HTTP Observatory Report

Report Feedback

Scan summary: test-sso.cfia.or.cr/sso

B

Score: 70 / 100
Scan Time: Just now
Tests Passed: 7 / 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 **data:** **script-src**, overly broad sources **object-src** and **script-src**, and **object-src** and **script-src** are s
Cookies	0* ✓	All cookies use the **Secure** flag, session cookies use the **HttpOnly** flag, and cross-origin restrictions are in place via the **SameSite** flag.	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

Test	Score	Reason	Recommendation
Strict Transport Security (HSTS)	0 ✓	**Strict-Transport-Security** header set to a minimum of six months (15768000).	Consider preloading: this requires the **preload** and **includeSubDomai** directives and setting **max-age** to a **31536000** (1 year), and submitting to https://hstspreload.org/.
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	−5 ✗	**X-Content-Type-Options** header not implemented.	Set to **nosniff**.
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 provides C strongest protection against cross-site scripting attac Moving JavaScript to external files can also help mak 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 can prevent the execution of untrusted code.
Blocks execution of plug-ins, using **object-src** restrictions	✓	Blocking the execution of plug-ins via **object-src 'n** as inherited from **default-src** can prevent attackers loading Flash or Java in the context of your page.

Test	Result	Info
Blocks inline styles by not allowing `'unsafe-inline'` inside `style-src`	✗	Blocking inline styles can help prevent attackers from modifying the contents or appearance of your page. M styles to external stylesheets can also help make you more maintainable.
Blocks loading of active content over HTTP or FTP	✓	Loading JavaScript or plugins can allow a man-in-the to execute arbitrary code or your website. Restricting policy and changing links to HTTPS can help prevent
Blocks loading of passive content over HTTP or FTP	✓	This site's Content Security Policy allows the loading passive content such as images or videos over insecu protocols such as HTTP or FTP. Consider changing th load them over HTTPS.
Clickjacking protection, using `frame-ancestors`	✓	The use of CSP's `frame-ancestors` directive offers fi grained control over who can frame your site.
Deny by default, using `default-src 'none'`	✓	Denying by default using `default-src 'none'` can ens your Content Security Policy doesn't allow the loading 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 loac 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 modify sensitive form data is submitted to or create additiona for data exfiltration.
Uses CSP3's `'strict-dynamic'` directive to allow dynamic script loading (optional)	-	`'strict-dynamic'` lets you use a JavaScript shim loa load all your site's JavaScript dynamically, without ha track `script-src` origins.

Cookies

✓ All cookies use the `Secure` flag, session cookies use the `HttpOnly` flag, and cross-origin restrictions are in place via the `SameSite` flag.

Name	Expires	Path	Secure	HttpOnly	SameSite
ASP.NET_SessionId	Session	/	✓	✓	Lax

Raw server headers

Header	Value
Date	Tue, 14 Apr 2026 17:21:52 GMT
Vary	Accept-Encoding
Server	
Alt-Svc	h3=":443"; ma=86400; persist=1
Connection	close
Set-Cookie	ASP.NET_SessionId=4q055opqypt1nk31u22e0exl; path=/; secure; HttpOnly; Same
Content-Type	text/html; charset=utf-8
Cache-Control	private
Content-Length	7078
Referrer-Policy	strict-origin-when-cross-origin
X-Aspnet-Version	4.0.30319
Permissions-Policy	geolocation=(), microphone=(), camera=(), payment=(), usb=()
Reporting-Endpoints	csp-endpoint="https://dev-sso.cfia.or.cr/csp-receiver/ReceiveCspReport.ashx"
Content-Security-Policy	default-src 'none'; script-src 'report-sample' https://api.smooch.io/ https://unpkg.c https://*.cfia.or.cr https://*.jquery.com https://*.alignetsac.com https://*.verifika.com https://cdn.datatables.net/ 'unsafe-eval' 'unsafe-inline' blob: https://www.google-analytics.com/analytics.js https://www.google.com/recaptcha/api.js https://www.gstatic.com/recaptcha/releases/ https://static.zdassets.com/web_widget/classic/latest/ https://www.googletagmanager.com/ https://static.zdassets.com/ https://analytics.google.com/ https://www.google-analytics.com/ https://*.cloudfro https://cdn.jsdelivr.net/ https://cdnjs.cloudflare.com/; media-src https://*.zdassets. blob:; object-src 'none'; img-src * data: blob:; style-src * 'unsafe-inline' 'report-sa manifest-src https://*.cfia.or.cr; font-src https: data:; connect-src https://*.cfia.or.cr https://cfia.aurainteractiva.com/ https://*.hacienda.go.cr https://analytics.google.co https://www.google-analytics.com/ https://*.googleapis.com https://*.google.com https://stats.g.doubleclick.net/ https://*.alignetsac.com https://*.verifika.com https: f.fontawesome.com/ wss://widget-mediator.zopim.com wss://localhost:31337 https://localhost:31337 wss://*.cfia.or.cr wss://api.smooch.io/ https://ekr.zdassets.c https://*.zendesk.com https://*.placetopay.com; frame-ancestors https://*.cfia.or.cr https://*.google.com https://*.alignetsac.com https://*.verifika.com; frame-src https://*.cfia.or.cr https://*.google.com https://*.alignetsac.com https://*.verifika.com uri 'self'; report-uri https://sso.cfia.or.cr/csp-receiver/ReceiveCspReport.ashx; repo csp-endpoint;

Header	Value
Strict-Transport-Security	max-age=31536000; includeSubDomains; preload

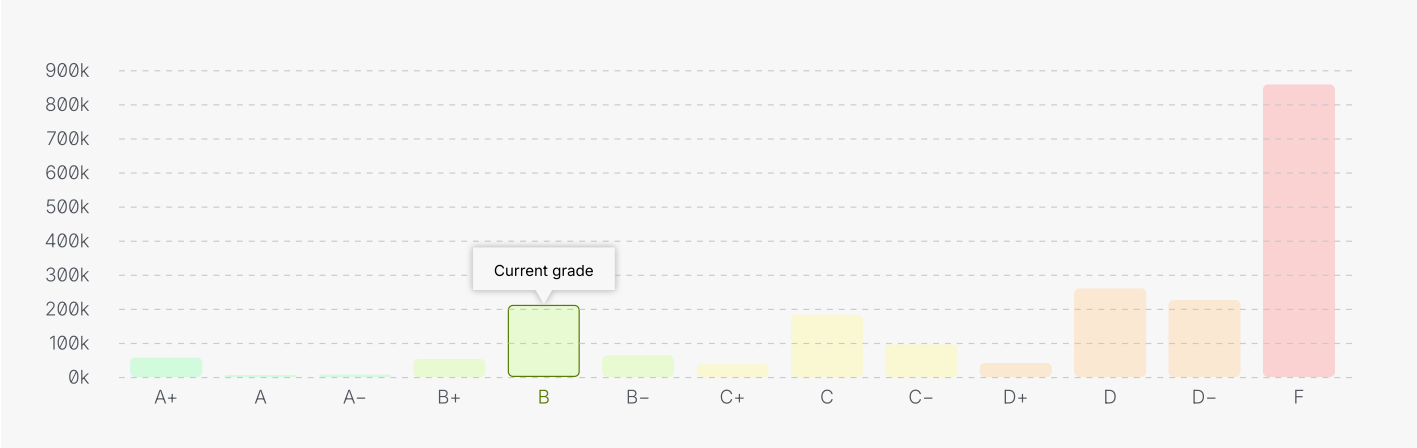
Scan history

Changes in score over time

Date	Score	Grade
Apr 14, 2026, 11:21:52 AM	70	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.