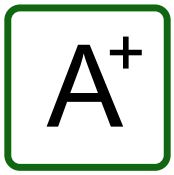
HTTP Observatory | TLS Observatory | SSH Observatory | Third-party Tests

Scan Summary



Host:	chat-app-server.eu-de.mybluemix.net
Scan ID #:	10754908 (unlisted)
Start Time:	May 7, 2019 9:28 PM
Duration:	1 seconds
Score:	110/100
Tests Passed:	11/11

Recommendation

Initiate Rescan

We don't have any!

Make sure to check back occasionally to ensure that your website is keeping up with the latest in web security standards.

In the meantime, thanks for everything you're doing to keep the internet a safe, secure, and private place!

Test Scores

Test	Pass	Score	Reason
Content Security Policy	✓	+10	Content Security Policy (CSP) implemented with `default-src 'none'` and no `'unsafe'`
Cookies	–	0	No cookies detected
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)
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	–	0	Referrer-Policy header set to `"no-referrer-when-downgrade"`
Subresource Integrity	–	0	Subresource Integrity (SRI) is only needed for html resources
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 9:28 PM	110	A+
May 7, 2019 9:15 PM	75	B
May 7, 2019 9:03 PM	55	C
May 7, 2019 6:58 PM	50	C
May 7, 2019 6:45 PM	40	D+
May 7, 2019 4:48 PM	0	F
May 7, 2019 1:46 PM	40	D+

Raw Server Headers

Header	Value
Connection:	Keep-Alive
Content-Security-Policy:	default-src 'none'
Date:	Tue, 07 May 2019 19:28:47 GMT
Referrer-Policy:	no-referrer-when-downgrade
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:	757647023
X-Xss-Protection:	1; mode=block