## 1- إعداد قاعدة بيانات اختبارية

افتح **MySQL Workbench** واتصل بقاعدة البيانات.

**إنشاء قاعدة بيانات وجدول:**

```
CREATE DATABASE SecurityTest;
USE SecurityTest;
CREATE TABLE Users (
   id INT AUTO_INCREMENT PRIMARY KEY,
   username VARCHAR(50),
   password VARCHAR(50)   );
INSERT INTO Users(username, password)VALUES('admin','password123'),('user1',
'mypassword');
```

---

## 2- محاكاة هجمات حقنSQL

**استعلام SQL بسيط يستخدم في تسجيل الدخول:**

```
SELECT * FROM Users WHERE username = 'input' AND password = 'input';
```

**تجربة حقن SQL عبر MySQL Workbench**

```
SELECT * FROM Users WHERE username = 'admin' -- ' AND password = 'anything';
```

- **التأثير** :تجاهل فحص كلمة المرور والسماح بالدخول غير المصرح به.

**هجوم آخر:**

```
SELECT * FROM Users WHERE username = '' OR '1'='1' -- ' AND password = '';
```

- **التأثير** :الشرط دائمًا صحيح، مما يكشف جميع المستخدمين.

## 3- منع حقنSQL

### استخدام العبارات المجهزة(Prepared Statements)

```
PREPARE stmt FROM 'SELECT * FROM Users WHERE username = ? AND password = ?';
SET @user = 'admin', @pass = 'password123';
EXECUTE stmt USING @user, @pass;
```

### تنفيذ أفضل الممارسات:

- تقييد إدخال المستخدم.
- استخدام تقنيات **تنقية البيانات**.
- منح أقل عدد ممكن من الصلاحيات **(Least Privilege Principle)**.