LU11b - SQLi Angriffsvarianten

Lernziele

1. Die Grundlagende Funktionsweise von SQLi erklären und demonstrieren können
2. Angriffsvektoren für SQLi nennen können.
3. Nennen können wie SQLi gegen die das CIA-Triade durchgeführt wird

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.

CIA-Triad = Drei Dimensionen der IT-Sicherheit

Eine Applikation im Business-Umfeld hat grundsätzlich drei Dimensionen bzw. Ziele der Sicherheit zu gewährleisten:

- **Vertraulichkeit:** Userdaten sind weder bewusst noch unbewusst unbefugten zugänglich.
- **Verfügbarkeit:** Das System ist zu vereinbarten Zeiten vollumfänglich verfügbar.
- **Integrität:** Die Daten liegen unverfälscht vor.

Durch die Attacke *SQLi* wird im besten Falle eine, und schlimmsten Falle alle drei Dimension dieser Sicherheitsziele verletzt.

Angriff auf die Vertraulichkeit

Ein Angriff auf die Vertraulichkeit der Daten bedeutet, dass vertrauliche Informationen in die falschen Hände geraten. Die Absicht möglicher Angreifer ist es zusätzliche Informationen zu erbeuten. Beispiele solcher Informationen wäre spezifische

- Firmengeheimnisse
- Zugangsdaten
- Creditkarten-Informationen
- Etc.

Eine-SQLI, die auf die Vertraulichkeit abzielt hönnte wie folgt aussehen:

Original-SQL-Befehl	Ergänzter SQL-Befehl
SELECT author, subject, text FROM artikel WHERE ID=42;	SELECT author, subject, text FROM artikel WHERE ID=42 UNION SELECT login, password, 'x' FROM user;

Angriff auf die Verfügbarkeit

Je nach Geschäftsumfeld, ist die Verfügbarkeit von Business-Applikationen priorisiert. Der Lebensmittelladen um die Ecke kann sicherlich sein Geschäft auch ohne allzeit verfügbares IT-System betreiben. Ein Online-Shop hingegen kann sich nahezu keinen Ausfall leisten. Eine Verfügbarkeits-Attacke auf eine solche Applikation kann beispielsweise durch Löschen verschiedener Tabellen in der Datenbank erfolgen.

Original-SQL-Befehl	Ergänzter SQL-Befehl
SELECT * FROM user WHERE ID=105;	SELECT * FROM user WHERE ID=105;+DROP TABLE suppliers;<color> FROM user;

Angriff auf die Integrität

Ein Angriff auf die Integrität der Daten bedeutet, dass die Verlässlichkeit der Informationen verletzt wurde. Hier werden Informationen, mit oder ohne das Wissen der Betroffenen verändert. Das nachfolgende Szenario soll dies verdeutlichen. Mit dem nachfolgenden SQL-Statement

Original-SQL-Befehl	Ergänzter SQL-Befehl
SELECT author, subject, text FROM artikel WHERE ID=42;	SELECT author, subject, text FROM artikel WHERE ID=42;UPDATE USER SET TYPE=„admin“ WHERE ID=23;