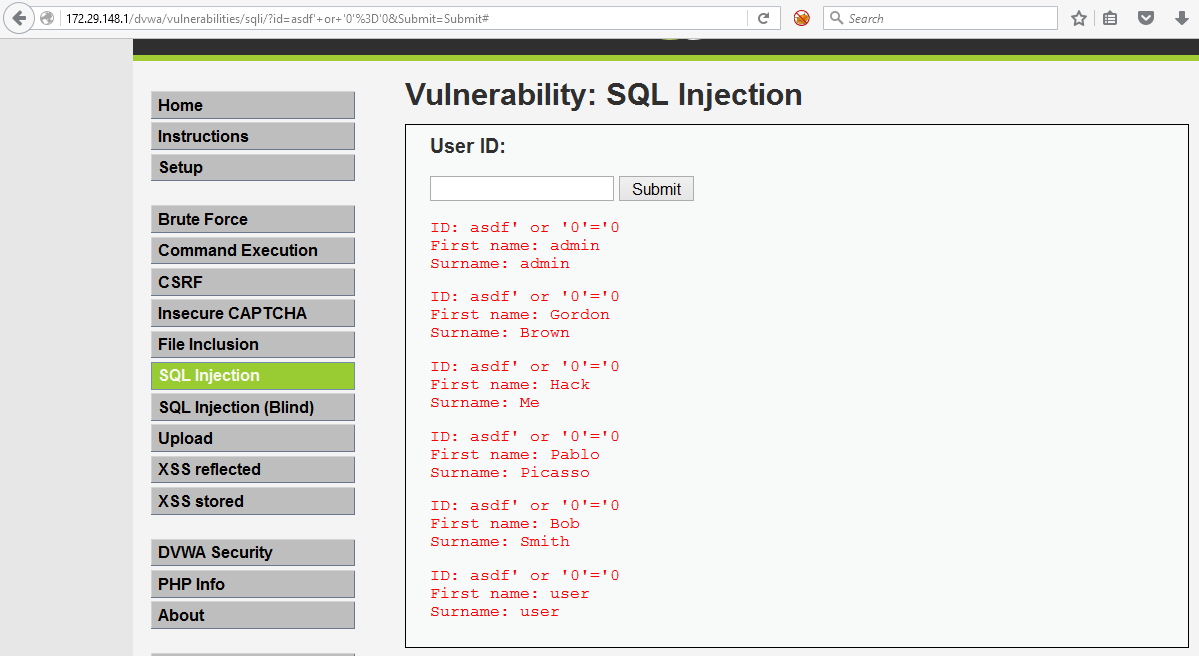
**QUESTION 1:** Download the HW6\_Lab\_Instructions from the Lab Instructions folder in Blackboard which will be used to answer the following questions.  Upload the screenshot of the result from Step 7 to answer this question.



### QUESTION 2: Explain what happened in Step 7 and why this attack worked.

It is a SQL injection. An attacker uses the injected data trick the interpreter into executing unintended commands or accessing data without authorization in order to steal data. This attack worked because the web application codes direct queries to a database for a web form submit button and attackers can inject their own queries.

### QUESTION 3: Explain why adding a final single quote after the last 0 in Step 8 doesn't allow this attack to work.

Anything between two single quotes is interpreted as a string (not as a query command.) Hence, if we add this single quote, the last 0 is interpreted as a string not a query command.

### QUESTION 4: From the result of Step 11, what is the server's OS?

5.1.41-3ubuntu12.6-log

### QUESTION 5: From the result of Step 13,  the SQL injection command that you entered was executed as which user?

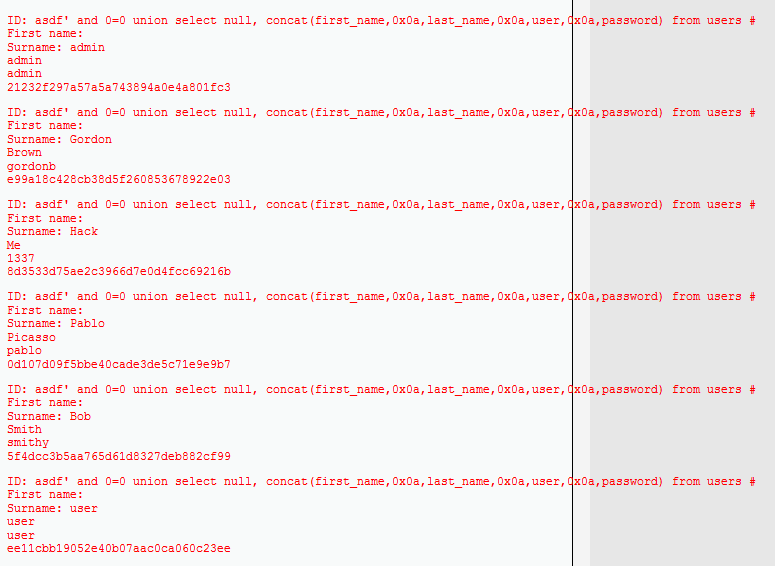
dvwa@localhost

### QUESTION 6: From the result of Step 15, what is the name of the database?  Also, why is the pound sign being used in these queries?

The database is dvwa.

# is the start of a comment in MySQL. It means that anything after that will be skipped by the parser. Using it can cause MySQL to ignore whatever is behind the # and execute only the stuff that comes before it. This is only effective against single-line SQL statements.

### QUESTION 7: Upload the screenshot of the result from Step 20.



### QUESTION 8: Take the password hashes from the result of Step 20 and decode the passwords using an online free password cracker.  Provide the clear text password result from each of the 6 hashes to answer the question.

clear text password result:

admin

abc123

charley

letmein

password

user

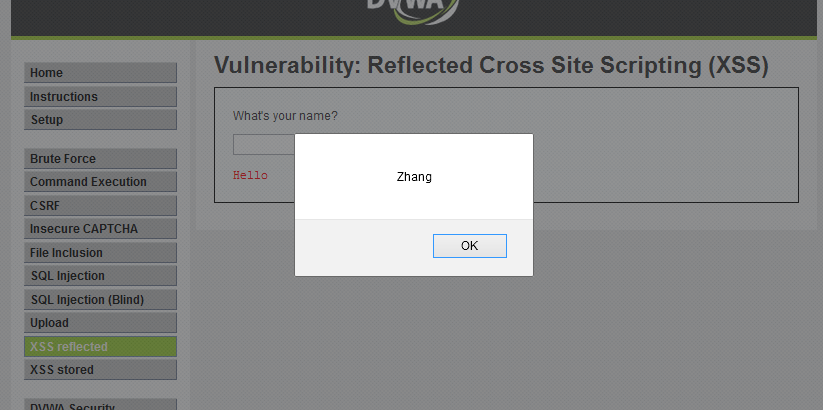
### QUESTION 9: What hashing algorithm was used on the password hashes?

### md5

### QUESTION 10: Enter the javascript code that allowed your last name to pop up in Step 25.

**<script>alert(“Zhang”)</script>**

### QUESTION 11: Submit the screen shot showing the pop up from Step 25.



### QUESTION 12: Upload the screenshot of the result from Step 36 showing the record with the iFrame.

