beb-186-55-18-210.ngrok-free.app/
Method	GET
Attack	
Evidence	default-src 'self' https://cdn.ngrok.com 'unsafe-eval' 'unsafe-inline'; img-src data: w3.org/svg/2000
Other Info	script-src includes unsafe-inline.
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	CSP: style-src unsafe-inline
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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	https://0beb-186-55-18-210.ngrok-free.app/
Method	GET
Attack	

Evidence	default-src 'self' https://cdn.ngrok.com 'unsafe-eval' 'unsafe-inline'; img-src data: w3.org/svg /2000
Other Info	style-src includes unsafe-inline.
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**Content Security Policy (CSP) Header Not Set**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://0beb-186-55-18-210.ngrok-free.app/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcY__O
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcZ1B5
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/rest/user/login
Method	POST
Attack	
Evidence	
Other Info	

URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcRAu_&sid=y2kAw6sy8UpAEDc-AAAE
Method	POST
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2fL-&sid=lSw1Y6_voLBrTtBzAAAC
Method	POST
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2oFJ&sid=v9frk5rKtcuvg6ZkAAAE
Method	POST
Attack	
Evidence	
Other Info	
Instances	7
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	https://0beb-186-55-18-210.ngrok-free.app/
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	https://0beb-186-55-18-210.ngrok-free.app/705.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	https://0beb-186-55-18-210.ngrok-free.app/api/Addresss
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	https://0beb-186-55-18-210.ngrok-free.app/api/Addresss/7
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	https://0beb-186-55-18-210.ngrok-free.app/api/BasketItems/9
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	https://0beb-186-55-18-210.ngrok-free.app/api/Cards
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	https://0beb-186-55-18-210.ngrok-free.app/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	https://0beb-186-55-18-210.ngrok-free.app/api/Deliverys
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	https://0beb-186-55-18-210.ngrok-free.app/api/Deliverys/1
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	https://0beb-186-55-18-210.ngrok-free.app/api/Products/24?d=Tue%20May%2006%202025
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	https://0beb-186-55-18-210.ngrok-free.app/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	https://0beb-186-55-18-210.ngrok-free.app/api/SecurityQuestions/
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	https://0beb-186-55-18-210.ngrok-free.app/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	https://0beb-186-55-18-210.ngrok-free.app/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	https://0beb-186-55-18-210.ngrok-free.app/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	https://0beb-186-55-18-210.ngrok-free.app/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	https://0beb-186-55-18-210.ngrok-free.app/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	https://0beb-186-55-18-210.ngrok-free.app/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	https://0beb-186-55-18-210.ngrok-free.app/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	https://0beb-186-55-18-210.ngrok-free.app/rest/basket/6
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	https://0beb-186-55-18-210.ngrok-free.app/rest/continue-code
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	https://0beb-186-55-18-210.ngrok-free.app/rest/languages
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	https://0beb-186-55-18-210.ngrok-free.app/rest/products/24/reviews
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	https://0beb-186-55-18-210.ngrok-free.app/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	https://0beb-186-55-18-210.ngrok-free.app/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	https://0beb-186-55-18-210.ngrok-free.app/rest/wallet/balance
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	https://0beb-186-55-18-210.ngrok-free.app/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	https://0beb-186-55-18-210.ngrok-free.app/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	https://0beb-186-55-18-210.ngrok-free.app/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.
URL	https://0beb-186-55-18-210.ngrok-free.app/api/Addresss/
Method	POST
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	https://0beb-186-55-18-210.ngrok-free.app/api/BasketItems/
Method	POST
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	https://0beb-186-55-18-210.ngrok-free.app/api/Complaints/
Method	POST
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	https://0beb-186-55-18-210.ngrok-free.app/api/SecurityAnswers/
Method	POST
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	https://0beb-186-55-18-210.ngrok-free.app/api/Users/
Method	POST
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	https://0beb-186-55-18-210.ngrok-free.app/rest/user/login
Method	POST
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	https://0beb-186-55-18-210.ngrok-free.app/api/BasketItems/9
Method	PUT
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	36
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	**Information Disclosure - JWT in Browser localStorage**
Description	JWT was stored in browser localStorage. This is dangerous because data stored in localStorage does not expire. .
URL	https://0beb-186-55-18-210.ngrok-free.app/#/search
Method	GET
Attack	
Evidence	
Other Info	The following JWT was set: Key: token Header: {"typ":"JWT","alg":"RS256"} Payload: {"status":" /uploads/default.svg","totpSecret":"","isActive":true,"createdAt":"2025-05-06 16:28:37.778 +00:0 98c7e469ffe27671a13063115c5aeae172ff07861971c588826f381716c460a05035c63009c2d00 Note that this alert will only be raised once for each URL + key.
URL	https://0beb-186-55-18-210.ngrok-free.app/#/search
Method	GET
Attack	
Evidence	
Other Info	The following JWT was set: Key: token Header: {"typ":"JWT","alg":"RS256"} Payload: {"status":" /uploads/default.svg","totpSecret":"","isActive":true,"createdAt":"2025-05-06 19:23:23.697 +00:0 9528c5a2943796cd908b3e41394187438a6368b1e6f9212900a0cae34d9210685fd3e04561926 Note that this alert will only be raised once for each URL + key.
URL	https://0beb-186-55-18-210.ngrok-free.app/profile
Method	GET
Attack	
Evidence	
Other Info	The following JWT was set: Key: token Header: {"typ":"JWT","alg":"RS256"} Payload: {"status":" /uploads/default.svg","totpSecret":"","isActive":true,"createdAt":"2025-05-06 19:23:23.697 +00:0 9528c5a2943796cd908b3e41394187438a6368b1e6f9212900a0cae34d9210685fd3e04561926 Note that this alert will only be raised once for each URL + key.
Instances	3
Solution	This is an informational alert and no action is necessary.
Reference	https://www.zaproxy.org/blog/2020-09-03-zap-jwt-scanner/
CWE Id	922
WASC Id	13
Plugin Id	120002

