ThinkPHP5.0.10框架exp表达式慎重使用不然可导致sql注入

0x00 说说说说说说说说说说说明

ThinkPHP是一个免费开源的，快速、简单的面向对象的轻量级PHP开发框架，是为了敏捷WEB应用开发和简化企业应用开发而诞生的。ThinkPHP从诞生以来一直秉承简洁实用的设计原则，在保持出色的性能和至简的代码的同时，也注重易用性。

Thinkphp提供非常多的表达式，其中 EXP可以外部操控时，会因没有过滤导致sql注入。

0x01漏洞利用

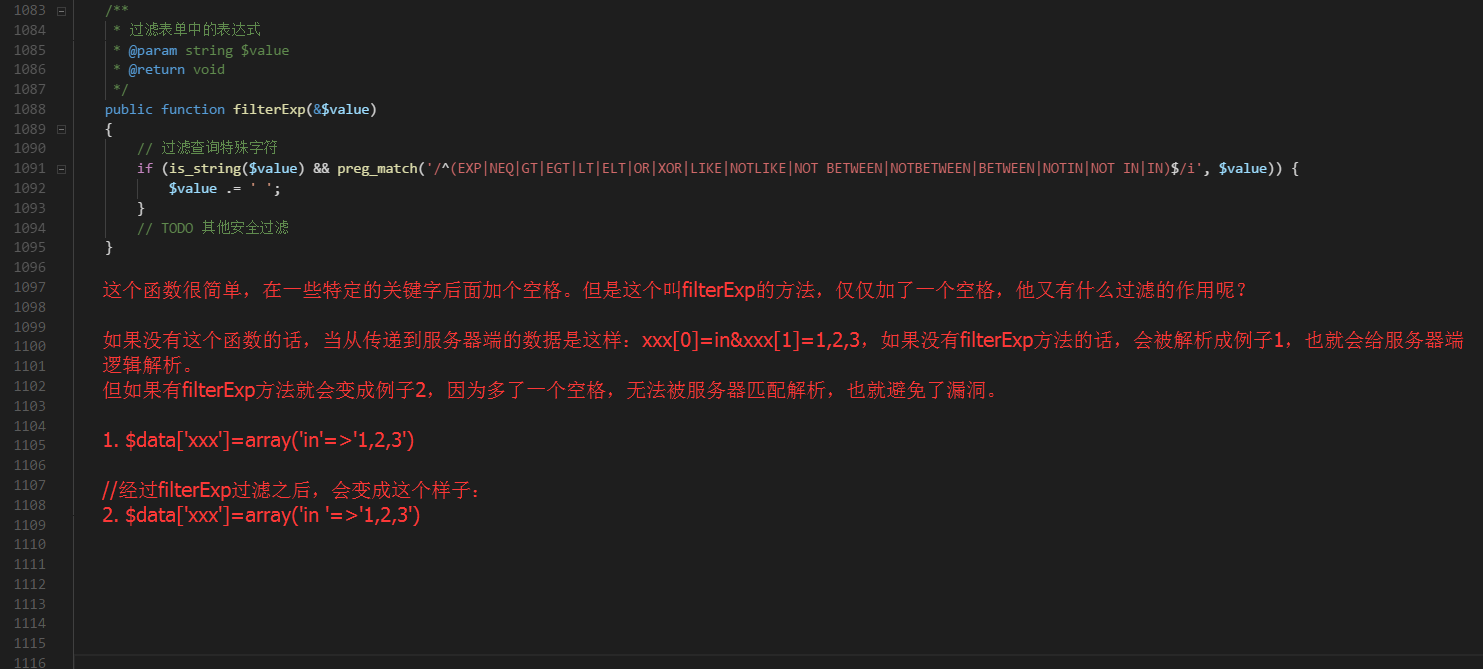
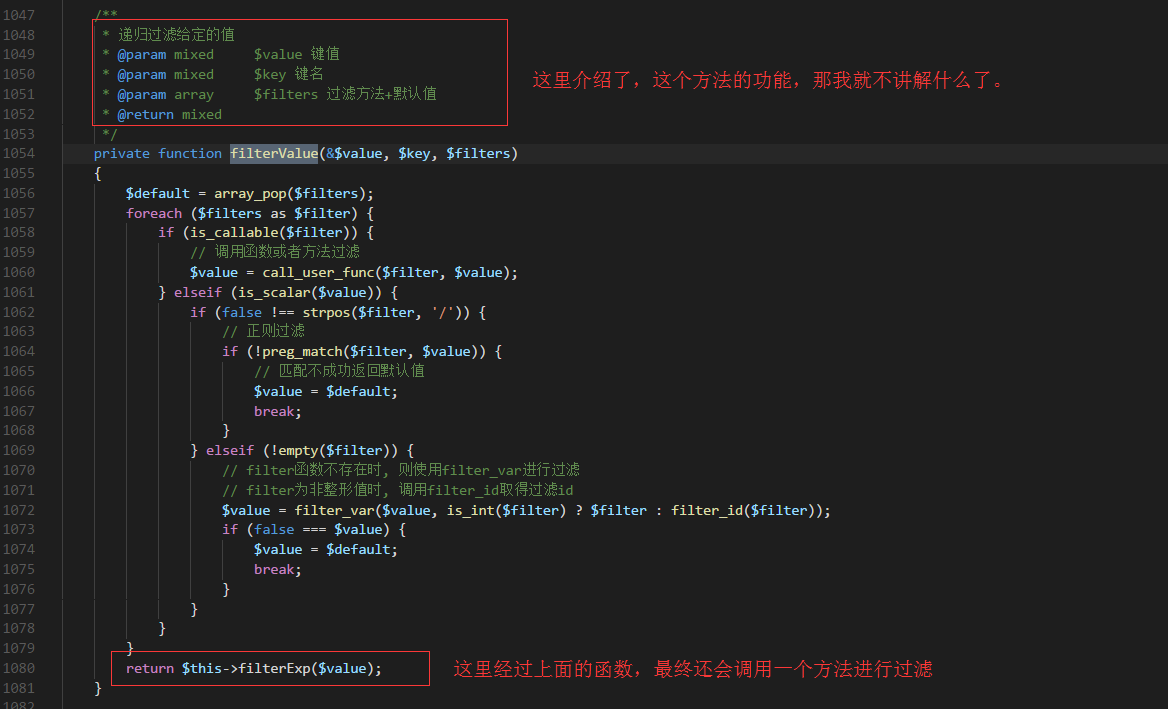
