

# DRUPAL CHECKLISTE

---

- Default Credentials ändern**
- File Zugriff einschränken**
- Datenbank absichern**
- Fehlermeldungen deaktivieren**
- Security Module nutzen**
- Nicht genutzte Module deaktivieren**
- Seite regelmäßig prüfen**
- Informiert bleiben**

# DRUPAL CHECKLISTE

## **Default Credentials ändern**

Nach der Installation sind die Default Credentials admin/amdin@123 und sollten sofort geändert werden.

## **File Zugriff einschränken**

Im .htaccess file können Zugriffsberechtigungen für sensible Files (upgrade.php, authorize.php, cron.php etc.) vergeben werden.

## **Datenbank absichern**

In settings.php sollte ein selbstgewähltes Prefix für Tabellen der Datenbank angegeben werden (erschwert SQL Injections).

## **Fehlermeldungen deaktivieren**

Unter Configuration/ Development/ Logging and Errors, sollten Error Reports auf „None“ gesetzt werden.

## **Security Module nutzen**

Security Module können die Sicherheit einer Drupal Anwendung weiter erhöhen.

## **Nicht genutzte Module deaktivieren**

Module die nicht mehr genutzt werden sollten deaktiviert werden um die Angriffsfläche der Seite zu minimieren.

## **Seite regelmäßig prüfen**

Mit dem Security Reviews Modul sollte die Seite in regelmäßigen Abständen auf ihre Sicherheit überprüft werden.

## **Informiert bleiben**

Unter [drupal.org/security](http://drupal.org/security) veröffentlicht das Entwicklerteam Meldungen zu Sicherheitslücken und Schwachstellen.