SSL/TLS Vulnerability Scan Report

Scan Initiated By:	**Maaz**
Timestamp:	2025-04-19 13:10:11
Target Host:	saucedemo.com

Version: 2.1.5

OpenSSL 3.4.0 22 Oct 2024

Connected to 185.199.110.153

Testing SSL server saucedemo.com on port 443 using SNI name saucedemo.com

SSL/TLS Protocols:

SSLv2 disabled

SSLv3 disabled

TLSv1.0 disabled

TLSv1.1 disabled

TLSv1.2 enabled

TLSv1.3 enabled

TLS Fallback SCSV:

Server supports TLS Fallback SCSV

TLS renegotiation:

Session renegotiation not supported

TLS Compression:

Compression disabled

Heartbleed:

TLSv1.3 not vulnerable to heartbleed

TLSv1.2 not vulnerable to heartbleed

Supported Server Cipher(s):

Preferred TLSv1.3 128 bits TLS_AES_128_GCM_SHA256 Curve 25519 DHE 253

Accepted TLSv1.3 256 bits TLS_AES_256_GCM_SHA384 Curve 25519 DHE 253

Accepted TLSv1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253

Preferred TLSv1.2 256 bits ECDHE-RSA-CHACHA20-POLY1305 Curve 25519 DHE 253

Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253

Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve 25519 DHE 253

Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve 25519 DHE 253

Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve 25519 DHE 253

Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve 25519 DHE 253

Accepted TLSv1.2 128 bits AES128-GCM-SHA256

Accepted TLSv1.2 128 bits AES128-SHA

Accepted TLSv1.2 256 bits AES256-SHA

Server Key Exchange Group(s):

TLSv1.3 128 bits secp256r1 (NIST P-256)

TLSv1.3 192 bits secp384r1 (NIST P-384)

TLSv1.3 128 bits x25519

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

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

TLSv1.2 128 bits x25519

SSL Certificate:

Signature Algorithm: sha256WithRSAEncryption

RSA Key Strength: 2048

Subject: www.saucedemo.com

Altnames: DNS:saucedemo.com, DNS:www.saucedemo.com

Issuer: R10

Not valid before: Mar 6 06:21:16 2025 GMT

Not valid after: Jun 4 06:21:15 2025 GMT