Pentest Tools

SSL/TLS Vulnerability Scanner Report

✓ **dgtalbug.dev**

The Light SSL/TLS Scanner only checked for port 443. Upgrade to run Deep scansagainst multiple SSL-enabled ports.

Summary

Overall risk level:

Info

Risk ratings:

Critical:	0
High:	0
Medium:	0
Low:	0
Info:	5

Scan information:

Start time:	Nov 01, 2025 / 23:01:30 UTC+0530
Finish time:	Nov 01, 2025 / 23:03:27 UTC+0530
Scan duration:	1 min, 57 sec
Tests performed:	5/5
Scan status:	Finished

Findings

Open ports discovery

Port	State	Service	Server version	Uses SSL/TLS
443	open	https		Yes

SSL/TLS: Certificate is trusted

port 443/tcp

The domain has been found among Subject Alternate Names (SAN) or is the Common Name (CN) itself.
Therefore, it is considered protected by the certificate.

The Server Name Indication (SNI) has also been found. SNI is an extension to the TLS protocol that allows a client or browser to indicate which hostname it is trying to connect to at the start of the TLS handshake.
This allows the server to present multiple certificates on the same IP address and port number.

SSL/TLS: Certificate is Valid

port 443/tcp

The certificate will expire in 313 days.

SSL/TLS: CA Issuer is invalid or it cannot be identified

port 443/tcp

Sectigo public server authentication ca dv r36 (sectigo limited from gb)

Details

Risk description:
The certificate does not have a valid Certificate Authority Issuer, which are important for checking identity of the owner. Having this risk may result in the browsers not being able to validate the server's identity, compromising the communication between the server and users.

Recommendation:
We recommend you to configure a valid Certificate Authority Issuer for your servers's certificates.

Tested for certificate issues.

port 443/tcp

Certificate number: #1
Issuer: Sectigo Public Server Authentication CA DV R36 (Sectigo Limited from GB)
Signature: SHA256 with RSA
Serial number: 34649C3F7BD88CFF465FFB80B1B6A5DF

Scan coverage information

List of tests performed (5/5)

- ✓ Scanned for SSL/TLS services
- ✓ Tested the certificate is trusted
- ✓ Tested if the certificate is expired
- ✓ Tested for Certificate Authority Issuer
- ✓ Tested for certificate issues on port 443

Scan parameters

Target:	dgtalbug.dev
Preset:	Light
Scanning engines:	Certificate, Vulnerability
Ports to scan:	443