

Sicherheits-Dokumentation – WordPress Plugin

Gültig für alle von Fabian Pursche / online-effect.de entwickelten Plugins

Version: 1.0

Stand: 29.07.2025

Entwickler: Fabian Pursche

Website: <https://online-effect.de>

Sicherheitsprinzipien

Dieses Plugin wurde unter Berücksichtigung der offiziellen WordPress Coding Standards entwickelt. Ziel ist es, eine sichere, datensparsame und stabile Integration in bestehende WordPress-Installationen zu gewährleisten.

Wichtige Maßnahmen im Code

Maßnahme	Status
Verwendung von Nonces (CSRF-Schutz)	✓
Sanitize/Validate von Benutzereingaben	✓
Escape von Ausgaben (z. B. in HTML)	✓
Einsatz von <code>current_user_can()</code> -Prüfungen	✓
Kein Einsatz externer Tracking-Tools	✓
Keine sensiblen Daten gespeichert	✓
Keine AJAX-Endpunkte ohne Berechtigungsprüfung	✓
DSGVO-konforme Programmierung	✓

Technische Hinweise

- **Kompatibilität:** WordPress \geq 5.8, PHP \geq 7.4
 - **Speichertypen:** Wenn überhaupt, nur Einstellungen in wp_options (per register_setting)
 - **Verarbeitung personenbezogener Daten:** *Nicht vorgesehen* (außer bei Plugins mit Kontakt- oder DSGVO-Funktion – dann entsprechend dokumentiert)
-

Empfehlungen für Anwender

- Halten Sie WordPress, Plugins und PHP-Version aktuell.
 - Nutzen Sie sichere Administrator-Passwörter.
 - Prüfen Sie die Datenschutzerklärung Ihrer Website auf Ergänzungsbedarf bei Plugin-Einsatz.
 - Führen Sie regelmäßig Backups durch – vor und nach Plugin-Aktivierung.
-

Qualitätssicherung

- Alle Plugins werden in einer lokalen Staging-Umgebung mit aktuellen WP-Versionen getestet.
- Es erfolgt ein manueller Check auf:
 - Dateizugriffsrechte
 - Output-Escaping
 - Berechtigungsprüfungen
- Optionaler Einsatz von Tools wie:
PHP_CodeSniffer, Query Monitor, WP_DEBUG, Log Viewer.



Kontakt bei Sicherheitsbedenken

Wenn Sie eine potenzielle Schwachstelle feststellen, kontaktieren Sie bitte direkt:

Fabian Pursche

E-Mail: info@online-effect.de

Website: <https://online-effect.de>

Lizenz: GPLv2 oder höher

Transparenz: Quellcode offen einsehbar – keine versteckten Funktionen