

Website-Konfiguration

Subscore 73

DNS

73

- **Nameserver** Erforderlich · Niedrig
2 Nameserver sind konfiguriert, aber keiner ist über IPv6 erreichbar.
Empfehlung: Konfigurieren Sie mindestens zwei Nameserver und stellen Sie sicher, dass diese auch über IPv6 erreichbar sind.
- **IPv4-Adresse** Erforderlich
Die Domain löst auf 1 IPv4-Adresse(n) auf, z. B. 192.185.44.208.
- **IPv6-Adresse** Empfohlen · Niedrig
Die Domain hat keinen AAAA-Record (IPv6).
Empfehlung: Ergänzen Sie einen AAAA-Record, damit reine IPv6-Clients die Seite erreichen.
- **MX-Records** Optional
Für die Domain sind 1 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

39

- **Erreichbarkeit** Erforderlich
Die Seite ist über HTTPS erreichbar.
- **IPv6-Erreichbarkeit** 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.
- **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 (gzip) ist aktiv – ein Performance-Pluspunkt.
[Empfehlung: Aktivieren Sie HTTP-Kompression \(gzip oder Brotli\) für Text-Antworten, um Ladezeiten und Bandbreite zu verbessern.](#)

TLS

95

- **HTTPS erreichbar** Erforderlich
Ein HTTPS-Dienst ist erreichbar und hat einen TLS-Handshake abgeschlossen.
- **TLS-Versionen** Erforderlich
Es werden nur moderne TLS-Versionen (1.2 und/oder 1.3) angeboten.
- **Cipher Suite** Erforderlich
Die ausgehandelte Cipher Suite (TLS_AES_256_GCM_SHA384) bietet Forward Secrecy.
- **Zertifikat** Erforderlich
Das Zertifikat ist vertrauenswürdig und für diesen Host gültig.
- **Zertifikatsschlüssel** Erforderlich
Das Zertifikat verwendet einen starken RSA-Schlüssel (2048 Bit).
- **Zertifikatssignatur** Erforderlich
Das Zertifikat verwendet einen sicheren Signaturalgorithmus (SHA256-RSA).
- **OCSP-Stapling** Empfohlen · Niedrig
Der Server liefert keine OCSP-Antwort per Stapling mit.
[Empfehlung: Aktivieren Sie OCSP-Stapling auf dem Webserver.](#)