Checkvanta

example2.com

Security and configuration report

Generated on: 25/07/2026, 04:15:40 UTC

78
Overall score

Website configuration

Subscore 78

DNS

83

- **Name servers** Required
  2 name servers are configured, 2 of them reachable over IPv6.
- **IPv4 address** Required
  The domain resolves to 2 IPv4 address(es), e.g. 188.114.96.12.
- **IPv6 address** Recommended
  The domain resolves to 2 IPv6 address(es), e.g. 2a06:98c1:3120::c.
- **MX records** Optional
  3 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

71

- **Reachability** Required
  The site is reachable over HTTPS.
- **IPv6 reachability** Recommended
  The web server is reachable over IPv6 (2a06:98c1:3121::c).
- **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
  A Content-Security-Policy header is set.
- **X-Frame-Options** Recommended
  An X-Frame-Options header is set.
- **X-Content-Type-Options** Recommended
  The X-Content-Type-Options header is set to nosniff.

- **Referrer-Policy** Recommended
  A Referrer-Policy header is set.
- **HTTP compression** Optional · Low
  HTTP compression (br) is active — a performance plus.
  Recommendation: Enable HTTP compression (gzip or Brotli) for text responses to improve load time and bandwidth.

TLS 70

- **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_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.