SQL Commands to Demo

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

1. Log into the database.
2. use dvwa;
3. show tables;
4. SELECT \* FROM guestbook;
5. SELECT \* FROM users;
6. SELECT \* FROM users WHERE user\_id=’’;
   1. 1
   2. 2
   3. 6
   4. 1’ or ‘’=’
      1. Why did this work?
      2. What else could we have tried?
      3. Any questions?
7. describe users;
8. You’ll learn what all of this means. But what do you notice now that you recognize already?
9. Do you notice something weird with our command (retype it) and this table description?  
   SELECT \* FROM users WHERE user\_id=’1’;
   1. Hint: Something weird about the command and one of the columns
   2. Hint hint: the data types column
10. SELECT \* FROM users WHERE user\_id=5;
11. SELECT \* FROM users WHERE first\_name LIKE ‘b%’;

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.