HTTP Observatory

TLS Observatory

SSH Observatory

Third-party Tests

Scan Summary

F

Host:	shop.spacex.com
Scan ID #:	53548283 (unlisted)
Start Time:	July 18, 2024 7:51 PM
Duration:	2 seconds
Score:	0/100
Tests Passed:	7/11

Recommendation

Fantastic work using HTTPS! Did you know that you can ensure users never visit your site over HTTP accidentally?

HTTP Strict Transport Security tells web browsers to only access your site over HTTPS in the future, even if the user attempts to visit over HTTP or clicks an `http://` link.

- Mozilla Web Security Guidelines (HSTS)
- MDN on HTTP Strict Transport Security

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	✗	-20	Cookies set without using the `Secure` flag or set over HTTP
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers

Test	Pass	Score	Reason
HTTP Strict Transport Security	✗	-10	HTTP Strict Transport Security (HSTS) header set to less than six months (15768000)
Redirection	✓	0	Initial redirection is to HTTPS on same host, final destination is HTTPS
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)
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	✓	+5	X-Frame-Options (XFO) implemented via the CSP `frame-ancestors` directive
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 ()
_cmp_a	July 31, 1724 8:00 AM	/	✗	✗	Lax	✗
_landing_page	September 1, 1726 7:00 AM	/	✗	✓	Lax	✗

Name	Expires	Path	Secure ()	HttpOnly ()	SameSite ()	Prefixed ()
_orig_referrer	September 1, 1726 7:00 AM	/	✗	✓	Lax	✗
_shopify_s	December 24, 1723 8:00 AM	/	✗	✗	Lax	✗
_shopify_y	April 27, 1759 8:00 AM	/	✗	✗	Lax	✗
_tracking_consent	April 27, 1759 7:00 AM	/	✗	✗	Lax	✗
cart_currency	September 1, 1726 8:00 AM	/	✗	✗	Lax	✗
localization	April 27, 1759 8:00 AM	/	✗	✗	Lax	✗
secure_customer_sig	April 27, 1759 8:00 AM	/	✓	✓	Lax	✗

Grade History

Date	Score	Grade
July 18, 2024 7:51 PM	0	F
July 25, 2019 7:29 PM	35	D
December 28, 2016 2:15 AM	15	F

Raw Server Headers

Header	Value
CF-Cache-Status:	DYNAMIC
CF-RAY:	8a5661bacb76c3d5-SEA
Connection:	keep-alive
Content-Encoding:	gzip
Content-Type:	text/html; charset=utf-8
Date:	Thu, 18 Jul 2024 23:51:47 GMT
NEL:	{"success_fraction":0.01,"report_to":"cf-nel","max_age":604800}
Report-To:	{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=vfcl7e%2BK7Bqp20hRrKU4zBzzU9BpNoMaN6XGOUI3lcuxsTcUFMMwJTue%2BqCcMkZvBc%2BEot%2FljJp8DfjYj80UVxY4VGk5IjGC4tzXvsLZKHRADcoi4dsEt1hlUbd%2FBPaMoA%3D%3D"}],"group":"cf-nel","max_age":604800}
Server:	cloudflare
Transfer-Encoding:	chunked
X-Content-Type-Options:	nosniff

Header	Value
X-Download-Options:	noopen
X-Permitted-Cross-Domain-Policies:	none
X-Sorting-Hat-PodId:	78
X-Sorting-Hat-ShopId:	26126155855
X-Storefront-Renderer-Rendered:	1
X-XSS-Protection:	1; mode=block
alt-svc:	h3=":443"; ma=86400
content-language:	en
content-security-policy:	block-all-mixed-content; frame-ancestors 'none'; upgrade-insecure-requests;
etag:	W/"cacheable:015206ce430cb931a7814a60f49db01f"
link:	<https://cdn.shopify.com>; rel="preconnect", <https://cdn.shopify.com>; rel="preconnect"; crossorigin
powered-by:	Shopify
server-timing:	processing;dur=16;desc="gc:1", db;dur=3, asn;desc="396982", edge;desc="SEA", country;desc="US", theme;desc="127641092175", pageType;desc="index", servedBy;desc="pcrz", requestID;desc="dafc9cf6-7528-4f9c-8a1a-2f02378cf169-1721346707", cfRequestDuration;dur=45.000076
set-cookie:	secure_customer_sig=; path=/; expires=Fri, 18 Jul 2025 23:51:47 GMT; secure; HttpOnly; SameSite=Lax, localization=US; path=/; expires=Fri, 18 Jul 2025 23:51:47 GMT, cart_currency=USD; path=/; expires=Thu, 01 Aug 2024 23:51:47 GMT, _tracking_consent=%7B%22con%22%3A%7B%22CMP%22%3A%7B%22a%22%3A%22%22%2C%22m%22%3A%22%22%2C%22p%22%3A%22%22%2C%22s%22%3A%22%22%7D%7D%2C%22v%22%3A%222.1%22%2C%22region%22%3A%22USOR%22%2C%22reg%22%3A%22%22%7D; domain=spacex.com; path=/; expires=Fri, 18 Jul 2025 23:51:47 GMT; SameSite=Lax, _cmp_a=%7B%22purposes%22%3A%7B%22a%22%3Atrue%2C%22p%22%3Atrue%2C%22m%22%3Atrue%2C%22t%22%3Atrue%7D%2C%22display_banner%22%3Afalse%2C%22sale_of_data_region%22%3Afalse%7D; domain=spacex.com; path=/; expires=Fri, 19 Jul 2024 23:51:47 GMT; SameSite=Lax, _shopify_y=f0650eec-a829-40a2-9834-511d8e6104a4; Expires=Fri, 18-Jul-25 23:51:47 GMT; Domain=spacex.com; Path=/; SameSite=Lax, _shopify_s=8b64c3ca-4ab2-4623-abf8-abb99a9c3ea8; Expires=Fri, 19-Jul-24 00:21:47 GMT; Domain=spacex.com; Path=/; SameSite=Lax, _orig_referrer=; Expires=Thu, 01-Aug-24 23:51:47 GMT; Domain=spacex.com; Path=/; HttpOnly; SameSite=Lax, _landing_page=%2F; Expires=Thu, 01-Aug-24 23:51:47 GMT; Domain=spacex.com; Path=/; HttpOnly; SameSite=Lax
strict-transport-security:	max-age=7889238
vary:	Accept
x-cache:	hit, server

Header	Value
x-dc:	gcp-us-west1,gcp-us-west1,gcp-us-west1
x-frame-options:	DENY
x-request-id:	dafc9cf6-7528-4f9c-8a1a-2f02378cf169-1721346707
x-shardid:	78
x-shopid:	26126155855
x-shopify-nginx-no-cookies:	0