SQL Injection

Inhaltsverzeichnis

SQL Injection manipuliert Datenbankabfragen über unsicher zusammengesetzte Eingaben. Angreifer können Daten lesen, ändern oder in schweren Fällen sogar Systemkommandos auf dem Datenbankhost auslösen.

1 Funktionsweise

Wenn Benutzereingaben direkt in SQL-Strings gelangen, kann die Abfragelogik umgebogen werden. Prepared Statements und ORM-Parameterbindung trennen Code und Daten.

- **In-Band:** Ergebnis direkt in der Antwort
- **Blind:** Ableitung über Verhalten/Zeit
- **Second Order:** später ausgeführte gespeicherte Payloads

2 Typische Einsatzbereiche

- Webfrontends mit Datenbankanbindung
- Legacy-Apps mit String-Konkatenation
- API-Endpunkte mit Filter-/Suchparametern

3 Wichtige Hinweise

- Prepared Statements sind Standardschutz.
- Least Privilege auf DB-Accounts begrenzt Schaden.
- WAF hilft ergänzend, ersetzt sicheren Code nicht.

4 Fazit

SQL Injection ist vermeidbar und dennoch häufig – parametrisierte Queries und enge DB-Rechte sind die Basisabwehr.