Scan your site now

https://rubberduckiesft Scan

Hide results Follow redirects

Security Report Summary

A

Site:	https://rubberduckiesftw.wpcomstaging.com/
IP Address:	192.0.78.20
Report Time:	01 Dec 2024 02:59:20 UTC
Headers:	✔ X-Frame-Options ✔ X-Content-Type-Options ✔ Referrer-Policy ✔ Permissions-Policy ✔ Strict-Transport-Security ✖ Content-Security-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

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 prevent the browser from loading malicious assets.

Warnings

Referrer-Policy	The "origin-when-cross-origin" value is not recommended.

Raw Headers

HTTP/2	200
server	nginx
date	Sun, 01 Dec 2024 02:59:19 GMT
content-type	text/html; charset=UTF-8
vary	Accept-Encoding
x-hacker	Want root? Visit join.a8c.com and mention this header.
host-header	WordPress.com
set-cookie	PHPSESSID=7868364253bb78b172010a2c5bd3c3f7; path=/
expires	Thu, 19 Nov 1981 08:52:00 GMT
cache-control	no-store, no-cache, must-revalidate
pragma	no-cache
vary	accept, content-type, cookie
x-frame-options	**sameorigin**
x-xss-protection	1
x-content-type-options	**nosniff**
referrer-policy	**origin-when-cross-origin**
permissions-policy	**accelerometer**=(self), **autoplay**=(self), **camera**=(self), **encrypted-media**=(self), **fullscreen**=(self), **geolocation**=(self), **gyroscope**=(self), **magnetometer**=(self), **microphone**=(self), **midi**=(self), **payment**=(self), **usb**=(self)
link	<https://rubberduckiesftw.wpcomstaging.com/wp-json/>; rel="https://api.w.org/"
link	<https://wp.me/g9OBf>; rel=shortlink
content-encoding	gzip
x-ac	2.lhr _atomic_ams MISS
strict-transport-security	**max-age**=31536000; **includeSubDomains**; **preload**

alt-svc	h3=":443"; ma=86400

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.
set-cookie	The 'httpOnly' flag is not set on this cookie. The 'secure' flag is not set on this cookie. There is no Cookie Prefix on this cookie. This is not a SameSite Cookie.
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 you can 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; mode=block" but you should now look at Content Security Policy instead.
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 only valid value for this header is "X-Content-Type-Options: nosniff".
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 document and should be set by all sites.
permissions-policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.
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 User Agent to enforce the use of HTTPS.