Medium	**Missing Anti-clickjacking Header**
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	https://0beb-186-55-18-210.ngrok-free.app/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcRAu_&sid=y2kAw6sy8UpAEDc-AAAE
Method	POST

Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2fL-&sid=lSw1Y6_voLBrTtBzAAAC
Method	POST
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2oFJ&sid=v9frk5rKtcuvg6ZkAAAE
Method	POST
Attack	
Evidence	
Other Info	
Instances	4
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	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcRAv8&sid=y2kAw6sy8UpAEDc-AAAE
Method	GET
Attack	
Evidence	y2kAw6sy8UpAEDc-AAAE
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcRBPd&sid=y2kAw6sy8UpAEDc-AAAE
Method	GET
Attack	
Evidence	y2kAw6sy8UpAEDc-AAAE
Other Info	

URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2fM1&sid=lSw1Y6_voLBrTtBzAAAC
Method	GET
Attack	
Evidence	lSw1Y6_voLBrTtBzAAAC
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2fmC&sid=lSw1Y6_voLBrTtBzAAAC
Method	GET
Attack	
Evidence	lSw1Y6_voLBrTtBzAAAC
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2gQ9&sid=lSw1Y6_voLBrTtBzAAAC
Method	GET
Attack	
Evidence	lSw1Y6_voLBrTtBzAAAC
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2oJ8&sid=v9frk5rKtcuvg6ZkAAAE
Method	GET
Attack	
Evidence	v9frk5rKtcuvg6ZkAAAE
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2p3B&sid=v9frk5rKtcuvg6ZkAAAE
Method	GET
Attack	
Evidence	v9frk5rKtcuvg6ZkAAAE
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=websocket&sid=lSw1Y6_voLBrTtBzAAAC
Method	GET
Attack	
Evidence	lSw1Y6_voLBrTtBzAAAC
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=websocket&sid=v9frk5rKtcuvg6ZkAAAE
Method	GET
Attack	
Evidence	v9frk5rKtcuvg6ZkAAAE

Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=websocket&sid=y2kAw6sy8UpAEDc-AAAE
Method	GET
Attack	
Evidence	y2kAw6sy8UpAEDc-AAAE
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcRAu_&sid=y2kAw6sy8UpAEDc-AAAE
Method	POST
Attack	
Evidence	y2kAw6sy8UpAEDc-AAAE
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2fL-&sid=lSw1Y6_voLBrTtBzAAAC
Method	POST
Attack	
Evidence	lSw1Y6_voLBrTtBzAAAC
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2oFJ&sid=v9frk5rKtcuvg6ZkAAAE
Method	POST
Attack	
Evidence	v9frk5rKtcuvg6ZkAAAE
Other Info	
Instances	13
Solution	For secure content, put session ID in a cookie. To be even more secure consider using a combination of cookie and URL rewrite.
Reference	https://seclists.org/webappsec/2002/q4/111
CWE Id	598
WASC Id	13
Plugin Id	3

Low	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	https://0beb-186-55-18-210.ngrok-free.app/
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	

URL	https://0beb-186-55-18-210.ngrok-free.app/
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/
Method	GET
Attack	
Evidence	<script id="script" src="https://cdn.ngrok.com/static/js/error.js" type="text/javascript"></script>
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcY__O
Method	GET
Attack	
Evidence	<script id="script" src="https://cdn.ngrok.com/static/js/error.js" type="text/javascript"></script>
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcZ1B5
Method	GET
Attack	
Evidence	<script id="script" src="https://cdn.ngrok.com/static/js/error.js" type="text/javascript"></script>
Other Info	
Instances	5
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	https://0beb-186-55-18-210.ngrok-free.app/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	497
WASC Id	13
Plugin Id	2

Low	**Strict-Transport-Security Header Not Set**
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://0beb-186-55-18-210.ngrok-free.app/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/705.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/api/Addresss
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/api/Addresss/7
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/api/BasketItems/9
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/api/Cards
Method	GET
Attack	

Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/api/Challenges/?name=Score%20Board
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/api/Deliverys
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/api/Deliverys/1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/api/Products/24?d=Tue%20May%2006%202025
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/api/Quantitys/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/api/SecurityQuestions/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/assets/i18n/en.json
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/font-mfizz.woff
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/main.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/MaterialIcons-Regular.woff2
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/polyfills.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/rest/admin/application-configuration
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/rest/admin/application-version
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/rest/basket/6
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/rest/continue-code

Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/rest/languages
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/rest/products/24/reviews
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/rest/products/search?q=
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/rest/user/whoami
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/rest/wallet/balance
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/runtime.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcRARR
Method	GET

Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcRAv8&sid=y2kAw6sy8UpAEDc-AAAE
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcRBPd&sid=y2kAw6sy8UpAEDc-AAAE
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcY__O
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcZ1B5
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2ehK
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2fM1&sid=lSw1Y6_voLBrTtBzAAAC
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2fmC&sid=lSw1Y6_voLBrTtBzAAAC
Method	GET

Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2gQ9&sid=lSw1Y6_voLBrTtBzAAAC
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2nxr
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2oJ8&sid=v9frk5rKtcuvg6ZkAAAE
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2p3B&sid=v9frk5rKtcuvg6ZkAAAE
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=websocket&sid=lSw1Y6_voLBrTtBzAAAC
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=websocket&sid=v9frk5rKtcuvg6ZkAAAE
Method	GET
Attack	
Evidence	
Other Info	
	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?

URL	EIO=4&transport=websocket&sid=y2kAw6sy8UpAEDc-AAAE
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/styles.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/vendor.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/api/Addresss/
Method	POST
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/api/BasketItems/
Method	POST
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/api/Complaints/
Method	POST
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/api/SecurityAnswers/
Method	POST
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/api/Users/
Method	POST

Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/rest/user/login
Method	POST
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcRAu_&sid=y2kAw6sy8UpAEDc-AAAE
Method	POST
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2fL-&sid=lSw1Y6_voLBrTtBzAAAC
Method	POST
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2oFJ&sid=v9frk5rKtcuvg6ZkAAAE
Method	POST
Attack	
Evidence	
Other Info	
URL	https://0beb-186-55-18-210.ngrok-free.app/api/BasketItems/9
Method	PUT
Attack	
Evidence	
Other Info	
Instances	54
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319

