Part 1

1. **Using Prepared Statements (with Parameterized Queries)**

Prepared statements are easier for users to write and understand than dynamic SQL queries. Instead of inserting values directly into the command, SQL Command uses parameters to prevent the backend from running malicious queries that are harmful to the database.

1. **Validating use input**

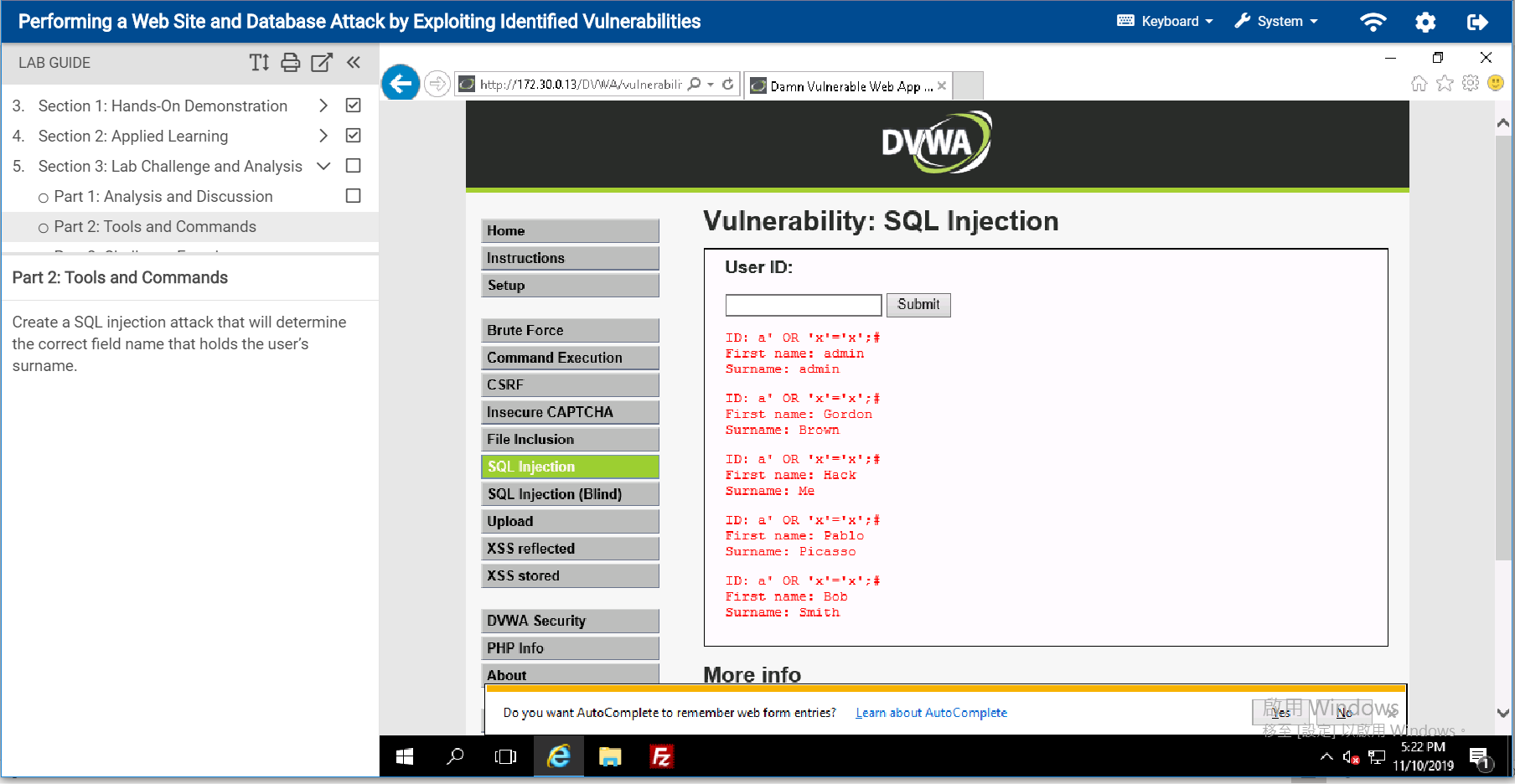
**Only the input which passed the validation can be processed to the database. We need to make sure the value is the accepted type, length, format, etc.**

