SSL/TLS Vulnerability Scan Report

Scan Initiated By:	**Maaz**
Timestamp:	2025-04-19 13:25:06
Target Host:	thinking-tester-contact-list.herokuapp.com

Version: 2.1.5

OpenSSL 3.4.0 22 Oct 2024

Connected to 3.229.186.102

Testing SSL server thinking-tester-contact-list.herokuapp.com on port 443 using SNI name thinking-tester-contact-list.herokuapp.com

SSL/TLS Protocols:

SSLv2 disabled

SSLv3 disabled

TLSv1.0 disabled

TLSv1.1 disabled

TLSv1.2 enabled

TLSv1.3 disabled

TLS Fallback SCSV:

Server supports TLS Fallback SCSV

TLS renegotiation:

Session renegotiation not supported

TLS Compression:

Compression disabled

Heartbleed:

TLSv1.2 not vulnerable to heartbleed

Supported Server Cipher(s):

Preferred TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve P-256 DHE 256

Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve P-256 DHE 256

Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256

Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-256 DHE 256

Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256

Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256

Accepted TLSv1.2 128 bits AES128-GCM-SHA256

Accepted TLSv1.2 128 bits AES128-SHA256

Accepted TLSv1.2 128 bits AES128-SHA

Accepted TLSv1.2 256 bits AES256-GCM-SHA384

Accepted TLSv1.2 256 bits AES256-SHA256

Accepted TLSv1.2 256 bits AES256-SHA

Server Key Exchange Group(s):

TLSv1.2 128 bits secp256r1 (NIST P-256)

TLSv1.2 192 bits secp384r1 (NIST P-384)

TLSv1.2 260 bits secp521r1 (NIST P-521)

SSL Certificate:

Signature Algorithm: sha256WithRSAEncryption

RSA Key Strength: 2048

Subject: *.herokuapp.com

Altnames: DNS:*.herokuapp.com

Issuer: Amazon RSA 2048 M02

Not valid before: Jan 30 00:00:00 2025 GMT

Not valid after: Feb 27 23:59:59 2026 GMT