LU10a - SQLi Grundlagen

Lernziele

1. Erklären können was eine SQLi ist und welches grundlegende Ziel diese Attacke hat.
2. Ursachen nennen können, warum SQLi auch in der Gegenwart ernstgenommen werden muss.

Einleitung

Die *SQL-Injection* ist eine Technik, die sich auf der OWASP-Top10-Liste seit Jahren grösster Beliebtheit erfreuen darf. Die *Popularität* verdankt das verdankt der Tatsache Attacken auf schlecht gesicherte Seiten einfach zu ermöglichen.

Ein *Injection* bedeutet *Einspritzung*, bzw. *einschleusen*. Eine SQL-Injection startet also Angriffe auf Datenbanken mithilfe von SQL-Anweisungen mit dem Ziel unrechtmässig an den Datenbankinhalt zu gelangen.

Bekannte Attacken

Diese nachfolgenden Beispiele zeigen, dass auch professionell erstellte Webapplikationen anfällig auf SQLI-Attacken sind.

- ListenpunktIm Oktober 2014 wturde in den Medien über einen Datenverlust bei der *PSN* (Playstation-Network) berichtet. Hinter der Schlagzeile «SQL-Injektion: Sicherheitslücke erlaubt Zugriff auf Sony-Kundendaten …“ verbarg sich eine SQLI-Attacke. Die 7 Millionen Benutzerdaten, die seitens unberechtigten abgezogen wurden, führten zu einem massiven Imageverlust.
- ListenpunktDie Business-Socialmedia-Plattform *linkedin* hat auf die gleiche Art und Weise im Jahre 2012 6.5 Millionen Benutzerdaten verloren.
- ListenpunktIm Juni 2016 verlor die „University of Greenich“ 2.7 GB vertraulicher Benutzerdaten

ihrer Studenten und Mitarbeitende.

Die eben aufgeführten Beispiele sind nur einige aus der lange Liste der *SQLI Hall-of-Shame*. Man kann also daraus folgern, dass die SQLI-Vulnerability (Verwundbarkeit) auch in der Gegenwart ernstgenommen werden muss.

Quellennachweis

- PortSwigger-What is SQLi?
