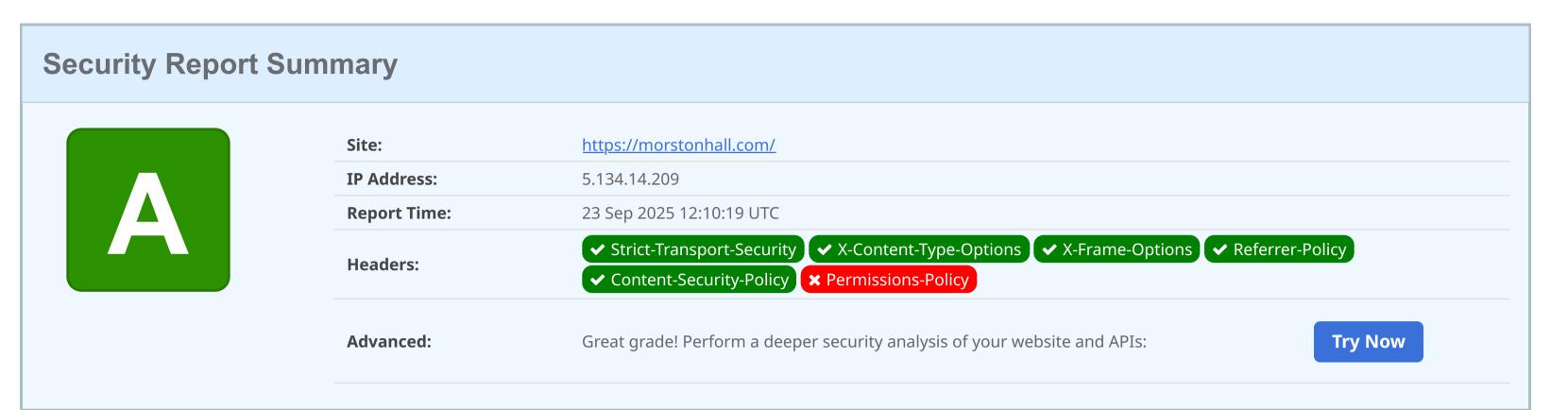


## Scan your site now

https://morstonhall.com Scan ■ Hide results **☑** Follow redirects



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.

aw Headers	
HTTP/2	200
content-type	text/html; charset=UTF-8
ink	<a "<="" api.w.org="" href="https://morstonhall.com/wp-json/&gt;; rel=" https:="" td=""></a>
ink	<a ;="" <="" alternate";="" href="https://morstonhall.com/wp-json/wp/v2/pages/65&gt;; rel=" td="" title="JSON" type="application/json"></a>
ink	<https: morstonhall.com=""></https:> ; rel=shortlink
ત-litespeed-cache-control	public,max-age=604800
र-litespeed-tag	08e_front,08e_URL.6666cd76f96956469e7be39d750cc7d9,08e_F,08e_Po.65,08e_PGS,08e_
etag	"41-1758629419;gz"
ห-litespeed-cache	miss
content-encoding	gzip
vary	Accept-Encoding
date	Tue, 23 Sep 2025 12:10:19 GMT
strict-transport-security	max-age=31536000; includeSubDomains
x-content-type-options	nosniff
x-frame-options	SAMEORIGIN
referrer-policy	strict-origin-when-cross-origin
content-security-policy	upgrade-insecure-requests; frame-ancestors 'self'; base-uri 'self'
alt-svc	h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"

Upcoming Headers	
Cross-Origin-Embedder-Policy	<u>Cross-Origin Embedder Policy</u> 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	<u>Cross-Origin Resource Policy</u> allows a resource owner to specify who can load the resource.

Additional Information		
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.	
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".	
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.	
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.	
content-security-policy	<u>Content Security Policy</u> 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. <u>Analyse</u> this policy in more detail. You can sign up for a free account on <u>Report URI</u> to collect reports about problems on your site.	

A <u>snyk.io</u> project - <u>CC-BY-SA 4.0</u> Powered by <u>Snyk</u>