Checkvanta

example1.com

Security and configuration report

Generated on: 25/07/2026, 04:12:45 UTC

73
Overall score

Website configuration

Subscore 73

DNS

73

- **Name servers** Required · Low
  2 name servers are configured, but none is reachable over IPv6.
  Recommendation: Configure at least two name servers and make sure they are also reachable over IPv6.
- **IPv4 address** Required
  The domain resolves to 1 IPv4 address(es), e.g. 192.185.44.208.
- **IPv6 address** Recommended · Low
  The domain has no AAAA (IPv6) record.
  Recommendation: Add an AAAA record so IPv6-only clients can reach the site.
- **MX records** Optional
  1 mail server(s) (MX) are configured for the domain.
- **CAA record** Recommended · Low
  No CAA record is configured.
  Recommendation: Add a CAA record listing your certificate authority.
- **DNSSEC** 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

39

- **Reachability** Required
  The site is reachable over HTTPS.
- **IPv6 reachability** 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.
- **HTTPS redirect** Recommended · Medium
  Plain HTTP is not redirected to HTTPS.
  Recommendation: Configure a permanent redirect from http:// to https:// for the same host.
- **HSTS** 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.
- **Content-Security-Policy** Recommended · Medium
  No Content-Security-Policy header is set.
  Recommendation: Define a Content-Security-Policy that only allows the sources your site actually needs.

- **X-Frame-Options** Recommended · Low
  No X-Frame-Options header is set.
  Recommendation: Send X-Frame-Options: DENY or SAMEORIGIN, or an equivalent frame-ancestors CSP directive.
- **X-Content-Type-Options** Recommended · Low
  The X-Content-Type-Options header is missing or not set to nosniff.
  Recommendation: Send X-Content-Type-Options: nosniff.
- **Referrer-Policy** Recommended · Low
  No Referrer-Policy header is set.
  Recommendation: Send a Referrer-Policy such as strict-origin-when-cross-origin or no-referrer.
- **HTTP compression** 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 95

- **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_256_GCM_SHA384) 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.