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

Scan Summary

Host:	www.imoving.com
Scan ID #:	29017185
Start Time:	August 29, 2022 12:56 AM
Duration:	3 seconds
Score:	25/100
Tests Passed:	6/11

Recommendation

Initiate Rescan

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	Public content is visible via cross-origin resource sharing (CORS) `Access-Control-Allow-Origin` header
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)
HTTP Strict Transport Security	✗	-10	HTTP Strict Transport Security (HSTS) header set to less than six months (15768000)

Test	Pass	Score	Reason
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	✘	-5	Subresource Integrity (SRI) not implemented, but all external scripts are loaded over HTTPS
X-Content-Type-Options	✔	0	X-Content-Type-Options header set to `"nosniff"`
X-Frame-Options	✘	-20	X-Frame-Options (XFO) header cannot be recognized
X-XSS-Protection	✔	0	X-XSS-Protection header set to `"1; mode=block"`

Content Security Policy 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 ()
__RequestVerificationToken	Session	/	✘	✔	✘	✘

Name	Expires	Path	Secure ()	HttpOnly ()	SameSite ()	Prefixed ()
incap_ses_133_1175853	Session	/	✔	✘	None	✘
visid_incap_1175853	September 4, 1694 3:00 AM	/	✔	✔	None	✘

Grade History

Date	Score	Grade
August 29, 2022 12:56 AM	25	D-

Raw Server Headers

Header	Value
Access-Control-Allow-Headers:	Content-Type
Access-Control-Allow-Methods:	GET,PUT,POST,DELETE,OPTIONS
Access-Control-Allow-Origin:	*
Cache-Control:	private
Content-Encoding:	gzip
Content-Length:	31862

Header	Value
Content-Security-Policy:	default-src 'self' blob:; style-src 'self' https://fonts.googleapis.com https://cdnjs.cloudflare.com https://api.ucalc.pro 'unsafe-inline'; script-src 'self' http://maps.googleapis.com https://lagoonmedia.go2cloud.org https://www.google-analytics.com https://code.jquery.com https://cdnjs.cloudflare.com https://www.youtube.com https://js-agent.newrelic.com https://www.googletagmanager.com https://rec.smartlook.com https://code.upscope.io https://az416426.vo.msecnd.net https://apis.google.com https://www.google.com https://ucalc.pro https://bam.nr-data.net https://www.googleadservices.com https://connect.facebook.net https://js.hs-scripts.com https://cdn.mxpnl.com https://edge.fullstory.com https://js.upscope.io https://dc.services.visualstudio.com https://manager.eu.smartlook.cloud https://manager.us.smartlook.cloud https://googleads.g.doubleclick.net https://js.usemessages.com https://js.hs-analytics.net https://js.hscollectedforms.net https://js.hs-banner.com http://www.google-analytics.com https://www.imoving.com https://www.googletagmanager.com https://conoret.com https://www.gstatic.com 'unsafe-inline' 'unsafe-eval' blob:; connect-src 'self' http://maps.googleapis.com https://lagoonmedia.go2cloud.org https://www.google-analytics.com https://stats.g.doubleclick.net https://bam.nr-data.net https://dc.services.visualstudio.com https://manager.eu.smartlook.cloud https://manager.us.smartlook.cloud https://rs.fullstory.com https://api-js.mixpanel.com https://api.hubspot.com https://forms.hubspot.com https://events-writer.smartlook.com https://assets-proxy.smartlook.cloud https://web-writer.sg.smartlook.cloud https://www.facebook.com https://web-writer.us.smartlook.cloud https://web-writer.eu.smartlook.cloud wss:; img-src 'self' https://maps.gstatic.com https://www.google-analytics.com http://www.google-analytics.com https://maps.googleapis.com https://dashboard.umbraco.org https://www.google.com https://www.google.kg https://www.facebook.com https://forms.hsforms.com https://track.hubspot.com https://www.googletagmanager.com https://googleads.g.doubleclick.net data:; font-src 'self' https://fonts.gstatic.com https://www.imoving.com; frame-src 'self' https://www.facebook.com https://storage.upscope.io https://www.youtube.com https://api.ucalc.pro https://app.hubspot.com https://bid.g.doubleclick.net https://www.google.com
Content-Type:	text/html; charset=utf-8
Date:	Mon, 29 Aug 2022 04:56:16 GMT
Set-Cookie:	__RequestVerificationToken=ccjv6_KR-do3YzSAnbg82enhZLHV-2SIB8ubVC2cnjAW-3iPktQRMx-lT6Oy9bCZRir_N931SsGQXW6OvokY_U7LVCnJzJEyFHTNmsNZyTo1; path=/; HttpOnly, visid_incap_1175853=US3jd18iQ3mmU6ohsH6/Ce9GDGMAAAAAQUIPAAAAADpvaaZVdNn+dLU3J/gXsJr; expires=Mon, 28 Aug 2023 06:18:23 GMT; HttpOnly; path=/; Domain=.imoving.com; Secure; SameSite=None, incap_ses_133_1175853=ndPVItc4byHoSvcbJIPYAe9GDGMAAAAAL2UpLajOIfxKi3jJrYpPAA==; path=/; Domain=.imoving.com; Secure; SameSite=None
Strict-Transport-Security:	max-age=10886400
Vary:	Accept-Encoding
X-CDN:	Imperva
X-Content-Type-Options:	nosniff
X-Frame-Options:	SAMEORIGIN, SAMEORIGIN

Header	Value
X-Iinfo:	14-142586133-142586154 NNNN CT(32 131 0) RT(1661748975460 56) q(0 0 1 0) r(2 2) U5
X-XSS-Protection:	1; mode=block