WASC Id	15
Plugin Id	10035

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://0beb-186-55-18-210.ngrok-free.app/
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 17:10:37.
URL	https://0beb-186-55-18-210.ngrok-free.app/
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 16:35:49.
URL	https://0beb-186-55-18-210.ngrok-free.app/
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 12:02:31.
URL	https://0beb-186-55-18-210.ngrok-free.app/main.js
Method	GET
Attack	
Evidence	1734944650
Other Info	1734944650, which evaluates to: 2024-12-23 06:04:10.
URL	https://0beb-186-55-18-210.ngrok-free.app/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1969196030
Other Info	1969196030, which evaluates to: 2032-05-26 11:53:50.
URL	https://0beb-186-55-18-210.ngrok-free.app/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1970691216
Other Info	1970691216, which evaluates to: 2032-06-12 19:13:36.
URL	https://0beb-186-55-18-210.ngrok-free.app/rest/products/search?q=
Method	GET
Attack	

Evidence	1969196030
Other Info	1969196030, which evaluates to: 2032-05-26 11:53:50.
URL	https://0beb-186-55-18-210.ngrok-free.app/rest/products/search?q=
Method	GET
Attack	
Evidence	1970691216
Other Info	1970691216, which evaluates to: 2032-06-12 19:13:36.
URL	https://0beb-186-55-18-210.ngrok-free.app/styles.css
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 17:10:37.
URL	https://0beb-186-55-18-210.ngrok-free.app/styles.css
Method	GET
Attack	
Evidence	1680327869
Other Info	1680327869, which evaluates to: 2023-04-01 02:44:29.
URL	https://0beb-186-55-18-210.ngrok-free.app/styles.css
Method	GET
Attack	
Evidence	1701244813
Other Info	1701244813, which evaluates to: 2023-11-29 05:00:13.
URL	https://0beb-186-55-18-210.ngrok-free.app/styles.css
Method	GET
Attack	
Evidence	1818181818
Other Info	1818181818, which evaluates to: 2027-08-13 15:30:18.
URL	https://0beb-186-55-18-210.ngrok-free.app/styles.css
Method	GET
Attack	
Evidence	1839622642
Other Info	1839622642, which evaluates to: 2028-04-17 19:17:22.
URL	https://0beb-186-55-18-210.ngrok-free.app/styles.css
Method	GET
Attack	
Evidence	1863874346
Other	

Info	1863874346, which evaluates to: 2029-01-23 11:52:26.
URL	https://0beb-186-55-18-210.ngrok-free.app/styles.css
Method	GET
Attack	
Evidence	1917098446
Other Info	1917098446, which evaluates to: 2030-10-01 12:20:46.
URL	https://0beb-186-55-18-210.ngrok-free.app/styles.css
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 16:35:49.
URL	https://0beb-186-55-18-210.ngrok-free.app/styles.css
Method	GET
Attack	
Evidence	2033195021
Other Info	2033195021, which evaluates to: 2034-06-06 05:23:41.
URL	https://0beb-186-55-18-210.ngrok-free.app/styles.css
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 12:02:31.
Instances	18
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
Plugin Id	10096

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcRARR
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	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcRAv8&sid=y2kAw6sy8UpAEDc-AAAE
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcRBPd&sid=y2kAw6sy8UpAEDc-AAAE
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2ehK
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2fM1&sid=ISw1Y6_voLBrTtBzAAAC
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2fmC&sid=ISw1Y6_voLBrTtBzAAAC
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2gQ9&sid=ISw1Y6_voLBrTtBzAAAC
Method	GET
Attack	

Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2nxr
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2oJ8&sid=v9frk5rKtcuvg6ZkAAAE
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2p3B&sid=v9frk5rKtcuvg6ZkAAAE
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQcRAu_&sid=y2kAw6sy8UpAEDc-AAAE
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2fL-&sid=lSw1Y6_voLBrTtBzAAAC
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://0beb-186-55-18-210.ngrok-free.app/socket.io/?EIO=4&transport=polling&t=PQd2oFJ&sid=v9frk5rKtcuvg6ZkAAAE

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	13
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