

=====

DJSWISS Website Security Report

****Ziel:**** <https://share.djswiss.ch/login.php>

****Domain:**** share.djswiss.ch

****Score:**** 79 / 100 • Note B

****Datum:**** 2026-06-24T16:40:43+00:00

Zusammenfassung

- Critical: 0
- High: 1
- Medium: 0
- Low: 2
- Info: 7

Technische Findings

[LOW] CSP erlaubt unsafe-inline

****Hinweis:**** default-src 'self'; style-src 'self' 'unsafe-inline'; script-src 'self';
img-src 'self' data:; frame-ancestors 'none'; base-uri 'self'; form-action 'self'
****Fix:**** Inline-Skripte reduzieren; Nonce/Hash-Strategie verwenden.

[LOW] X-Content-Type-Options fehlt

****Hinweis:**** nosniff nicht gesetzt
****Fix:**** Header setzen: X-Content-Type-Options: nosniff

[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] 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://share.djswiss.ch/.well-known/security.txt> nicht gefunden
****Fix:**** Optional security.txt veröffentlichen, damit Sicherheitsmeldungen korrekt ankommen.

[INFO] robots.txt fehlt

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

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

[INFO] sitemap.xml fehlt

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

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

[HIGH] Apache server-status öffentlich erreichbar

****Hinweis:**** <https://share.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-/Einbruchsanleitung.