Sicherheitsüberlegungen

Beim Umgang mit Daten und Datenbanken müssen Sicherheitsüberlegungen von Beginn an bei der Anwendungsentwicklung berücksichtigt werden. Bei Applikationen, die Schnittstellen zum Internet haben, müssen solche Überlegungen eine noch zentralere Rolle spielen. Webapplikationen haben immer wieder schwerwiegende Sicherheitslücken, die dazu führen, dass sensitive Daten in falsche Hände oder die Öffentlichkeit gelangen.

Die OWASP listet in Ihrer "Top-Ten" die am häufigsten vorkommenden Fehler bei der Anwendungsentwicklung auf, auf Platz 1 befinden sich sogenannte "Injections" - diese Fehlerklasse betrachten wir im folgenden etwas genauer.

"Injection flaws"

> "Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization."

Weiterführende Informationen

Eine Injection-Sicherheitslücke entsteht vereinfacht gesagt immer dann, wenn man (Benutzer-)Eingaben ohne weitere Validierung übernimmt und an weitere Befehle oder in weitere Verarbeitungsschritte weiterreicht. Das passiert sehr leicht, da man beim Programmieren für gewöhnlich nicht darüber nachdenkt, welche unsinnigen oder gar bösartigen Eingaben Benutzer möglicherweise machen, sondern meist darauf konzentriert ist, die erwarteten Eingaben effektiv weiterzuverarbeiten.