Checkvanta

badssl.com

Security and configuration report

Generated on: 25/07/2026, 04:15:41 UTC

71

Overall score

Website configuration

Subscore 71

DNS

78

- Required
  4 name servers are configured, 4 of them reachable over IPv6.
- Required
  The domain resolves to 1 IPv4 address(es), e.g. 104.154.89.105.
- Recommended · Low
  The domain has no AAAA (IPv6) record.
  Recommendation: Add an AAAA record so IPv6-only clients can reach the site.
- Optional
  5 mail server(s) (MX) are configured for the domain.
- Recommended · Low
  No CAA record is configured.
  Recommendation: Add a CAA record listing your certificate authority.
- Recommended · Medium
  DNSSEC is not enabled for this domain.
  Recommendation: Enable DNSSEC at your DNS operator and publish the DS record at your registrar; fix any broken chain.

DNS servers

100

No findings.

HTTP / Security Headers

51

- Required
  The site is reachable over HTTPS.
- Recommended · Low
  The domain has no AAAA record, so the web server is not reachable over IPv6.
  Recommendation: Publish an AAAA record and make sure the web server accepts IPv6 connections on port 443.
- Recommended
  Plain HTTP is redirected to HTTPS.
- Recommended · Medium
  Your web server does not send an HSTS policy.
  Recommendation: HSTS requires that your site works fully over HTTPS, including a valid certificate from a publicly trusted authority. Proceed step by step:

  1. Make sure your site works fully over HTTPS now and permanently (e.g. with a reliable certificate-rollover process).
  2. Raise the HSTS lifetime gradually. After each step, check carefully for reachability problems and wait out the full `max-age` before moving to the next.
  3. Repeat steps 1–2 for every subdomain you want to protect. Only use `includeSubDomains` once you are sure that all (nested) subdomains support HTTPS reliably.
  4. Use `preload` only with great care — it is hard to undo and can break reachability of the whole domain and its subdomains.
- Recommended · Medium
  No Content-Security-Policy header is set.
  Recommendation: Define a Content-Security-Policy that only allows the sources your site actually needs.
- Recommended · Low
  No X-Frame-Options header is set.
  Recommendation: Send X-Frame-Options: DENY or SAMEORIGIN, or an equivalent frame-ancestors CSP directive.
- Recommended · Low
  The X-Content-Type-Options header is missing or not set to nosniff.
  Recommendation: Send X-Content-Type-Options: nosniff.

- Recommended · Low
  No Referrer-Policy header is set.
  Recommendation: Send a Referrer-Policy such as strict-origin-when-cross-origin or no-referrer.
- Optional · Low
  HTTP compression (gzip) is active — a performance plus.
  Recommendation: Enable HTTP compression (gzip or Brotli) for text responses to improve load time and bandwidth.

TLS 70

- Required
  An HTTPS service is reachable and completed a TLS handshake.
- 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.
- Required
  The negotiated cipher suite (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) provides forward secrecy.
- Required
  The certificate is trusted and valid for this host.
- Required
  The certificate uses a strong RSA key (2048 bits).
- Required
  The certificate uses a secure signature algorithm (SHA256-RSA).
- Recommended · Low
  The server does not staple an OCSP response.
  Recommendation: Enable OCSP stapling on the web server.