LU10b - SQLi Angriffsvarianten

Lernziele

1. Die Grundlagende Funktionsweise von SQLi erklären und demonstrieren können
2. Angriffsvektoren für SQLi nennen können.

Grundlegende Funktionsweise

Die Angriffstechnik *SQLI* verwendet Eingabemöglichkeiten aller Art (Angriffsvektoren) als Möglichkeit zu bestehenden SQL-Befehl zusätzliche einzuflechten. In der nachfolgenden Abbildung wird gezeigt, wie der im Programmcode bestehende SQL-Befehl durch eine vom Angreifer im Eingabefeld eingeschobenen SQL-Befehlserweiterung so verändert wird, dass der neue SQL-Befehl gültig und bleibt, die Gesamtlogik des SQL-Befehl aber massiv verändert wird.

Der neue Select-Befehl hat neu als Filterkriterium

```
…user_id=’’ OR 1=1’
```

Der erste Teil des Filters hat den Wahrheitswert *FALSE*, der zweite Teil hingegen TRUE. Die Datenbanklogik verknüpft diese beiden Werte durch eine OR-Verknüpfung, was logischer weise zu einem Filterwert *TRUE* führt. Alle Werte in der betroffenen Tabelle haben, sobald sie vorhanden sind, den Wert *TRUE*. Also wird der gesamte Datenbankinhalt herausgegeben.

Volkan Demir

From:
https://wiki.bzz.ch/ - **BZZ - Modulwiki**

Permanent link:
https://wiki.bzz.ch/modul/m183/learningunits/lu10/02?rev=1758264762

Last update: **2025/09/19 08:52**