

Scan Summary

F

Host:

www.dat.com

Scan ID #:

43562803 (unlisted)

Start Time:

October 23, 2023 11:33 AM

Duration:

6 seconds

Score:

10/100

Tests Passed:

8/11

Recommendation

Initiate Rescan

What’s a good next step?

The use of the **X-Frame-Options** header and Content Security Policy’s **frame-ancestors** directive are a simple and easy way to protect your site against clickjacking attacks.

• [Mozilla Web Security Guidelines \(X-Frame-Options\)](#)

Once you've successfully completed your change, click Initiate Rescan for the next piece of advice.

Test Scores				
Test	Pass	Score	Reason	Info
<a href="#">Content Security Policy</a>	✗	-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.	ⓘ
<a href="#">Cookies</a>	—	0	No cookies detected	ⓘ
<a href="#">Cross-origin Resource Sharing</a>	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	ⓘ
<a href="#">HTTP Public Key Pinning</a>	—	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)	ⓘ
<a href="#">HTTP Strict Transport Security</a>	✓	0	HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000)	ⓘ
<a href="#">Redirection</a>	✓	0	Initial redirection is to HTTPS on same host, final destination is HTTPS	ⓘ
<a href="#">Referrer Policy</a>	—	0	Referrer-Policy header not implemented (optional)	ⓘ
<a href="#">Subresource Integrity</a>	✗	-50	Subresource Integrity (SRI) not implemented, and external scripts are loaded over HTTP or use protocol-relative URLs via src="//..."	ⓘ
<a href="#">X-Content-Type-Options</a>	✓	0	X-Content-Type-Options header set to "nosniff"	ⓘ
<a href="#">X-Frame-Options</a>	✗	-20	X-Frame-Options (XFO) header not implemented	ⓘ
<a href="#">X-XSS-Protection</a>	✓	0	X-XSS-Protection header set to "1; mode=block"	ⓘ

https://observatory.mozilla.org/analyze/www.dat.com

1/3

## Content Security Policy Analysis

Test	Pass	Info
Blocks execution of inline JavaScript by not allowing 'unsafe-inline' inside script-src	✗	ⓘ
Blocks execution of JavaScript's eval() function by not allowing 'unsafe-eval' inside script-src	✓	ⓘ
Blocks execution of plug-ins, using object-src restrictions	✗	ⓘ
Blocks inline styles by not allowing 'unsafe-inline' inside style-src	✗	ⓘ
Blocks loading of active content over HTTP or FTP	✓	ⓘ
Blocks loading of passive content over HTTP or FTP	✓	ⓘ
Clickjacking protection, using frame-ancestors	✗	ⓘ
Deny by default, using default-src 'none'	✗	ⓘ
Restricts use of the <base> tag by using base-uri 'none', base-uri 'self', or specific origins	✗	ⓘ
Restricts where <form> contents may be submitted by using form-action 'none', form-action 'self', or specific URIs	✗	ⓘ
Uses CSP3's 'strict-dynamic' directive to allow dynamic script loading (optional)	—	ⓘ

Looking for additional help? Check out Google's CSP Evaluator!

## Grade History

Date	Score	Grade
July 31, 2023 6:45 PM	10	F
January 15, 2022 6:06 PM	0	F
December 12, 2021 3:37 AM	45	C-
October 2, 2021 11:29 PM	0	F
January 6, 2021 9:02 PM	50	C
August 18, 2017 2:53 PM	0	F

## Raw Server Headers

Header	Value
CF-Cache-Status:	DYNAMIC
CF-RAY:	81ab09eacb6e16ao-SJC

Header	Value
Cache-Control:	max-age=15552000, must-revalidate
Connection:	keep-alive
Content-Encoding:	gzip
Content-Security-Policy:	upgrade-insecure-requests
Content-Type:	text/html; charset=UTF-8
Date:	Mon, 23 Oct 2023 15:33:29 GMT
Last-Modified:	Thu, 20 Jul 2023 05:50:03 GMT
Link:	<https://www.dat.com/>; rel=shortlink
Server:	cloudflare
Set-Cookie:	handl_landing_page=https%3A%2F%2Fwww.dat.com%2F; expires=Sun, 19-Nov-2023 18:48:14 GMT; Max-Age=2592000; path=/; domain=.domain.com; secure; SameSite=None, handl_ip=107.222.136.89; expires=Sun, 19-Nov-2023 18:48:14 GMT; Max-Age=2592000; path=/; domain=.domain.com; secure; SameSite=None, handl_url_base=https%3A%2F%2Fwww.dat.com%2F; expires=Sun, 19-Nov-2023 18:48:14 GMT; Max-Age=2592000; path=/; domain=.domain.com; secure; SameSite=None, handl_url=https%3A%2F%2Fwww.dat.com%2F; expires=Sun, 19-Nov-2023 18:48:14 GMT; Max-Age=2592000; path=/; domain=.domain.com; secure; SameSite=None, user_agent=Uptime-Kuma%2F1.23.3; expires=Sun, 19-Nov-2023 18:48:14 GMT; Max-Age=2592000; path=/; domain=.domain.com; secure; SameSite=None
Strict-Transport-Security:	max-age=31536000; includeSubDomains; preload
Transfer-Encoding:	chunked
Vary:	Accept-Encoding, Accept-Encoding, Accept-Encoding, Accept-Encoding, Cookie
X-Cache:	HIT: 33955
X-Cache-Group:	normal
X-Cacheable:	YES:15552000.000
X-Content-Type-Options:	nosniff
X-Powered-By:	WP Engine
X-XSS-Protection:	1; mode=block
alt-svc:	h3=":443"; ma=86400