Scan your site now

bbsillc.com Scan

Hide results Follow redirects

Security Report Summary

A

Site:	https://bbsillc.com/
IP Address:	160.153.0.165
Report Time:	29 Oct 2026 02:57:01 UTC
Headers:	✔ Content-Security-Policy ✔ Permissions-Policy ✔ Referrer-Policy ✔ Strict-Transport-Security ✔ X-Content-Type-Options ✔ X-Frame-Options
Warning:	Grade capped at A, please see warnings below.
Advanced:	Great grade! Perform a deeper security analysis of your website and APIs: Try Now

Warnings

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

Raw Headers

HTTP/2	200
date	Thu, 29 Oct 2026 02:57:01 GMT
content-type	text/html; charset=utf-8
cache-control	no-cache
content-security-policy	**default-src** 'self'; **script-src** 'self' 'unsafe-inline' https://www.googletagmanager.com https://www.google-analytics.com; **style-src** 'self' 'unsafe https://fonts.googleapis.com https://unpkg.com; **font-src** 'self' https://fonts.gstatic.com data:; **img-src** 'self' data: blob: https://www.google-analytics.com https://www.googletagmanager.com https://airo-assets.imgix.net https://*.airoapp.ai https://img1.wsimg.com https://*.wsimg.c https://server.arcgisonline.com; **media-src** 'self' blob: https://airo-assets.imgix.net https://*.airoapp.ai https://blobby.wsimg.com https://*.wsim **connect-src** 'self' https://www.google-analytics.com https://analytics.google.com https://www.googletagmanager.com https://server.arcgisonl **frame-src** 'self' blob:; **object-src** 'self' blob:; **base-uri** 'self'; **form-action** 'self'; upgrade-insecure-requests
etag	W/"15697-H9bi+jhU+IoUvqO9tAkUC3dL1Wk"
permissions-policy	**camera**=(), **microphone**=(), **geolocation**=(), **payment**=()
referrer-policy	**strict-origin-when-cross-origin**
ss-product-id	aab-v1
strict-transport-security	**max-age**=31536000; **includeSubDomains**
vary	Origin
x-content-type-options	**nosniff**
x-frame-options	**DENY**
x-powered-by	Express
x-request-id	b2ff415b656fd778

cf-cache-status	DYNAMIC
set-cookie	__cf_bm=Hd_MX7iqXLjV9.4s1xk.OY9Bx_IDO2W1M5TJ5qrU824-1793242620.9671915-1.0.1.1-beMRN7WV6VJbF98VXqJZlXAxcricHbH7per9Dt2BhzJ3DFspbfsvNcLd5ej_NILaeMooei9X58JAwFFrUboAWMSSXbyv29WNP9C_aippDQes0YuQRUqFVwX; **HttpOnly**; **SameSite**=None; **Secure**; Path=/; Domain=bbsillc.com; Expires=Thu, 29 Oct 2026 03:27:01 GMT
content-encoding	gzip
server	cloudflare
cf-ray	a51ee90d0b6abe09-DUB

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

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 prev 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 abo lems on your site.
permissions-policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.
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 documen 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 User A 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 o 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 yo fend against attacks like clickjacking.
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 give your server is a good idea. This header should be removed or the value changed.
server	Server value has been changed. Typically you will see values like "Microsoft-IIS/8.0" or "nginx 1.7.2".