# JTL-Shop: falk_plus ALTCHA Spam- und Botschutz

Selbst gehostetes, quelloffenes Spam- und Botschutz-Plugin für JTL-Shop 5 auf Basis von ALTCHA, einem quelloffenen Proof-of-Work-Verfahren (MIT-Lizenz). Schützt Registrierung, Newsletter-Anmeldung und Kontaktformular vor Spam-Bots und automatisierten Fake-Anmeldungen – ohne Daten an Dritte weiterzugeben. Bewusst ohne Google reCAPTCHA und ohne Umleitung über Cloudflare oder ähnliche Dienste.

## 1. Was macht das Plugin

Das Plugin blendet in den drei genannten Formularen unauffällig eine kleine Sicherheitsprüfung ein. Der Browser des Besuchers löst dabei im Hintergrund eine kurze Rechenaufgabe (Proof-of-Work), bevor das Formular abgeschickt werden kann. Für Menschen ist das kaum spürbar (in der Regel deutlich unter einer Sekunde), für automatisierte Bot-Skripte, die kein JavaScript ausführen oder einfach nur Formularfelder befüllen, stellt es dagegen eine wirksame Hürde dar.

Da die gesamte Prüfung selbst gehostet läuft, verlassen keine Besucherdaten den eigenen Server, es gibt keine Weiterleitung an Google oder Cloudflare und keine Cookie- oder Datenschutz-Implikationen durch Drittanbieter-Dienste.

## 2. Hintergrund

Anlass war ein Bot-Problem: über einen längeren Zeitraum liefen massenhaft Fake-Registrierungen und Newsletter-Anmeldungen mit immer demselben Muster auf („Test“/„Test User“ in Vorname/Nachname/Ort/Straße, aber echte, unterschiedliche Fremd-E-Mail-Adressen). Andere getestete Maßnahmen wie Rate-Limiting konnten das Problem nicht zuverlässig lösen, da deren Prüfungen an anderer Stelle ansetzen (z. B. an Kommentar- oder Nachrichtenfeldern, die weder das Registrierungs- noch das Newsletter-Formular besitzen).

Dieses Plugin prüft stattdessen direkt beim Absenden von Registrierung, Newsletter-Anmeldung und Kontaktformular selbst – unabhängig davon, welche Felder das jeweilige Formular sonst enthält. Mittlerweile schützt es alle drei Formulare nach demselben Prinzip.

## 3. Funktionsweise (ALTCHA)

ALTCHA ist ein quelloffenes, selbst hostbares Proof-of-Work-Verfahren als datenschutzfreundliche Alternative zu klassischen Captchas. Der Ablauf:

1. Der Server erzeugt beim Laden der Seite eine zufällige Rechenaufgabe (Challenge) und signiert sie.
2. Der Browser des Besuchers löst diese Aufgabe im Hintergrund per JavaScript, bevor das

Formular abgeschickt werden kann.
3. Beim Absenden prüft der Server die eingereichte Lösung anhand der Signatur. Passt sie nicht oder fehlt sie, wird die Anfrage abgelehnt.

Die Bibliothek und das Verfahren stehen unter der MIT-Lizenz und werden unverändert vom offiziellen Projekt übernommen (siehe altcha-org/altcha-lib-php auf GitHub). Es findet keine Kommunikation mit externen Diensten statt, die gesamte Prüfung läuft auf dem eigenen Server.

# 4. Geschützte Formulare

- Kundenregistrierung (`/Registrieren`)
- Newsletter-Anmeldung (`/Newsletter`)
- Kontaktformular (`/Kontakt`)

Jedes der drei Formulare lässt sich in den Plugin-Einstellungen einzeln aktivieren oder deaktivieren.

# 5. Installation / Download

Das Plugin wird als ZIP-Datei über das JTL-Shop-Backend installiert (*Plugins → Plugin hochladen*). Diese installierbare ZIP gibt es auf zwei Wegen:

1. **Fertige ZIP unter Releases:** im Gitea-Repository gibt es zu jeder Version einen Eintrag unter Releases; sobald dort eine ZIP-Datei als Anhang vorliegt, lässt sie sich ohne weitere Anpassung direkt hochladen und installieren. Ein Commit oder Push allein erzeugt in Gitea noch keine solche ZIP – die Datei muss einmalig manuell als Release-Anhang bereitgestellt werden.
2. **Quellcode-Download über „Code → Download ZIP“:** dieser Weg liefert den reinen Quellcode des Repos und packt ihn zusätzlich in einen Ordner mit Repo- und Branch-Namen. Für die Installation muss danach der enthaltene Unterordner `fp_altcha_spamschutz` neu, direkt als Wurzelverzeichnis der ZIP, gepackt werden.

Nach dem Hochladen wird das Plugin wie gewohnt im JTL-Shop-Backend aktiviert. Ein HMAC-Geheimschlüssel muss nicht manuell hinterlegt werden – das Plugin erzeugt beim ersten Aufruf automatisch einen zufälligen Schlüssel und speichert ihn im Plugin-Verzeichnis.

Repository: vw.falk.plus/JensFalk/JTL-Shop-ALTCHA-Spamschutz

# 6. Einstellungen

In den Plugin-Einstellungen im JTL-Shop-Backend lassen sich konfigurieren:

- **HMAC-Geheimschlüssel** – optional, wird sonst automatisch erzeugt.
- **Sicherheitsstufe (Rechenaufwand)** – wie viel Rechenarbeit der Browser vor dem Absenden leisten muss (niedrig/mittel/hoch).
- **Gültigkeit der Prüfung** – wie lange eine erzeugte Prüfung gültig bleibt, bevor sie abläuft.
- **Formulare** – Registrierung, Newsletter-Anmeldung und Kontaktformular einzeln aktivierbar.
- **Debug-Logging** – schreibt zusätzliche Diagnoseinformationen ins Error-Log, nur zum Testen

gedacht.

## 7. Test nach der Installation

Nach der Installation sollte einmal geprüft werden, dass:

- in Registrierung, Newsletter-Anmeldung und Kontaktformular die Sicherheitsprüfung sichtbar erscheint und nach kurzer Zeit zweizeilig „Sicherheitsprüfung bestanden“ anzeigt,
- eine normale, korrekt ausgefüllte Anfrage in allen drei Formularen anstandslos durchgeht,
- ein Absenden ohne JavaScript bzw. ohne gelöste Prüfung zuverlässig abgelehnt wird.

## 8. Bekannte Einschränkungen

Das Widget wird über das umgebende Formular-Element eingebunden. Bei stark individualisierten Theme-Anpassungen, die die Formularstruktur wesentlich verändern, kann es in seltenen Fällen nötig sein, die verwendeten CSS-Selektoren im Plugin anzupassen.

## 9. Weiterführende Links

- Gitea-Repository (Quellcode, Releases, Issues): https://vw.falk.plus/JensFalk/JTL-Shop-ALTCHA-Spamschutz
- ALTCHA-Projekt: https://altcha.org
- ALTCHA PHP-Bibliothek (MIT-Lizenz): https://github.com/altcha-org/altcha-lib-php