Checkvanta

github.com

Security and configuration report

Generated on: 25/07/2026, 04:15:24 UTC

90
Overall score

Website configuration

Subscore **90**

TLS

90

- **HTTPS reachable** Required
  An HTTPS service is reachable and completed a TLS handshake.
- **TLS versions** Required
  Only modern TLS versions (1.2 and/or 1.3) are offered.
- **Cipher suite** Required
  The negotiated cipher suite (TLS_AES_128_GCM_SHA256) provides forward secrecy.
- **Certificate** Required
  The certificate is trusted and valid for this host.
- **Certificate key** Required
  The certificate uses a strong ECDSA key (256 bits).
- **Certificate signature** Required
  The certificate uses a secure signature algorithm (ECDSA-SHA256).
- **OCSP stapling** Recommended · Low
  The server does not staple an OCSP response.
  Recommendation: Enable OCSP stapling on the web server.
- **DANE (HTTPS)** Optional · Low
  No DANE (TLSA) records are published for HTTPS.
  Recommendation: With DNSSEC in place, publish TLSA records at `_443._tcp.<host>` that match your certificate, and rotate them together with the certificate.
- **Cipher order** Recommended
  With TLS 1.3 the server chooses from a small set of uniformly strong suites — ordering is not a concern.
- **Key exchange** Required
  The key exchange uses ECDHE with hash SHA256 — forward secrecy is provided.
- **TLS compression** Required
  TLS 1.3 has no record compression — the weakness does not apply.
- **Renegotiation** Required
  TLS 1.3 removed renegotiation entirely — no attack surface.
- **Extended Master Secret** Recommended
  TLS 1.3's key schedule supersedes Extended Master Secret — the weakness does not apply.
- **TLS 1.3 0-RTT (early data)** Optional
  The server does not accept 0-RTT — the safest default.