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 testen. Du brauchst dazu die Eingabe nicht zu verstehen, sondern kannst dich auf das Resultat konzentrieren.

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

```
test' union select 1,studentID,student_email,student_firstname FROM studenten; -- '
```

5. SPRECHE MIT DEINER GRUPPE DARÜBER, WIESO DIESE EINGABEN EINEN SOLCHEN EINFLUSS AUF DAS RESULTAT HABEN KÖNNEN.