Checkvanta

badssl.com

Sicherheits- und Konfigurationsbericht

Erstellt am: 25.7.2026, 04:14:27 UTC

71

Gesamtscore

Website-Konfiguration

Subscore 71

DNS

78

- Erforderlich
  4 Nameserver sind konfiguriert, 4 davon über IPv6 erreichbar.
- Erforderlich
  Die Domain löst auf 1 IPv4-Adresse(n) auf, z. B. 104.154.89.105.
- Empfohlen · Niedrig
  Die Domain hat keinen AAAA-Record (IPv6).
  Empfehlung: Ergänzen Sie einen AAAA-Record, damit reine IPv6-Clients die Seite erreichen.
- Optional
  Für die Domain sind 5 Mail Server (MX) konfiguriert.
- Empfohlen · Niedrig
  Es ist kein CAA-Record konfiguriert.
  Empfehlung: Ergänzen Sie einen CAA-Record mit Ihrer Zertifizierungsstelle.
- 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

51

- Erforderlich
  Die Seite ist über HTTPS erreichbar.
- Empfohlen · Niedrig
  Die Domain hat keinen AAAA-Record, daher ist der Webserver über IPv6 nicht erreichbar.
  Empfehlung: Veröffentlichen Sie einen AAAA-Record und stellen Sie sicher, dass der Webserver IPv6-Verbindungen auf Port 443 annimmt.
- Empfohlen
  Einfaches HTTP wird auf HTTPS umgeleitet.
- 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.
- Empfohlen · Mittel
  Es ist kein Content-Security-Policy-Header gesetzt.
  Empfehlung: Definieren Sie eine Content-Security-Policy, die nur die tatsächlich benötigten Quellen erlaubt.
- Empfohlen · Niedrig
  Es ist kein X-Frame-Options-Header gesetzt.
  Empfehlung: Senden Sie X-Frame-Options: DENY oder SAMEORIGIN, oder eine gleichwertige frame-ancestors-CSP-Direktive.

- Empfohlen · Niedrig
  Der X-Content-Type-Options-Header fehlt oder ist nicht auf nosniff gesetzt.
  Empfehlung: Senden Sie X-Content-Type-Options: nosniff.
- Empfohlen · Niedrig
  Es ist kein Referrer-Policy-Header gesetzt.
  Empfehlung: Senden Sie eine Referrer-Policy wie strict-origin-when-cross-origin oder no-referrer.
- Optional · Niedrig
  HTTP-Kompression (gzip) ist aktiv – ein Performance-Pluspunkt.
  Empfehlung: Aktivieren Sie HTTP-Kompression (gzip oder Brotli) für Text-Antworten, um Ladezeiten und Bandbreite zu verbessern.

TLS 70

- Erforderlich
  Ein HTTPS-Dienst ist erreichbar und hat einen TLS-Handshake abgeschlossen.
- 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.
- Erforderlich
  Die ausgehandelte Cipher Suite (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) bietet Forward Secrecy.
- Erforderlich
  Das Zertifikat ist vertrauenswürdig und für diesen Host gültig.
- Erforderlich
  Das Zertifikat verwendet einen starken RSA-Schlüssel (2048 Bit).
- Erforderlich
  Das Zertifikat verwendet einen sicheren Signaturalgorithmus (SHA256-RSA).
- Empfohlen · Niedrig
  Der Server liefert keine OCSP-Antwort per Stapling mit.
  Empfehlung: Aktivieren Sie OCSP-Stapling auf dem Webserver.