PHP & MYSQL – WOCHE 9

Arbeitsblätter zum PHP-Unterricht

AUFGABE 1 – MYSQL INJECTION BEOBACHTEN

Du brauchst dazu

- Datenbank mit eingerichteter Tabelle «studenten»
- Lokalen Testserver (http://localhost)
- Script «student-search-form_ungesichert.php»

Falls dies noch nicht geschehen ist, bereite das Script vor, in dem du es im Testserver ablegst und in der Funktion mysqli_connect() Datenbank-Namen sowie allenfalls das Passwort anpasst. Es darf beim ersten Aufruf kein MySQL Verbindungsfehler angezeigt werden.

1. Schau dir zuerst im PHP-Code den Aufbau des SQL-Statements an.
   Welches Resultat erwartest du von dem Statement? Entspricht es dem, was die App verspricht?

2. Teste das Script, indem du eine Benutzereingabe machst. Wähle einen Namen, der in der Datenbank existiert, wie z.B. «Lena» oder «Peter»
   Was geschieht? Entspricht es dem, was das Statement tun sollte?

3. Nun bist du ein Hacker, und gibst statt einem Namen den folgenden Text ins Suchfeld:

```
test' OR 1 = 1; -- ' ]
```

   Was geschieht? Entspricht es dem, was das Statement tun sollte?

4. Du kannst noch weitere Eingaben ausprobieren, wenn du willst. Du musst dazu die Eingabe nicht unbedingt verstehen, sondern kannst dich auf das Resultat konzentrieren.

```
test' union select 2,'DB System: ',version(),'','; -- '
```

```
test' union select 1,ID,email,vorname,nachname FROM studenten; -- '
```

5. TAUSCHE DICH MIT DEINER GRUPPE AUS:

Mögliche Leitfragen:

- Wie können diese Eingaben ein solch unerwartetes Resultat erzeugen?
- Was wird da genau per User Input mitgeschickt?
- Wieso ist eine Manipulation, die z.B. die Version sichtbar macht, ein Problem?
- Inwiefern sind die Möglichkeiten für eine SQL-Injection abhängig vom ursprünglichen SQL Statement im Code?