SQL Injection Checkliste

Maßnahme	Erläuterung
1. Prepared Statements / Parameter	Trenne SQL-Code und Nutzereingaben, um Injection zu verhindern.
2. Input Validation / Whitelisting	Erlaube nur erwartete Eingaben (z. B. E-Mail, Zahl, Liste) und blockiere alles andere.
3. Minimale Rechte für Datenbank-User	Jeder Datenbank-Account sollte nur die nötigsten Berechtigungen haben.
4. Keine Admin-Accounts für Webanwendung	Root oder sa für Webanwendungen vermeiden – reduziert Schadenspotenzial.
5. ORM korrekt nutzen	Nur sichere ORM-Funktionen verwenden, keine direkte String-Konkatenation.
6. WAF / Firewall einsetzen	Web Application Firewalls erkennen und blockieren Angriffe automatisch.
7. SQL-Fehler protokollieren	Fehler speichern, aber nicht an Nutzer ausgeben – sonst können Angreifer Details sehen.
8. Verdächtige Requests überwachen	Angriffe wie UNION SELECT, ' OR 1=1-- etc. erkennen und blockieren.
9. Tests in Testumgebung durchführen	SQLi-Tests nur in sicheren Testumgebungen durchführen, nicht auf Live-Systemen.
10. Sicherheitsscanner nutzen	Tools wie OWASP ZAP oder Burp Suite helfen, Schwachstellen systematisch aufzudecken.