Hello All!  
  
As far as databases are concerned, most of my professional experience has been in MySQL, administering it through the MySQL workbench. That is why I have chosen MySQL to be the dialect of topic for this discussion on SQL injection.

Like most SQL injection, MySQL can be vulnerable to appended statements that always equal true.

Such as ‘1’=’1’ or ‘a’=’a’. If a user is able to inject on to the statement an query that always returns true then the statement will execute.

According to OWASP, when an attacker is probing the database, they should first append a statement that is false and note the results( Example is 1=2). If they next append a statement that is true (Example 1=1) and the results from the first false test differ from results of the second true test, then the attacker has grounds to attempt a blind SQL attack. This is because they now know there is a different response for true and false statements and can query blindly accordingly.

Tips for preventing SQL injection

-Less User supplied input.

-Good user input validation.

-Using Prepared statements / Stored Procedures.

-Enforcing least privilege.

Thanks again!

-ERIC WEBB

<https://owasp.org/www-community/attacks/SQL_Injection>

<https://owasp.org/www-community/attacks/Blind_SQL_Injection>