Checkvanta

example.org

Sicherheits- und Konfigurationsbericht

Erstellt am: 25.7.2026, 04:15:38 UTC

39
Gesamtscore

Website-Konfiguration

Subscore **39**

HTTP / Security-Header

39

- **Erreichbarkeit** Erforderlich
  Die Seite ist über HTTPS erreichbar.
- **IPv6-Erreichbarkeit** Empfohlen
  Der Webserver ist über IPv6 erreichbar (2606:4700:10::ac42:9ded).
- **Gleiche Website über IPv6** Empfohlen
  IPv6 und IPv4 liefern dieselbe Website aus (Textähnlichkeit 100%).
- **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 · Mittel
  Es ist kein Content-Security-Policy-Header gesetzt.
  Empfehlung: Definieren Sie eine Content-Security-Policy, die nur die tatsächlich benötigten Quellen erlaubt.
- **X-Frame-Options** 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.
- **X-Content-Type-Options** Empfohlen · Niedrig
  Der X-Content-Type-Options-Header fehlt oder ist nicht auf nosniff gesetzt.
  Empfehlung: Senden Sie X-Content-Type-Options: nosniff.
- **Referrer-Policy** Empfohlen · Niedrig
  Es ist kein Referrer-Policy-Header gesetzt.
  Empfehlung: Senden Sie eine Referrer-Policy wie strict-origin-when-cross-origin oder no-referrer.
- **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.
- **security.txt** Empfohlen · Niedrig
  Es ist keine security.txt veröffentlicht.
  Empfehlung: Veröffentlichen Sie eine signierte `/.well-known/security.txt` mit mindestens einem `Contact:`- und einem `Expires:`-Feld.
- **HTTP/2** Empfohlen
  Der Webserver unterstützt HTTP/2.

- **HTTP/3** Optional · Info
  Der Webserver kündigt kein HTTP/3 (QUIC) an.
  Empfehlung: Optional: Aktivieren Sie HTTP/3 in Ihrem Webserver/Reverse Proxy und stellen Sie sicher, dass UDP-Port 443 in der Firewall geöffnet ist.
- **Cookie-Sicherheit** Empfohlen · Info
  Die Startseite setzt keine Cookies, die geprüft werden könnten.
- **Mixed Content** Erforderlich
  Die Seite bindet keine Ressourcen über unverschlüsseltes HTTP ein.
- **Subresource Integrity** Empfohlen · Info
  Die Seite bindet keine externen Skripte/Stylesheets ein, für die SRI sinnvoll wäre.