

=====

DJSWISS Website Security Report

****Ziel:**** https://check.djswiss.ch/

****Domain:**** check.djswiss.ch

****Score:**** 55 / 100 • Note D

****Datum:**** 2026-06-24T16:40:12+00:00

Zusammenfassung

- Critical: 0

- High: 1

- Medium: 3

- Low: 2

- Info: 9

Technische Findings

[MEDIUM] HSTS fehlt

****Hinweis:**** Strict-Transport-Security Header nicht gefunden

****Fix:**** Header setzen: Strict-Transport-Security: max-age=31536000; includeSubDomains; preload nur nach Prüfung.

[MEDIUM] Content-Security-Policy fehlt

****Hinweis:**** CSP Header nicht gefunden

****Fix:**** CSP schrittweise einführen; zuerst Report-Only testen, danach strenger aktivieren.

[MEDIUM] Clickjacking-Schutz fehlt

****Hinweis:**** Kein X-Frame-Options und kein CSP frame-ancestors gefunden

****Fix:**** CSP frame-ancestors oder X-Frame-Options setzen.

[LOW] X-Content-Type-Options fehlt

****Hinweis:**** nosniff nicht gesetzt

****Fix:**** Header setzen: X-Content-Type-Options: nosniff

[LOW] Referrer-Policy fehlt

****Hinweis:**** Referrer-Policy Header nicht gefunden

****Fix:**** Header setzen, z.B. strict-origin-when-cross-origin oder no-referrer.

[INFO] Permissions-Policy fehlt

****Hinweis:**** Permissions-Policy Header nicht gefunden

****Fix:**** Nicht benötigte Browser-Features explizit deaktivieren.

[INFO] Cross-Origin-Opener-Policy fehlt

****Hinweis:**** COOP Header nicht gefunden

****Fix:**** Optional: Cross-Origin-Opener-Policy: same-origin für isolierte Browser-Kontexte prüfen.

[INFO] Technologie-Information sichtbar: server

****Hinweis:**** Apache

****Fix:**** Versionen und Framework-Banner soweit möglich ausblenden; wichtiger: Systeme aktuell halten.

[INFO] CSRF-Schutz nicht sichtbar nachweisbar

****Hinweis:**** POST-Formular gefunden, aber kein offensichtlicher CSRF-Token im HTML

****Fix:**** Serverseitig CSRF-Token verwenden; dieser Hinweis ist nur eine Sichtprüfung.

[INFO] Keine MX Records gefunden

****Hinweis:**** djswiss.ch

****Fix:**** Falls die Domain E-Mail empfängt, MX Records prüfen.

[INFO] CAA Record fehlt

****Hinweis:**** djswiss.ch

****Fix:**** Optional CAA setzen, um Zertifizierungsstellen einzuschränken.

[INFO] security.txt fehlt

****Hinweis:**** <https://check.djswiss.ch/.well-known/security.txt> nicht gefunden

****Fix:**** Optional security.txt veröffentlichen, damit Sicherheitsmeldungen korrekt ankommen.

[INFO] robots.txt fehlt

****Hinweis:**** <https://check.djswiss.ch/robots.txt> nicht gefunden

****Fix:**** Optional robots.txt veröffentlichen, besonders wenn SEO relevant ist.

[INFO] sitemap.xml fehlt

****Hinweis:**** <https://check.djswiss.ch/sitemap.xml> nicht gefunden

****Fix:**** Optional sitemap.xml veröffentlichen, wenn SEO relevant ist.

[HIGH] Apache server-status öffentlich erreichbar

****Hinweis:**** <https://check.djswiss.ch/server-status> liefert HTTP 200

****Fix:**** Datei sofort entfernen oder per Webserver blockieren; Secrets rotieren, falls Inhalte öffentlich waren.

Dieser Bericht ist ein defensiver, passiver Website-Check. Keine Exploit-/Einbruchanleitung.