数字使用数字转换。 或者数字也用单引号包起来。。

文本使用单引号包含，并且转移单引号和反斜杠。。或者其他特殊符号

字段名表名使用 波浪号包含起来。。注意转义里面的波浪号

/// <summary>  
    /// 过滤不安全的字符串  
    /// </summary>  
    /// <param name="Str"></param>  
    /// <returns></returns>  
    public static string FilteSQLStr(string Str)  
    {  
  
        Str = Str.Replace("'", "");  
        Str = Str.Replace("\"", "");  
        Str = Str.Replace("&", "&amp");  
        Str = Str.Replace("<", "&lt");  
        Str = Str.Replace(">", "&gt");

  //单引号替换成两个单引号  
            source = source.Replace("'", "''");  
  
            //半角封号替换为全角封号，防止多语句执行  
            source = source.Replace(";", "；");  
  
            //半角括号替换为全角括号  
            source = source.Replace("(", "（");  
            source = source.Replace(")", "）");  
  
            ///要用正则表达式替换，防止字母大小写得情况////  
  
            //去除执行存储过程的命令关键字  
            source = source.Replace("Exec", "");  
            source = source.Replace("Execute", "");  
  
            //去除系统存储过程或扩展存储过程关键字  
            source = source.Replace("xp\_", "x p\_");  
            source = source.Replace("sp\_", "s p\_");

  //防止16进制注入  
            source = source.Replace("0x", "0 x");

/// 过滤SQL字符。  
        /// </summary>  
        /// <param name="str">要过滤SQL字符的字符串。</param>  
        /// <returns>已过滤掉SQL字符的字符串。</returns>  
        public static string ReplaceSQLChar(string str)  
        {  
            if (str == String.Empty)  
                return String.Empty; str = str.Replace("'", "‘");  
            str = str.Replace(";", "；");  
            str = str.Replace(",", ",");  
            str = str.Replace("?", "?");  
            str = str.Replace("<", "＜");  
            str = str.Replace(">", "＞");  
            str = str.Replace("(", "(");  
            str = str.Replace(")", ")");  
            str = str.Replace("@", "＠");  
            str = str.Replace("=", "＝");  
            str = str.Replace("+", "＋");  
            str = str.Replace("\*", "＊");  
            str = str.Replace("&", "＆");  
            str = str.Replace("#", "＃");  
            str = str.Replace("%", "％");  
            str = str.Replace("$", "￥");