SQL Injections:

Use prepared statements so that the sql query is not passed by user. Rather, the user just specifies the parameters.

http://php.net/manual/en/mysqli.prepare.php