

# WEBSEITEN CHECKLISTE

---

- User Input überprüfen**
- File Uploads überprüfen**
- Logins begrenzen**
- https verwenden**
- Passwörter sicher speichern**
- Backups anlegen**
- Speichern auf Server Seite**
- Restriktive Berechtigungen**

# WEBSITEN CHECKLISTE

## **User Input überprüfen**

Ob XSS oder SQL Injection die größte Gefahr geht von User Input aus. Dieser sollte deshalb bestmöglich gefiltert bzw. beschränkt werden.

## **File Uploads überprüfen**

Falls User Dateien hochladen können, prüfen Sie, ob wirklich nur genau die akzeptierten Dateitypen hochgeladen werden können.

## **Logins begrenzen**

Nach mehreren fehlerhaften Login Versuchen, sollte die Anzahl begrenzt werden. Etwa durch Captchas oder kurze Pausen.

## **https verwenden**

Verwenden Sie https um die Daten die User auf Ihrer Seite eingeben zu sichern.

## **Passwörter sicher speichern**

Passwörter sollten mit einem sicheren Algorithmus (NICHT MD5) gehashed werden.

## **Backups anlegen**

100%ige Sicherheit gibt es nicht. Für den Fall der Fälle sollten regelmäßig Backups aller wichtigen Daten angelegt werden.

## **Speichern auf Server Seite**

Relevante Daten (Preise o.ä.) sollten immer auf der Server Seite gespeichert werden, nie beim Client (etwa in einem Cookie).

## **Restriktive Berechtigungen**

Ob Mitarbeiter oder User, jeder sollte nur genau die Berechtigungen haben, die unbedingt nötig sind.