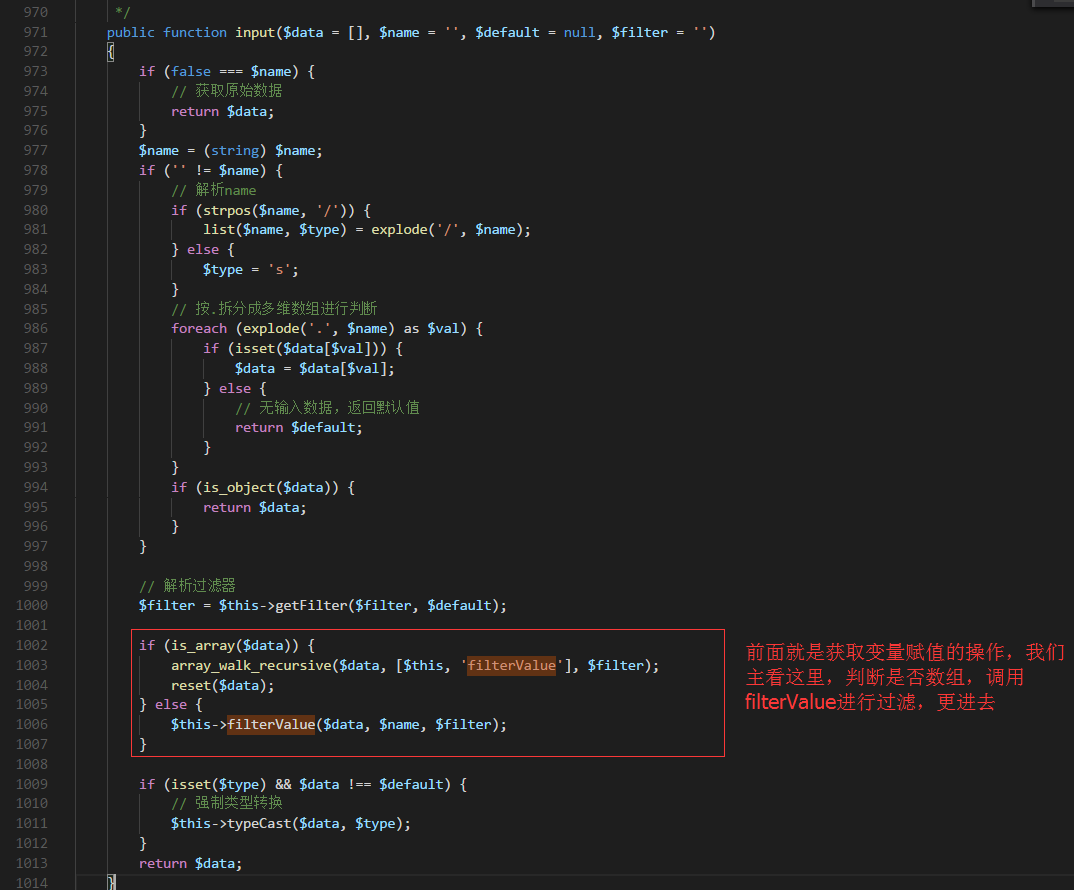




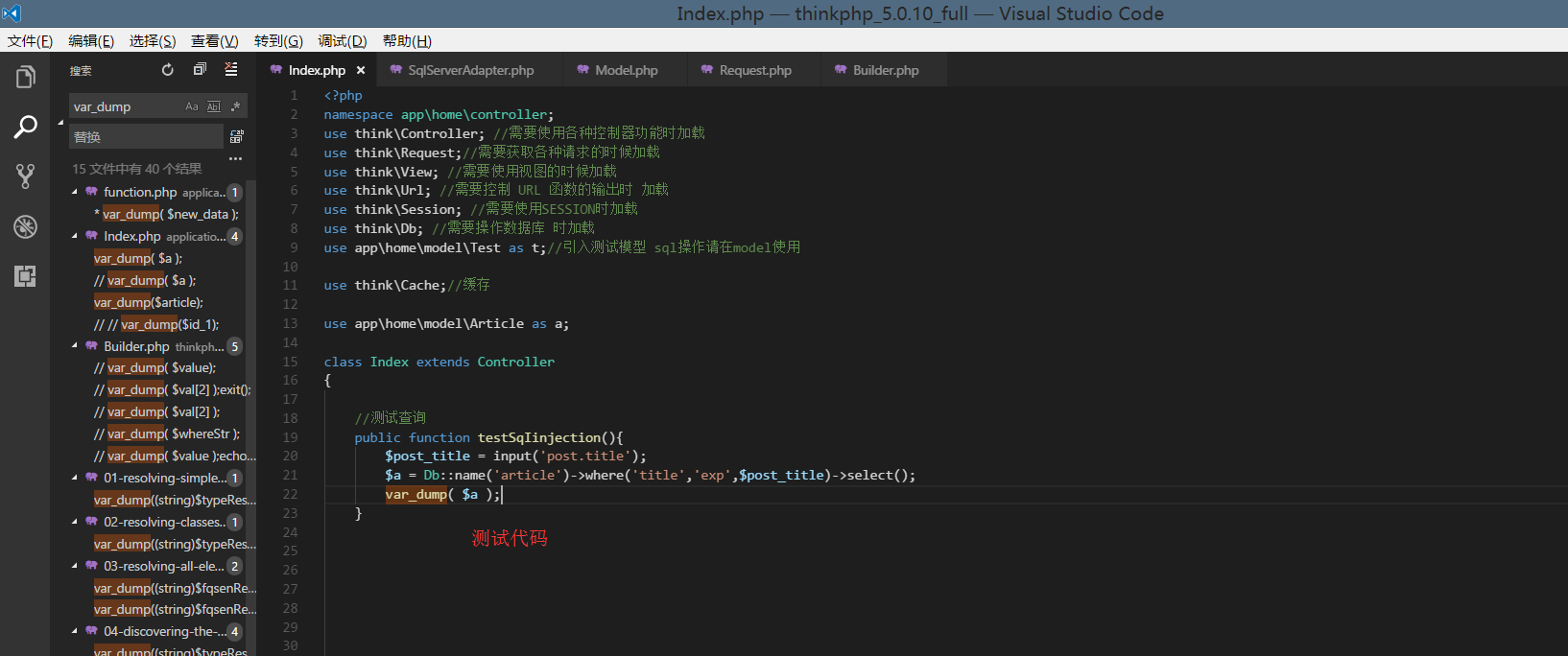
这里来看看TP系统核心安全函数之一input函数，