SSL/TLS Vulnerability Scan Report

Scan Initiated By:	**Maaz**
Timestamp:	2025-04-19 13:09:37
Target Host:	hackthissite.org

Version: 2.1.5

OpenSSL 3.4.0 22 Oct 2024

Connected to 137.74.187.103

Testing SSL server hackthissite.org on port 443 using SNI name hackthissite.org

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

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

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

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

Accepted TLSv1.2 256 bits AES256-GCM-SHA384

Accepted TLSv1.2 128 bits AES128-GCM-SHA256

Accepted TLSv1.2 256 bits AES256-SHA256

Accepted TLSv1.2 128 bits AES128-SHA256

Server Key Exchange Group(s):

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

SSL Certificate:

Signature Algorithm: sha256WithRSAEncryption

RSA Key Strength: 4096

Subject: hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion

Altnames: DNS:hackthissite.org, DNS:www.hackthissite.org, DNS:hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion

Issuer: HARICA DV TLS RSA

Not valid before: Mar 25 04:43:22 2025 GMT

Not valid after: Mar 25 04:43:22 2026 GMT