Solve challenge before viewing

answer!!

ANSWER ON NEXT PAGE

Entering **‘** as the username results in an error.

From the query, we can tell the general format of the SQL statement. –

**SELECT … FROM … WHERE username=’$username’ AND password=’$password’**

Since single quotes are not escaped, we are able to log in as username

**‘ or 1 #**

This is due to the SQL query we input evaluating to **true** and allowing us to log in.