Checkvanta

tls-v1-2.badssl.com

Security and configuration report

Generated on: 25/07/2026, 04:10:35 UTC

60
Overall score

Website configuration

Subscore **60**

TLS

60

- **HTTPS reachable** Required
  An HTTPS service is reachable and completed a TLS handshake.
- **TLS versions** Required · High
  The server still offers an outdated TLS version (1.0 or 1.1).
  Recommendation: Disable TLS 1.0 and 1.1 in your web server or CDN configuration and offer only TLS 1.2 and 1.3.
- **Cipher suite** Required
  The negotiated cipher suite (TLS_ECDHE_RSA_WITH_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 RSA key (2048 bits).
- **Certificate signature** Required
  The certificate uses a secure signature algorithm (SHA256-RSA).
- **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
  The server enforces its own cipher-suite order.
- **Key exchange** Required
  The key exchange uses ECDHE with hash SHA256 — forward secrecy is provided.
- **TLS compression** Required
  TLS compression is disabled.
- **Renegotiation** Required
  The server supports secure renegotiation and rejects client-initiated renegotiation.
- **Extended Master Secret** Recommended · Low
  The server does not support Extended Master Secret.
  Recommendation: Enable Extended Master Secret in your TLS stack (on by default in current OpenSSL/server versions) or move to TLS 1.3.