Security Headers   Home   Abc

Sponsored by

Scan your site now

https://playground.dev.msdevopsdude.c	Scan

☐ Hide results   ☑ Follow redirects

Security Report Summary

A	**Site:**	https://playground.dev.msdevopsdude.com/
	IP Address:	2620:1ec:bdf::10
	Report Time:	03 May 2020 10:33:56 UTC
	Headers:	✔ Feature-Policy ✔ Content-Security-Policy ✔ Strict-Transport-Security ✔ X-Content-Type-Optio ✔ X-Frame-Options ✔ Referrer-Policy
	Warning:	Grade capped at A, please see warnings below.

Supported By

Report URI	Quickly and easily enable reporting for CSP and other Security Headers!	Get Starte

Raw Headers

HTTP/1.1	200 OK
Cache-Control	public, max-age=604800
Content-Length	2372
Content-Type	text/html; charset=utf-8
Content-MD5	JTb2VdIC1vih3OAFXO07Ig==
Last-Modified	Sun, 03 May 2020 09:38:27 GMT
ETag	0x8D7EF45BB904F80
X-Cache	TCP_MISS
x-ms-request-id	efbae133-501e-0097-0836-214d95000000
x-ms-version	2009-09-19
x-ms-lease-status	unlocked
x-ms-blob-type	BlockBlob
X-Azure-Ref	0E56uXgAAAACuaEqpishvSZEvtlQM9O4nU0pDRURHRTA1MTkAMjgwZTc0YzYtNTU3YS00ODNmLWJmNDQtNzNlYWNmNDg3ZTJm
Feature-Policy	**payment** 'self'; **geolocation** 'self';
Content-Security-Policy	**script-src** 'self' 'unsafe-inline'; **style-src** 'self' 'unsafe-inline' https://fonts.googleapis.com;
X-XSS-Protection	**1**; **mode**=block
Strict-Transport-Security	**max-age**=31536000; **includeSubDomains**
X-Content-Type-Options	**nosniff**
x-frame-options	**SAMEORIGIN**
Referrer-Policy	**same-origin**
Date	Sun, 03 May 2020 10:33:55 GMT

Warnings

| **Content-Security-Policy** | This policy contains 'unsafe-inline' which is dangerous in the script-src directive. This policy contains 'unsafe-inline' which is dangerou src directive. |

Upcoming Headers

| **Expect-CT** | Expect-CT allows a site to determine if they are ready for the upcoming Chrome requirements and/or enforce their CT policy. |

Additional Information

Feature-Policy	Feature Policy is a new header that allows a site to control which features and APIs can be used in the browser.
Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you browser from loading malicious assets. Analyse this policy in more detail. You can sign up for a free account on Report URI to collect re problems on your site.
X-XSS-Protection	X-XSS-Protection sets the configuration for the XSS Auditor built into older browser. The recommended value was "X-XSS-Protection: 1 but you should now look at Content Security Policy instead.
Strict-Transport-Security	HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting tl to enforce the use of HTTPS.
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-typ valid value for this header is "X-Content-Type-Options: nosniff".
x-frame-options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing yoi defend against attacks like clickjacking.
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a should be set by all sites.