HTTP Observatory Report

ⓘ Report Feedback

Scan summary: safetynetbeta.com

B

Score: 75 / 100
Scan Time: Just now
Tests Passed: 8 / 10

Scan results

Scoring

Test	Score	Reason	Recommendation
Content Security Policy (CSP)	-20 ✗	Content Security Policy (CSP) implemented unsafely. This includes `'unsafe-inline'` or `data:` inside `script-src`, overly broad sources such as `https:` inside `object-src` or `script-src`, or not restricting the sources for `object-src` or `script-src`.	Remove `unsafe-inline` and `da` `script-src`, overly broad sour `object-src` and `script-src`, a `object-src` and `script-src` a
Cookies	-	No cookies detected	None
Cross Origin Resource Sharing (CORS)	0 ✓	Content is not visible via cross-origin resource sharing (CORS) files or headers.	None
Redirection	0 ✓	Initial redirection is to HTTPS on same host, final destination is HTTPS	None
Referrer Policy	0* ✓	`Referrer-Policy` header set to `no-referrer`, `same-origin`, `strict-origin` or `strict-origin-when-cross-origin`.	None
Strict Transport Security (HSTS)	0 ✓	`Strict-Transport-Security` header set to a minimum of six months (15768000).	Consider preloading: this requ the `preload` and `includeSubDo` directives and setting `max-age` `31536000` (1 year), and submitt to https://hstspreload.org/.

Test	Score	Reason	Recommendation
Subresource Integrity	-5 ✗	Subresource Integrity (SRI) not implemented, but all external scripts are loaded over HTTPS.	Add SRI to external scripts.
X-Content-Type-Options	0 ✓	**`X-Content-Type-Options`** header set to **`nosniff`**.	None
X-Frame-Options	0* ✓	**`X-Frame-Options`** (XFO) implemented via the CSP frame-ancestors directive.	None
Cross Origin Resource Policy	-	Cross Origin Resource Policy (CORP) is not implemented (defaults to **`cross-origin`**).	None

* Normally awards bonus points, however, in this case they are not included in the overall score (find out why).

CSP analysis

✗ Content Security Policy (CSP) implemented unsafely. This includes **`'unsafe-inline'`** or **`data:`** inside **`script-src`**, overly broad sources such as **`https:`** inside **`object-src`** or **`script-src`**, or not restricting the sources for **`object-src`** or **`script-src`**.

Test	Result	Info
Blocks execution of inline JavaScript by not allowing **`'unsafe-inline'`** inside **`script-src`**	✗	Blocking the execution of inline JavaScript provid strongest protection against cross-site scripting a Moving JavaScript to external files can also help i site more maintainable.
Blocks execution of JavaScript's **`eval()`** function by not allowing **`'unsafe-eval'`** inside **`script-src`**	✗	Blocking the use of JavaScript's **`eval()`** function prevent the execution of untrusted code.
Blocks execution of plug-ins, using **`object-src`** restrictions	✓	Blocking the execution of plug-ins via **`object-src`** as inherited from **`default-src`** can prevent attack loading Flash or Java in the context of your page.
Blocks inline styles by not allowing **`'unsafe-inline'`** inside **`style-src`**	✗	Blocking inline styles can help prevent attackers f modifying the contents or appearance of your pag styles to external stylesheets can also help make more maintainable.
Blocks loading of active content over HTTP or FTP	✓	Loading JavaScript or plugins can allow a man-in- to execute arbitrary code or your website. Restrict policy and changing links to HTTPS can help prev
Blocks loading of passive content over HTTP or FTP	✓	This site's Content Security Policy allows the load passive content such as images or videos over ins

Test	Result	Info
		protocols such as HTTP or FTP. Consider changir load them over HTTPS.
Clickjacking protection, using **`frame-ancestors`**	✓	The use of CSP's **`frame-ancestors`** directive offer grained control over who can frame your site.
Deny by default, using **`default-src 'none'`**	✗	Denying by default using **`default-src 'none'`** car your Content Security Policy doesn't allow the loa resources you didn't intend to allow.
Restricts use of the **`<base>`** tag by using **`base-uri 'none'`**, **`base-uri 'self'`**, or specific origins.	✗	The **`<base>`** tag can be used to trick your site into scripts from untrusted origins.
Restricts where **`<form>`** contents may be submitted by using **`form-action 'none'`**, **`form-action 'self'`**, or specific URIs	✗	Malicious JavaScript or content injection could m sensitive form data is submitted to or create addit for data exfiltration.
Uses CSP3's **`'strict-dynamic'`** directive to allow dynamic script loading (optional)	-	**`'strict-dynamic'`** lets you use a JavaScript shim load all your site's JavaScript dynamically, withou track **`script-src`** origins.

