

# LU03c - Angriffsvektoren

## □ Angriffsvektoren bei Software-Applikationen

Software-Applikationen sind zentrale Bestandteile moderner IT-Infrastrukturen – und gleichzeitig beliebte Ziele für Angreifer. Das Verständnis typischer Angriffsvektoren ist essenziell, um Sicherheitsmaßnahmen gezielt einzusetzen.

**Definition:** Ein *Angriffsvektor* beschreibt den *Weg oder die Methode*, über den ein Angreifer versucht, in ein System einzudringen oder es zu manipulieren.

## 1. Häufige Angriffsvektoren

### 1.1 Unsichere Eingaben (Input Validation)

- **Beispiel:** SQL-Injection, Cross-Site Scripting (XSS), Command Injection
- **Problem:** Daten vom Benutzer werden nicht ausreichend geprüft oder bereinigt.
- **Folge:** Manipulation von Datenbankabfragen, Einschleusen von Schadcode, Session-Übernahme

### 1.2 Schwache Authentifizierung

- **Beispiel:** Brute-Force-Angriffe, Credential Stuffing, Session Hijacking
- **Problem:** Ungenügende Passwortregeln, fehlende Zwei-Faktor-Authentifizierung
- **Folge:** Unberechtigter Zugriff auf Benutzerkonten oder Admin-Oberflächen

### 1.3 Fehlkonfigurationen

- **Beispiel:** Offen gelassene Admin-Schnittstellen, Standardpasswörter, unnötige Ports
- **Problem:** Systeme werden mit unsicheren Standardeinstellungen betrieben
- **Folge:** Leichter Zugang für automatisierte Angriffe oder Botnetze

### 1.4 Unsichere API-Schnittstellen

- **Beispiel:** Fehlende Authentifizierung, unverschlüsselte Kommunikation
- **Problem:** APIs erlauben Datenzugriffe ohne ausreichende Kontrolle
- **Folge:** Datenexfiltration (Datenabfluss/klau), unautorisierte Aktionen durch externe Dienste

### 1.5 Alte oder ungepatchte Komponenten

- **Beispiel:** Veraltete Frameworks, Bibliotheken mit bekannten Schwachstellen
- **Problem:** Sicherheitslücken bleiben offen, obwohl längst bekannt

- **Folge:** Angreifer nutzen öffentlich dokumentierte Exploits

## 2. Weitere Vektoren (nicht direkt am Code)

- **Soziale Manipulation (Social Engineering):** Phishing, Telefon-Tricks, gefälschte Loginseiten
- **Client-seitige Angriffe:** Drive-by-Downloads, Browser-Exploits, manipulierte Anhänge
- **Drittanbieter-Integrationen:** Unsichere Plugins oder externe Services

### □ Fazit

Angriffsvektoren bei Software-Applikationen sind 'vielschichtig' und entwickeln sich ständig weiter. Sie reichen von trivialen Konfigurationsfehlern bis zu raffinierten Angriffsstrategien. 'Sicherheitsbewusstsein', 'sauberer Code', 'regelmäßige Tests' und 'Updates' sind entscheidend, um diese Vektoren zu schließen.



Volkan Demir

From:

<https://wiki.bzz.ch/> - **BZZ - Modulwiki**

Permanent link:

<https://wiki.bzz.ch/modul/m183/learningunits/lu03/03?rev=1752585507>

Last update: **2025/07/15 15:18**

