OWASP:

The Open Web Application Security Project is an online community dedicated to web application security. The OWASP community includes corporations, educational organizations and individuals from around the world.

According to OWASP the top three software security vulnerabilities are:

* Cross Site Scripting (XSS)
* Injection Flaws
* Malicious File Execution

SQL Injection:

* A database server is an essential part of modern web applications. It stores and processes the content.
* Database servers may have many databases.
* Each database may contain many tables.
* In SQL syntax, text or string provided by the user should be always enclosed in single quotes: ‘aleks’.
* SQL Injection:

$menu\_name = “’); DROP TABLE subjects; ‘”;

* The single quote character is part of the SQL language, not part of user’s input!
* SQL injection is the easiest way to hack websites or stolen data from the database.
* SQL injection is a relatively simple type of attack, and can be avoided with strict adherence to some basic coding practices.
* SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
* In case you forgot what “escaping” means in the context of programming, basically it’s just allowing special characters (like single/double quotes, percent signs, backslashes, etc.) in strings to be saved so that they remain as part of the string, and are not mis-interpreted as something else. For example, if we want to include a single quote in a string that gets output to the browser in PHP (note in the word “it’s” we have a single quote that will be output), then we have to add a backslash to the single quote so that PHP outputs it as a single quote:

echo 'Programmer Interview - It\'s Great!';

So, when this is displayed on a webpage it will look like:

Programmer Interview - It's Great!

This is what’s called escaping strings. If we did not escape the quote in our string then it would not output anything, and would result in a PHP error because the quote is also used to enclose the characters in an echo statement.

Avoiding’s strategies against SQL Injection Attacks:

1. Avoid dynamic SQL with concatenated input.
2. Use bind arguments or Parameterized query or Prepared Statement.
3. Filter and sanitize input.