SQL Injection

CSC365

Examples

Query = "SELECT * FROM Users WHERE Name ='" + user + "' AND Pass ='" + Pass + "'";

User: ' or ''='

Pass: ' or ''='

Now query becomes:

SELECT * FROM Users WHERE Name ='' or ''='' AND Pass ='' or ''='';

This might succeed.

Do not use string concatenation