SQL Commands to Demo

This part will be done after students have submitted their worksheets.

1. **Log into the database.**
    a. SQL is the language to talk to a database with
    b. SQL and Sequel mean the same thing, but you'll find out in about a week why there are two pronunciations
    c. Need individuals logins to a db
2. **use dvwa;** A db is like an Excel workbook or a Google Sheets file.
3. **show tables;** A database can contain multiple tables, like how an Excel spreadsheet can contain multiple worksheets.
4. **SELECT * FROM guestbook;** Not much in here
    a. Inform students they will learn all that they'll see over the next week or two
5. **SELECT * FROM users;** This is the data you were working off.
6. Let's look at the first SQL query that you made on the database.
   SELECT user_id, first_name, last_name FROM users WHERE user_id='';
    a. 1st query: 1
    b. 1st that didn't work? 6
    c. What about 0?
    d. What was the vulnerability? What was the query you typed in the textbook that tripped up the database? 1' or ''='
        i. Why did this work?
        ii. What else could we have tried?
        iii. Leave as exercise the shortest trick (query) that works
        iv. Q/C/Cs? (Questions/Comments/Concerns?)
7. **describe users;** Let's look at the schema, or the structure, of this table.
    a. Big diff w/ spreadsheets: columns define tables
    b. Cannot store extraneous info in db
8. You'll learn what all of this means. But what do you notice now that you recognize already? What have you seen in other CS classes?
   SELECT * FROM users WHERE user_id='1'; Don't press enter yet.
    a. Let me know if you want a hint.
    b. Hint: Something weird about the command and one of the columns
    c. Hint hint: Has to do with the types
9. **SELECT * FROM users WHERE user_id=5;**
    a. SQL can auto-convert different types
    b. SQL was designed for more than computer programmers, but also businesspeople, scientists, etc. So it's more user-friendly.
    c. In fact, the indices are 1-based, not 0-based.
10. **SELECT * FROM users WHERE first_name LIKE 'b%';** We can ask more complicated questions.
    a. Does case matter?
11. Final Q/C/C's?

Students may ask: Can anyone on the Internet directly issue the command to the database? Answer: Usually not. The database checks the IP address of the issuer's IP address, which doesn't match the database server's IP address. However, if you can get onto the server then it's easier.

In fact, I leave as a challenge after this lesson for students to hack the database. I don't tell them directly but all the config files are on there with the web pages, so once you find the right file you can get the username and password to the database. By the end of the unit they will have learned the commands needed to modify the data.