Cookies

No cookies detected

Raw server headers

Header	Value
Age	0
Nel	{"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Date	Sat, 03 Jan 2026 05:12:32 GMT
Vary	accept-encoding
Cf-Ray	9b800072ae95682e-SEA
Server	cloudflare
Alt-Svc	h3=":443"; ma=86400

Report-To	{"group":"cf-nel","max_age":604800,"endpoints":
	[{"url":"https://a.nel.cloudflare.com/report/v4?
	s=mhs01lBkbd8Mtr9OzevTuUSaj7GeFqRy4qswK3WV2soVWgNeFzJfhipNEn1vg
	usDwR3kXdcZOtgINSnZ49jteoVtEDiU23vA%3D%3D"}]}

Connection	close

Header	Value
X-Vercel-Id	pdx1::xs8hw-1767417152564-1de86d988ab6
Content-Type	text/html; charset=utf-8
Cache-Control	public, max-age=0, must-revalidate
Last-Modified	Sat, 03 Jan 2026 05:12:32 GMT
Server-Timing	cfCacheStatus;desc="DYNAMIC", cfEdge;dur=8,cfOrigin;dur=415
X-Vercel-Cache	HIT
Cf-Cache-Status	DYNAMIC
Referrer-Policy	strict-origin-when-cross-origin
X-Frame-Options	DENY
X-Xss-Protection	1; mode=block
Transfer-Encoding	chunked
Permissions-Policy	camera=(), microphone=(), geolocation=()
Content-Disposition	inline
X-Content-Type-Options	nosniff
Content-Security-Policy	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.tailwi https://www.google.com https://www.gstatic.com https://challenges.cloudflare https://static.cloudflareinsights.com https://vercel.live; style-src 'self' 'unsafe-i https://fonts.googleapis.com; font-src 'self' https://fonts.gstatic.com; img-src ' https:; connect-src 'self' https://*.supabase.co https://www.google.com https://www.gstatic.com https://challenges.cloudflare.com https://static.cloudflareinsights.com https://safetynet-signup.campbell-mccord.workers.dev https://vercel.live; frame-src https://www.google.com https://www.gstatic.com https://challenges.cloudflare.com https://vercel.live; f ancestors 'none';
Strict-Transport-Security	max-age=31536000; includeSubDomains
Access-Control-Allow-Origin	*

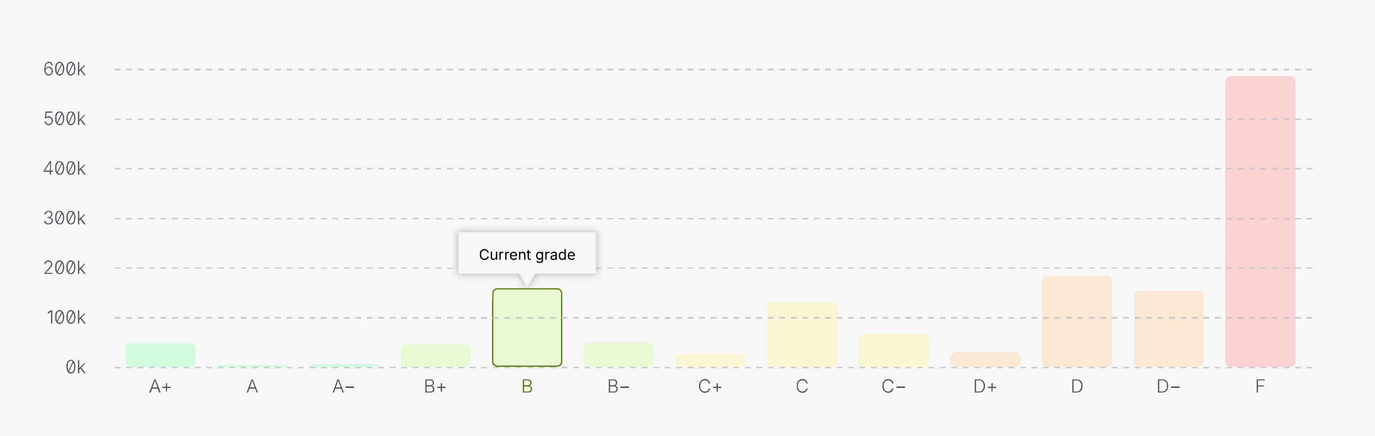
Scan history

Changes in score over time

Date	Score	Gra
3 Jan 2026, 12:12:32	75	B

Benchmark comparison

Performance trends from the past year



Refer to this graph to assess the website's current status. By following the recommendations provided and rescanning, you can expect an improvement in the website's grade.

Your blueprint for a better internet.