1. **Keeping database credentials separate and encrypted**

**Encrypt database credentials and store them in a separate file, do not store sensitive data, and remember to delete information when it is no longer in use**

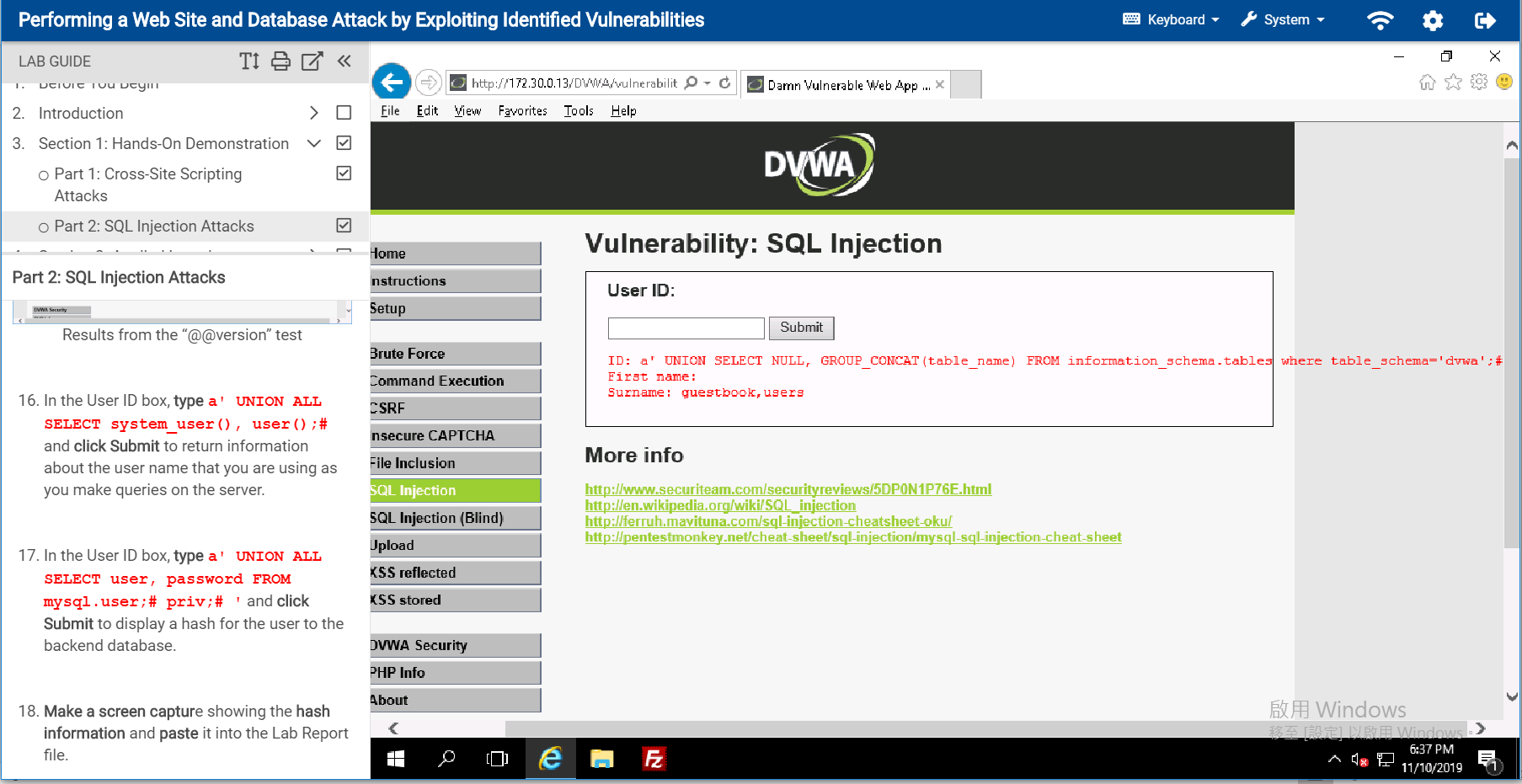
Source: <https://tableplus.com/blog/2018/08/best-practices-to-prevent-sql-injection-attacks.html>

Part 2



Part 3

The name of database that contains user data is dvwa. There are two tables under dvwa, guestbook table and users table.



Find all the column under the table schema: dvwa and table: users.

