📣 MDN HTTP Observatory is launched, and Mozilla Observatory is now deprecated. Learn more.

- HTTP Observatory
- TLS Observatory
- SSH Observatory
- Third-party Tests

Scan Summary

F

Host:	www.dyson.com.ua
Scan ID #:	55605742
Start Time:	September 13, 2024 10:00 PM
Duration:	3 seconds
Score:	20/100
Tests Passed:	7/10

Recommendation

You’re doing a wonderful job so far!

Did you know that a strong Content Security Policy (CSP) policy can help protect your website against malicious cross-site scripting attacks?

- Mozilla Web Security Guidelines (Content Security Policy)
- An Introduction to Content Security Policy
- Google CSP Evaluator
- Mozilla Laboratory CSP Generator

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

Test Scores

Test	Pass	Score	Reason
Content Security Policy	✗	-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`.
Cookies	✗	-10	Session cookie set without the `Secure` flag, but transmission over HTTP prevented by HSTS

Test	Pass	Score	Reason
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers
HTTP Strict Transport Security	✓	0	HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000)
Redirection	✓	0	Initial redirection is to HTTPS on same host, final destination is HTTPS
Referrer Policy	✓	+5	Referrer-Policy header set to `"no-referrer"`, `"same-origin"`, `"strict-origin"` or `"strict-origin-when-cross-origin"`
Subresource Integrity	✗	-50	Subresource Integrity (SRI) not implemented, and external scripts are loaded over HTTP or use protocol-relative URLs via `src="//..."`
X-Content-Type-Options	✓	0	X-Content-Type-Options header set to `"nosniff"`
X-Frame-Options	✓	0	X-Frame-Options (XFO) header set to `SAMEORIGIN` or `DENY`
X-XSS-Protection	✓	0	Deprecated X-XSS-Protection header set to `"1; mode=block"`

CSP Analysis

Test	Pass
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!

Cookies

Name	Expires	Path	Secure ()	HttpOnly ()	SameSite ()	Prefixed ()
ASP.NET_SessionId	Session	/	✗	✓	Lax	✗
__XSRFTOKEN	Session	/	✗	✓	✗	✗
shell#lang	Session	/	✗	✗	✗	✗

Grade History

Date	Score	Grade
September 13, 2024 10:00 PM	20	F

Raw Server Headers

Header	Value
Cache-Control:	no-cache, no-store,max-age=300
Connection:	keep-alive, Transfer-Encoding
Content-Encoding:	gzip
Content-Security-Policy:	upgrade-insecure-requests
Content-Type:	text/html; charset=utf-8
Date:	Fri, 13 Sep 2024 19:00:17 GMT
Dyson-Mobile:	False
Expires:	-1
Pragma:	no-cache
Referrer-Policy:	strict-origin-when-cross-origin
Server-Timing:	cdn-cache; desc=MISS, edge; dur=152, origin; dur=131, ak_p; desc="1726254017427_387976914_848748436_28282_8182_7_20_-";dur=1
Set-Cookie:	shell#lang=en; path=/, __XSRFTOKEN=3vy5aidMIqfhw/dQyqfGrIqZqNey+JnPfpUXLunzuxU=; path=/; HttpOnly
Strict-Transport-Security:	max-age=31536000; includeSubDomains
Transfer-Encoding:	chunked
Vary:	Accept-Encoding
X-Akamai-Transformed:	9l 165925 0 pmb=mRUM,2
X-Content-Type-Options:	nosniff

Header	Value
X-Correlation:	838165ef-fc92-48ef-8945-3ab02c98d8fc
X-FRAME-OPTIONS:	SAMEORIGIN
X-XSS-Protection:	1; mode=block