));

}

Most Active Record methods accept parameters. To be safe, you should use these instead of just passing the raw data in.

As for quoting table names, columns, and other keywords, you can either rely on Active Record or use the whitelist approach.

See also

In order to learn more about SQL injections and working with databases through Yii, refer to the following:

• <http://www.slideshare.net/billkarwin/sql-injection-myths-and-fallacies>

• [http://www.viiframework.com/doc-2.0/yii-db-connection.html](http://www.yiiframework.com/doc-2.0/yii-db-connection.html)

• [http://www.yiiframework.com/doc-2.0/yi'-db-command.html](http://www.yiiframework.com/doc-2.0/yii-db-command.html)

• [http://www.yiiframework.com/doc-2.0/guide-security-best-practices.html#avoiding-sql-injections](http://www.yiiframework.com/doc-2.0/guide-security-best-practices.html%23avoiding-sql-injections)

• The Getting data from a database recipe in Chapter 3, ActiveRecord, Model, and Database