SQL Injection

How it works, and the one fix that actually stops it.

Computing

Never build a query by concatenating user input. Pass it as a parameter, always.

BAD: "SELECT * FROM u WHERE n = '" + name + "'"

name = "'; DROP TABLE u; --" — **Two statements run**

The quote closes the string; the rest is code.

The fix — **WHERE n = ? with name passed separately**

The driver never treats it as SQL.

ORMs — **Safe by default, unsafe in raw mode**

Raw SQL methods bypass the protection.

THE COMMON MISTAKE

× Escaping quotes in the input yourself

✓ Using parameterised queries

Escaping depends on encoding, database and context. Parameterisation removes the question entirely.

Table and column names cannot be parameterised. If they must be dynamic, validate against an allowlist.