Die Methoden der Hacker
SQL-Injections

Kopiere zur Vorbereitung die Dateien 🗎`fussballem.db`, 🗎`YeOldCheeseShoppe.db` und das Projekt 🗀`SuperSecureServer` aus dem Tauschordner. Du kannst eine der Datenbankdateien durch Doppelklick im Programm DB Browser for SQLite öffnen. Hier kannst du dir den Inhalt der Datenbank anzeigen lassen und SQL-Anfragen ausführen.

🧍💻 Aufgabe 1

a) Öffne die Datenbank 🗎`fussballem.db` und erkunde das Programm. Sende dann einige `SELECT` Anfragen an die Datenbank.

b) Nutze den `INSERT` Befehl, um neue Daten in die Datenbank einzufügen. Suchen sie dazu im Internet nach Ergebnissen anderer EM-Jahrgänge.

c) Nutze den `UPDATE` Befehl, um einige Datensätze zu verändern.

d) Nutze den `DELETE` Befehl, um einige (oder alle) Datensätze zu löschen.

💡 **Hinweis:** Unter `https://link.ngb.schule/sqlbefehle` findest du eine Übersicht der SQL-Syntax und Befehle.

💡 **Hinweis:** Falls du die Datenbank beim Arbeiten löscht oder „kaputt“ machst, kannst du dir die Originalversion erneut aus dem Tauschordner kopieren.

🧍💻 Aufgabe 2

Öffnen die Seite `https://link.ngb.schule/sqlinjection` und lies den Text bis zur Überschrift „Wie können Webserver helfen?“. Erkläre dir selber, was eine „SQL-Injection“ ist und welche Schwachstelle sie ausnutzt.

Die Beispieldatenbank zum Text findest du in der Datei 🗎`YeOldCheeseShoppe.db`. Hier kannst du die Abfragen selber nachvollziehen.

💡 **Hinweis:** Den ersten Teil brauchst du nur überfliegen, da die Grundlagen von SQLite beschrieben werden, die nun bekannt sein sollten. Interessant wird es ab der Überschrift „Verkettung von Zeichenfolgen: Die Wurzel allen Übels?“.

🧍💻 Aufgabe 3

Öffne das Projekt 🗀`SuperSecureServer` in BlueJ.

a) Erstelle einen neuen `SuperSecureServer` und probiere dich Anmeldung. Die Datenbank mit Nutzerkonten ist im Projektordner unter dem Namen 🗎`auth.db` gespeichert.

b) Studiere die Klasse `SuperSecureServer` und analysiere sie auf mögliche SQL-Injection Schwachstellen.

c) Versuch einen Weg zu finden, dich erfolgreich am Server anzumelden, ohne Nutzernamen oder Passwort eines Nutzers zu kennen.