

=====

DJSWISS Website Security Report

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

****Domain:**** mail.djswiss.ch

****Score:**** 0 / 100 • Note E

****Datum:**** 2026-06-24T16:40:42+00:00

Zusammenfassung

- Critical: 1
- High: 4
- Medium: 1
- Low: 3
- Info: 6

Technische Findings

[MEDIUM] Content-Security-Policy fehlt

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

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

[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.

[LOW] Cookie ohne SameSite

****Hinweis:**** roundcube_sess

****Fix:**** SameSite=Lax oder Strict setzen; bei externen Login-Flows bewusst prüfen.

[HIGH] Fehlermeldungen im HTML sichtbar

****Hinweis:**** Debug-/PHP-/Stacktrace-Hinweise gefunden

****Fix:**** Debug-Ausgaben deaktivieren; Fehler serverseitig loggen, nicht öffentlich anzeigen.

[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 ohne Contact

Hinweis: <https://mail.djswiss.ch/.well-known/security.txt>

Fix: Contact-Zeile ergänzen, damit Meldungen ankommen.

[HIGH] SVN-Verzeichnis öffentlich erreichbar

Hinweis: <https://mail.djswiss.ch/.svn/entries> liefert HTTP 200

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

[HIGH] Backup-Datei möglicherweise öffentlich

Hinweis: <https://mail.djswiss.ch/backup.zip> liefert HTTP 200

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

[HIGH] Backup-Datei möglicherweise öffentlich

Hinweis: <https://mail.djswiss.ch/backup.tar.gz> liefert HTTP 200

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

[LOW] composer.lock öffentlich sichtbar

Hinweis: <https://mail.djswiss.ch/composer.lock> liefert HTTP 200

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

[LOW] composer.json öffentlich sichtbar

Hinweis: <https://mail.djswiss.ch/composer.json> liefert HTTP 200

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

[CRITICAL] Config-Backup öffentlich

Hinweis: <https://mail.djswiss.ch/config.php~> 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.