Checkvanta

example2.com

Sicherheits- und Konfigurationsbericht

Erstellt am: 25.7.2026, 04:14:24 UTC

78
Gesamtscore

Website-Konfiguration

Subscore **78**

DNS

83

- **Nameserver** Erforderlich
  2 Nameserver sind konfiguriert, 2 davon über IPv6 erreichbar.
- **IPv4-Adresse** Erforderlich
  Die Domain löst auf 2 IPv4-Adresse(n) auf, z. B. 188.114.96.12.
- **IPv6-Adresse** Empfohlen
  Die Domain löst auf 2 IPv6-Adresse(n) auf, z. B. 2a06:98c1:3120::c.
- **MX-Records** Optional
  Für die Domain sind 3 Mail Server (MX) konfiguriert.
- **CAA-Record** Empfohlen · Niedrig
  Es ist kein CAA-Record konfiguriert.
  Empfehlung: Ergänzen Sie einen CAA-Record mit Ihrer Zertifizierungsstelle.
- **DNSSEC** Empfohlen · Mittel
  DNSSEC ist für diese Domain nicht aktiviert.
  Empfehlung: Aktivieren Sie DNSSEC bei Ihrem DNS-Betreiber und veröffentlichen Sie den DS-Record beim Registrar; reparieren Sie eine gebrochene Kette.

DNS Server

100

Keine Befunde.

HTTP / Security-Header

71

- **Erreichbarkeit** Erforderlich
  Die Seite ist über HTTPS erreichbar.
- **IPv6-Erreichbarkeit** Empfohlen
  Der Webserver ist über IPv6 erreichbar (2a06:98c1:3121::c).
- **HTTPS-Redirect** Empfohlen · Mittel
  Einfaches HTTP wird nicht auf HTTPS umgeleitet.
  Empfehlung: Richten Sie eine dauerhafte Umleitung von http:// auf https:// für denselben Host ein.
- **HSTS** Empfohlen · Mittel
  Ihr Webserver sendet keine HSTS-Richtlinie.
  Empfehlung: HSTS setzt voraus, dass Ihre Website vollständig über HTTPS funktioniert – inklusive eines gültigen Zertifikats einer öffentlich vertrauenswürdigen Zertifizierungsstelle. Gehen Sie schrittweise vor:

  1. Stellen Sie sicher, dass Ihre Website jetzt und dauerhaft vollständig über HTTPS funktioniert (z. B. mit einem verlässlichen Zertifikats-Rollover-Prozess).
  2. Erhöhen Sie die HSTS-Gültigkeitsdauer stufenweise. Prüfen Sie nach jeder Stufe auf Erreichbarkeitsprobleme und warten Sie die volle `max-age`-Dauer ab, bevor Sie zur nächsten Stufe wechseln.
  3. Wiederholen Sie Schritt 1–2 für jede Subdomain, die Sie absichern möchten. Nutzen Sie `includeSubDomains` nur, wenn wirklich alle (verschachtelten) Subdomains HTTPS zuverlässig unterstützen.
  4. Nutzen Sie `preload` nur mit grosser Vorsicht — es ist schwer rückgängig zu machen und kann die Erreichbarkeit der gesamten Domain samt Subdomains beeinträchtigen.
- **Content-Security-Policy** Empfohlen
  Ein Content-Security-Policy-Header ist gesetzt.
- **X-Frame-Options** Empfohlen
  Ein X-Frame-Options-Header ist gesetzt.

- **X-Content-Type-Options** Empfohlen
  Der X-Content-Type-Options-Header ist auf nosniff gesetzt.
- **Referrer-Policy** Empfohlen
  Ein Referrer-Policy-Header ist gesetzt.
- **HTTP-Kompression** Optional · Niedrig
  HTTP-Kompression (br) ist aktiv – ein Performance-Pluspunkt.
  Empfehlung: Aktivieren Sie HTTP-Kompression (gzip oder Brotli) für Text-Antworten, um Ladezeiten und Bandbreite zu verbessern.

TLS 70

- **HTTPS erreichbar** Erforderlich
  Ein HTTPS-Dienst ist erreichbar und hat einen TLS-Handshake abgeschlossen.
- **TLS-Versionen** Erforderlich · Hoch
  Der Server bietet noch eine veraltete TLS-Version (1.0 oder 1.1) an.
  Empfehlung: Deaktivieren Sie TLS 1.0 und 1.1 in Ihrer Webserver- oder CDN-Konfiguration und bieten Sie nur TLS 1.2 und 1.3 an.
- **Cipher Suite** Erforderlich
  Die ausgehandelte Cipher Suite (TLS_AES_128_GCM_SHA256) bietet Forward Secrecy.
- **Zertifikat** Erforderlich
  Das Zertifikat ist vertrauenswürdig und für diesen Host gültig.
- **Zertifikatsschlüssel** Erforderlich
  Das Zertifikat verwendet einen starken ECDSA-Schlüssel (256 Bit).
- **Zertifikatssignatur** Erforderlich
  Das Zertifikat verwendet einen sicheren Signaturalgorithmus (ECDSA-SHA256).
- **OCSP-Stapling** Empfohlen · Niedrig
  Der Server liefert keine OCSP-Antwort per Stapling mit.
  Empfehlung: Aktivieren Sie OCSP-Stapling auf dem Webserver.