他可以帮助我们获取各种变量与自动过滤的功能等。

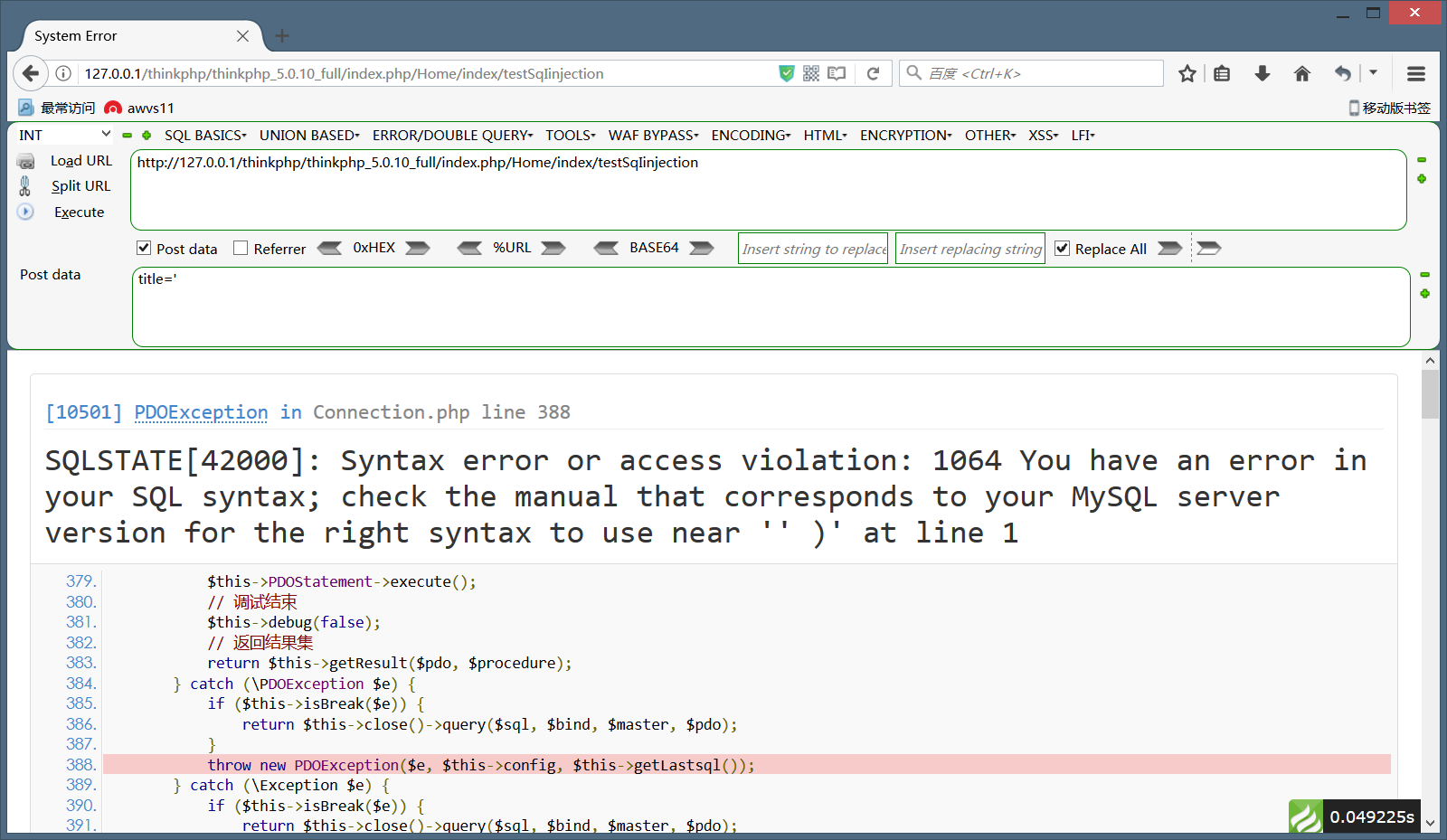
文件： thinkphp\library\think\Request.php

