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

Scan Summary

C

Host:	chat-app.eu-de.mybluemix.net
Scan ID #:	10750438 (unlisted)
Start Time:	May 7, 2019 1:50 PM
Duration:	2 seconds
Score:	55/100
Tests Passed:	8/11

Recommendation

Initiate Rescan

We noticed that your site is accessible over HTTPS, but still defaults to HTTP.

Automatically redirecting from HTTP to HTTPS helps ensure that your users get served a secure version of your site.

- Mozilla Web Security Guidelines (redirections)
- Mozilla TLS Configuration 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	–	0	No cookies detected
Cross-origin Resource Sharing	✓	0	Content is visible via cross-origin resource sharing (CORS) files or headers, but is restricted to specific domains
HTTP Public Key Pinning	✗	-5	HTTP Public Key Pinning (HPKP) header cannot be recognized
HTTP Strict Transport Security	✓	0	HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000)
Redirection	✗	-20	Does not redirect to an HTTPS site
Referrer Policy	–	0	Referrer-Policy header set to `"no-referrer-when-downgrade"`
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin
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	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!

Grade History

Date	Score	Grade
May 7, 2019 1:31 PM	55	C
May 7, 2019 11:05 AM	75	B
May 7, 2019 10:17 AM	0	F
May 2, 2019 6:51 PM	40	D+
May 2, 2019 6:47 PM	0	F
May 2, 2019 5:28 PM	40	D+
May 2, 2019 11:05 AM	0	F

Raw Server Headers

Header	Value
Access-Control-Allow-Origin:	https://chat-app-server.eu-de.mybluemix.net
Connection:	Keep-Alive
Content-Security-Policy:	default-src https://stackpath.bootstrapcdn.com https://maxcdn.bootstrapcdn.com https://use.fontawesome.com https://img.business.com https://unixtitan.net https://chat-app-server.eu-de.mybluemix.net wss://chat-app-server.eu-de.mybluemix.net frame-ancestors 'none' script-src 'self' 'unsafe-inline' style-src unsafe-inline'
Content-Type:	text/html; charset=utf-8
Date:	Tue, 07 May 2019 11:50:07 GMT
Etag:	"5cd16ff0-2e4"
Last-Modified:	Tue, 07 May 2019 11:45:52 GMT
Public-Key-Pins:	pin-sha256="base64+info1="; max-age=31536000
Referrer-Policy:	no-referrer-when-downgrade
Server:	nginx/1.15.12
Strict-Transport-Security:	max-age=31536000; includeSubdomains; preload
Transfer-Encoding:	chunked
X-Backside-Transport:	OK OK
X-Content-Type-Options:	nosniff
X-Frame-Options:	DENY
X-Global-Transaction-ID:	2732325999
X-Xss-Protection:	1; mode=block