The solution that I have presented to thwart an SQL Injection attack is fairly simple. Simply put, I have a section of code that searches for the keyword " OR " within the input, notably with the spaces before and after the word. With this specific spacing, the input would likely be an SQL Injection "or" attack, and thus it will be stopped. In order to clean the text, I search for that keyphrase again using find(), and then take the substring before the "or" as the input text. Surprisingly enough, I encountered no issues coding this SQL Injection fix that I needed to fix.