https://www.daguanren.cc/post/sql-injection.html

**防护 主要是采用方式1来解决**

1. 在设计应用程序时，完全使用参数化查询（Parameterized Query）来设计数据访问功能。
2. 在组合SQL字符串时，先针对所传入的参数作字符取代（将单引号字符取代为连续2个单引号字符）。
3. 使用其他更安全的方式连接SQL数据库。例如已修正过SQL注入问题的数据库连接组件。
4. 使用SQL防注入框架开发。