Hypertext Transfer Protocol Secure Testing Report

ISAN Security Gizmo Box

23 October 2023 06:45 AM

Scan Summary : it.msu.ac.th

23 October 2023 06:45 AM

testssl.sh is a free command line tool which checks a server's service on any port for the support of TLS/SSL ciphers, protocols as well as some cryptographic flaws.

Testing Summary

Domain name	*.msu.ac.th
Strict Transport Security	-
Certificate Expiration	122 >= 60 days
Certificate OCSP	intermediate certificate(s) is/are ok
Signature Algorithm	SHA256 with RSA
Certificate Transparency	yes (certificate extension)

Testing Protocols

SSV v2	No
SSV v3	No
TLS 1	Yes
TLS 1.1	Yes
TLS 1.2	Yes
TLS 1.3	Yes

Testing Vulnerabilities

POODLE (SSL v3)	No
DROWN	No
BEAST	Yes
Heartbleed	No
SWEET32	Yes
LUCKY13	Yes