**Sicherheitslücken und ihre Ursachen in einer Applikation erkennen**

Ein Bild, das Text, Screenshot enthält.

Automatisch generierte Beschreibung

Es gibt eine Sicherheitslücke in der Verarbeitung der Benutzereingaben, da diese direkt in die SQL-Abfrage eingefügt werden. Diese Schwachstelle könnte von potenziellen Angreifern ausgenutzt werden, indem sie speziell gestaltete Zeichenfolgen eingeben, welche die SQL-Abfrage somit verändern oder erweitern, um auf unerlaubte Weise Zugriff auf die Datenbank zu bekommen. Diese Angriffe nennt man SQL-Injection-Angriffe.

**Gegenmassnahmen vorschlagen und implementieren**

Als Gegenmassnahme zu der oben beschriebenen Sicherheitslücke eignet sich die Verwendung von parametrisierten Abfragen, vor allem LINQ (Language Integrated Query). Anstelle eines direkten Zusammenbaus von SQL-Abfragen werden in LINQ-Befehlen die Benutzereingaben als separate Parameter behandelt. Diese Herangehensweise eliminiert die direkte Einbettung von Benutzereingaben in die SQL-Abfragestruktur. Durch die Verwendung von Variablen, die auf Spaltenwerte zugreifen, wird sichergestellt, dass die Benutzereingaben nicht als direkter Bestandteil der Abfrage interpretiert werden. Stattdessen werden sie als eigenständige Werte behandelt und sicher in die Abfrage eingebunden.

Ein Bild, das Text, Screenshot, Software, Multimedia-Software enthält.

Automatisch generierte Beschreibung