



链滴

# 关于 sql 注入的简单过滤

作者: [limao](#)

原文链接: <https://ld246.com/article/1576650153524>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

```

/**
● SQL过滤
●

*/
public class SQLFilter {

/**
* SQL注入过滤
* @param str 待验证的字符串
*/
public static String sqlInject(String str){
    if(StringUtils.isBlank(str)){
        return null;
    }
    //去掉"|;"\字符
    str = StringUtils.replace(str, "|", "");
    str = StringUtils.replace(str, "\", "");
    str = StringUtils.replace(str, ";", "");
    str = StringUtils.replace(str, "\\", "");

    //转换成小写
    str = str.toLowerCase();

    //非法字符
    String[] keywords = {"master", "truncate", "insert", "select", "delete", "update", "declare", "alter", "drop"};

    //判断是否包含非法字符
    for(String keyword : keywords){
        if(str.indexOf(keyword) != -1){
            throw new RuntimeException("包含非法字符");
        }
    }

    return str;
}
}

```