LoginShield

Passwortschutz für Inhaltsbereiche in moziloCMS

Version 1.2.5 | 20. 10. 2026

Ursprüngliche Plugin-Idee: hausl78

Weiterentwicklung: Gerd Fischer

1. Kurzbeschreibung

LoginShield schützt beliebige Inhaltsbereiche einer moziloCMS-Seite mit einem Passwort. Das Plugin begrenzt fehlgeschlagene Login-Versuche, protokolliert temporäre Sperren, meldet Benutzer beim Verlassen der Seite automatisch ab und enthält im Adminbereich einen Passwort-Hash-Generator.

LoginShield basiert auf der ursprünglichen Idee des Plugins LoginContainer, wurde jedoch unter eigenem Namen, eigener PHP-Klasse und eigenem internen Namensraum weiterentwickelt.

2. Funktionen

- Passwortgeschützte Inhaltsbereiche mit beliebigem moziloCMS-Inhalt
- Konfigurierbare maximale Anzahl fehlgeschlagener Login-Versuche
- Konfigurierbares Zeitfenster für die temporäre Sperre
- Protokollierung von Lockouts in logs/lockouts.log
- CSRF-Schutz für Login, Logout und Hash-Generator
- HTTPS-Pflicht auf Produktivsystemen; lokales HTTP für XAMPP kann zugelassen werden
- Automatischer Logout beim Verlassen oder Schließen der Seite
- Rücksprung zum LoginShield-Bereich nach Login oder Logout
- Beschriftete Formularfelder und Fehlermeldungen mit role="alert"
- Eigenständige, responsive LoginShield-Oberfläche mit layoutneutralen CSS-Klassen
- Passwort kann auf Wunsch angezeigt und wieder verborgen werden
- Verständliche Fehler- und Sperrmeldungen mit verbleibenden Loginversuchen
- Passwortfeld wird nach einer Fehleingabe geleert und gezielt fokussiert
- Kompakter Statusbereich mit deutlich erkennbarem Abmeldebutton
- Pro Seite ein Login-Container

3. Voraussetzungen

- moziloCMS 2.x oder 3.x
- PHP 7.4 oder neuer; empfohlen wird PHP 8.1 oder neuer
- Schreibrecht für plugins/LoginShield/logs/
- HTTPS auf dem Webspace

4. Installation

Die ZIP-Datei über die Pluginverwaltung von moziloCMS installieren und LoginShield anschließend im Adminbereich Aktivierung kontrollieren.

LoginContainer und LoginShield dürfen als getrennte Pluginordner parallel installiert sein. Vorgesehen ist jedoch, nur das tatsächlich verwendete Plugin zu aktivieren. Ein gleichzeitiger Betrieb beider Plugins auf derselben Website wird nicht empfohlen.

Die Einstellungen und Daten von LoginContainer werden nicht automatisch übernommen. LoginShield verwaltet seine Konfiguration und seine Log-Datei ausschließlich im eigenen Pluginordner.

5. Konfiguration

- Max. Loginversuche: Standardwert 5
- Sperrfrist in Sekunden: Standardwert 300
- Passwort-Hash erzeugen: Passwort eingeben, Hash erzeugen und vollständig kopieren

Die Schalter für lokales HTTP, zusätzliche Entwicklungs-Hosts und Debug-Ausgaben befinden sich am Anfang der index.php und verwenden ausschließlich das Präfix LOGINSHIELD_.

6. Einbau und Syntax

6.1 Grundsyntax

```
{LoginShield|Ausgeblendeter Inhalt,PASSWORT-HASH}
```

6.2 Beispiel

```
{LoginShield|
Dieser Text ist geschützt.
Hier kann beliebiger Inhalt stehen.
,$2y$10$XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX}
```

Das letzte Komma im Pluginaufruf trennt den geschützten Inhalt vom Passwort-Hash. Im Inhalt selbst dürfen deshalb weitere Kommata vorkommen.

7. Umstieg von LoginContainer-2

Für Inhaltsseiten muss grundsätzlich nur der Pluginname im Aufruf geändert werden:

```
bisher: {LoginContainer|Inhalt,PASSWORT-HASH}
neu:    {LoginShield|Inhalt,PASSWORT-HASH}
```

Vorhandene Passwort-Hashes können unverändert weiterverwendet werden. Die Konfigurationswerte für Loginversuche und Sperrfrist müssen im Adminbereich von LoginShield neu gesetzt werden.

Eine vorhandene lockouts.log wird nicht automatisch übernommen. Falls alte Protokolle erhalten bleiben sollen, kann die Datei manuell nach plugins/LoginShield/logs/ kopiert werden. Das Datenformat und die relative Ablagestelle bleiben gleich.

8. Log-Datei

LoginShield schreibt Sperren nach plugins/LoginShield/logs/lockouts.log. Die Datei wird bei Bedarf automatisch angelegt, sofern das Verzeichnis beschreibbar ist.

Enthalten sind Zeitstempel, IP-Adresse, Zielseite und User-Agent. Da diese Angaben personenbezogen sein können, sollte die Datei vor unbefugtem Zugriff geschützt, regelmäßig geprüft und entsprechend der eigenen Datenschutzvorgaben gelöscht werden.

9. Hinweise zur Sicherheit

- Nur von password_hash() erzeugte Hashes verwenden; niemals Klartext-Passwörter in den Pluginaufruf schreiben.
- LOGINSHIELD_DEBUG auf Produktivsystemen deaktiviert lassen.
- Lokales HTTP nur für eindeutig lokale Entwicklungsumgebungen freigeben.
- Den direkten Browserzugriff auf logs/ serverseitig sperren, wenn die Protokolldatei nicht bewusst abrufbar sein soll.

10. Autor, Herkunft und Lizenz

Ursprüngliche Plugin-Idee: hausl78 (https://www.mozilo.de/)

Weiterentwicklung als LoginShield: G. Fischer

Lizenz: GPL v2

11. Versionsstand

Version 1.2.5 - 20. 10. 2026

- Deutsche und englische Sprachdateien für Frontend und Adminbereich
- Automatische Auswahl anhand der in moziloCMS eingestellten CMS- beziehungsweise Adminsprache
- Verbesserte Layoutverträglichkeit durch Vermeidung einer globalen header-Kollision; Pluginaufruf und Konfiguration bleiben kompatibel