Security Headers
Powered by Probely

Home Abo

Scan your site now

site.sassieshop.com Scan

Hide results Follow redirects

Security Report Summary

A

Site:	https://site.sassieshop.com/
IP Address:	104.199.122.126
Report Time:	18 Sep 2023 19:02:47 UTC
Headers:	✔ Content-Security-Policy ✔ X-Content-Type-Options ✔ X-Frame-Options ✔ Referrer-Policy ✔ Strict-Transport-Security ✖ Permissions-Policy
Warning:	Grade capped at A, please see warnings below.
Advanced:	Great grade! Perform a deeper security analysis of your website and APIs: Try Now

Missing Headers

Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Warnings

Content-Security-Policy	This policy contains 'unsafe-inline' which is dangerous in the script-src directive. This policy contains 'unsafe-eval' which is dangerous in the s directive. This policy contains 'unsafe-inline' which is dangerous in the style-src directive.
Referrer-Policy	The "origin" value is not recommended.

Raw Headers

HTTP/2	200
server	nginx
date	Mon, 18 Sep 2023 19:02:47 GMT
content-type	text/html; charset=UTF-8
vary	Accept-Encoding
vary	Accept-Encoding
vary	Accept-Encoding
content-security-policy	**default-src** *'self'*; **frame-src** *'self'* https://*.google.com https://*.gstatic.com; **script-src** *'unsafe-inline' 'unsafe-eval'* http:; **style-src** *'unsafe-inline* **img-src** http: data:; **font-src** http: data:; **sandbox** allow-forms allow-scripts
link	<https://site.sassieshop.com/wp-json/>; rel="https://api.w.org/"
link	<https://site.sassieshop.com/wp-json/wp/v2/pages/11>; rel="alternate"; type="application/json"
link	<https://site.sassieshop.com/>; rel=shortlink
x-powered-by	WP Engine

x-cacheable	SHORT
vary	Accept-Encoding,Cookie
cache-control	max-age=600, must-revalidate
x-cache	HIT: 3
x-cache-group	normal
x-content-type-options	**nosniff**
x-frame-options	**SAMEORIGIN**
x-xss-protection	**1**; **mode**=block
referrer-policy	**origin**
strict-transport-security	**max-age**=63072000; **includeSubDomains**
content-encoding	gzip

Upcoming Headers

Cross-Origin-Embedder-Policy	Cross-Origin Embedder Policy allows a site to prevent assets being loaded that do not grant permission to load them via CORS or CORP.
Cross-Origin-Opener-Policy	Cross-Origin Opener Policy allows a site to opt-in to Cross-Origin Isolation in the browser.
Cross-Origin-Resource-Policy	Cross-Origin Resource Policy allows a resource owner to specify who can load the resource.

Additional Information

server	This Server header seems to advertise the software being run on the server but you can remove or change this value.
content-security-policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can pr browser from loading malicious assets. Analyse this policy in more detail. You can sign up for a free account on Report URI to collect reports problems on your site.
x-powered-by	X-Powered-By can usually be seen with values like "PHP/5.5.9-1ubuntu4.5" or "ASP.NET". Trying to minimise the amount of information you g about your server is a good idea. This header seems to have been altered to remove such information, but could still be removed.
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-type. The 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 your site defend against attacks like clickjacking.
x-xss-protection	X-XSS-Protection sets the configuration for the XSS Auditor built into older browsers. The recommended value was "X-XSS-Protection: 1; mod but you should now look at Content Security Policy instead.
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 docun should be set by all sites.
strict-transport-security	HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the Use to enforce the use of HTTPS.