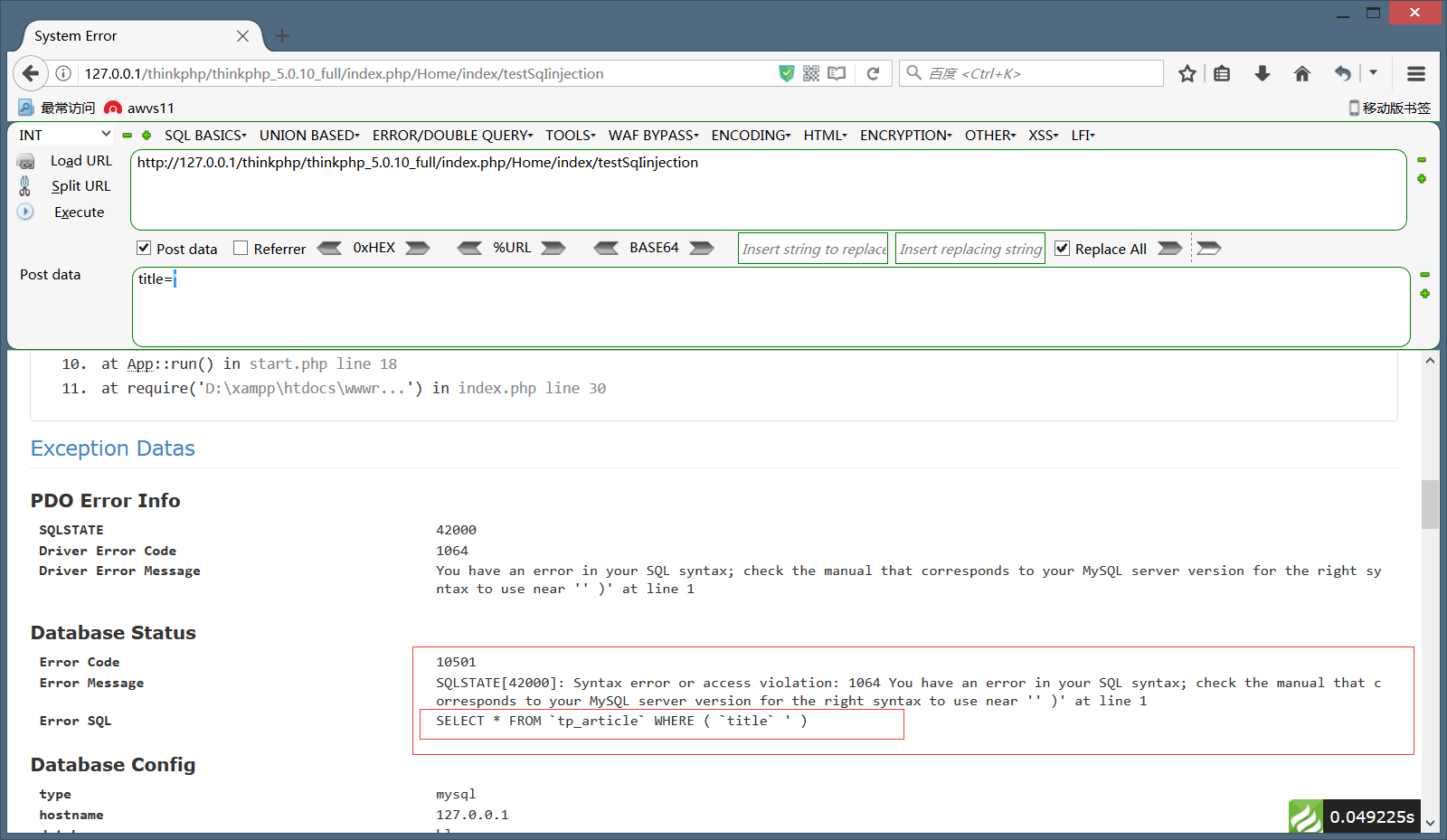
方法： input()

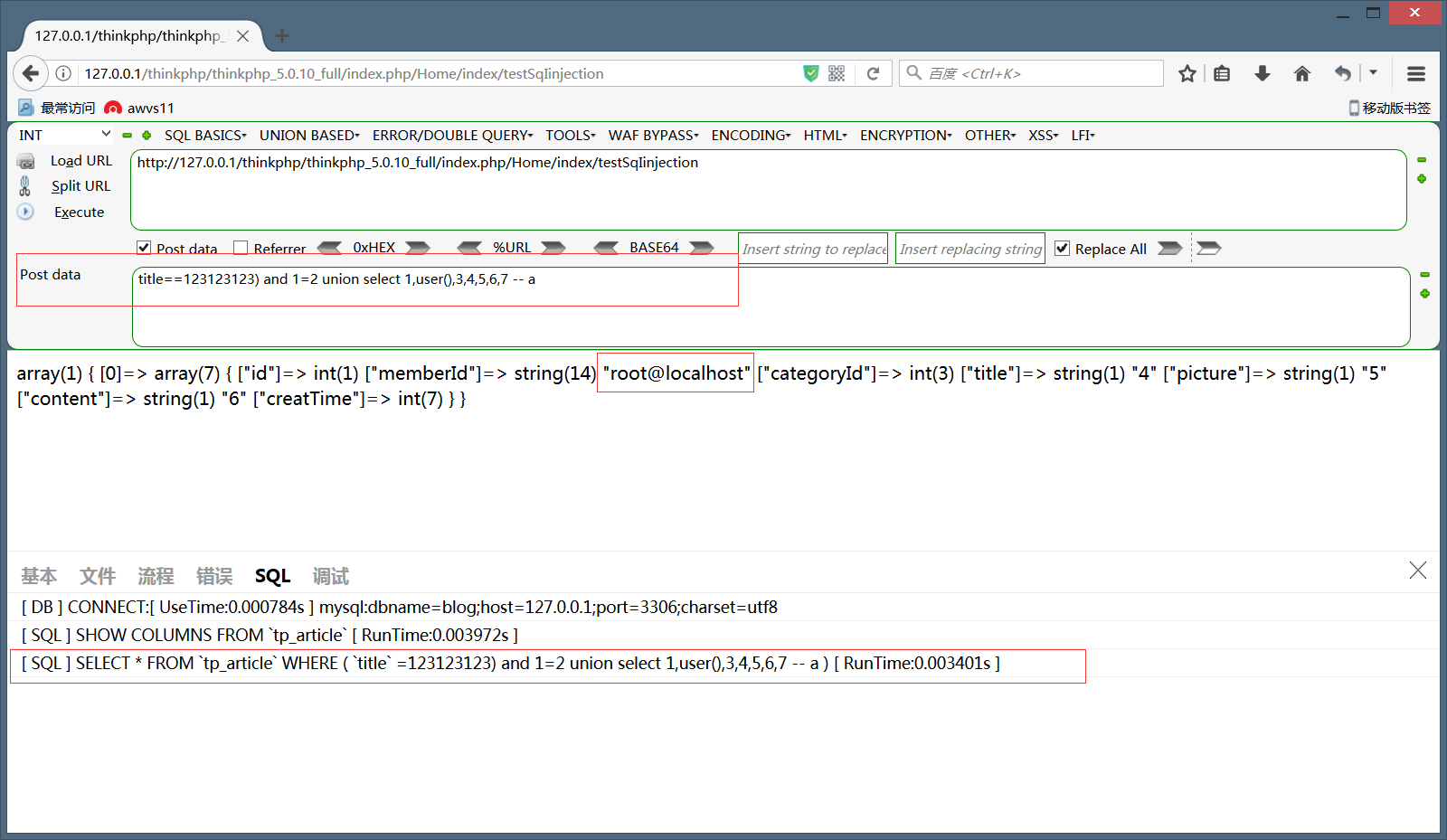


漏洞例子1：



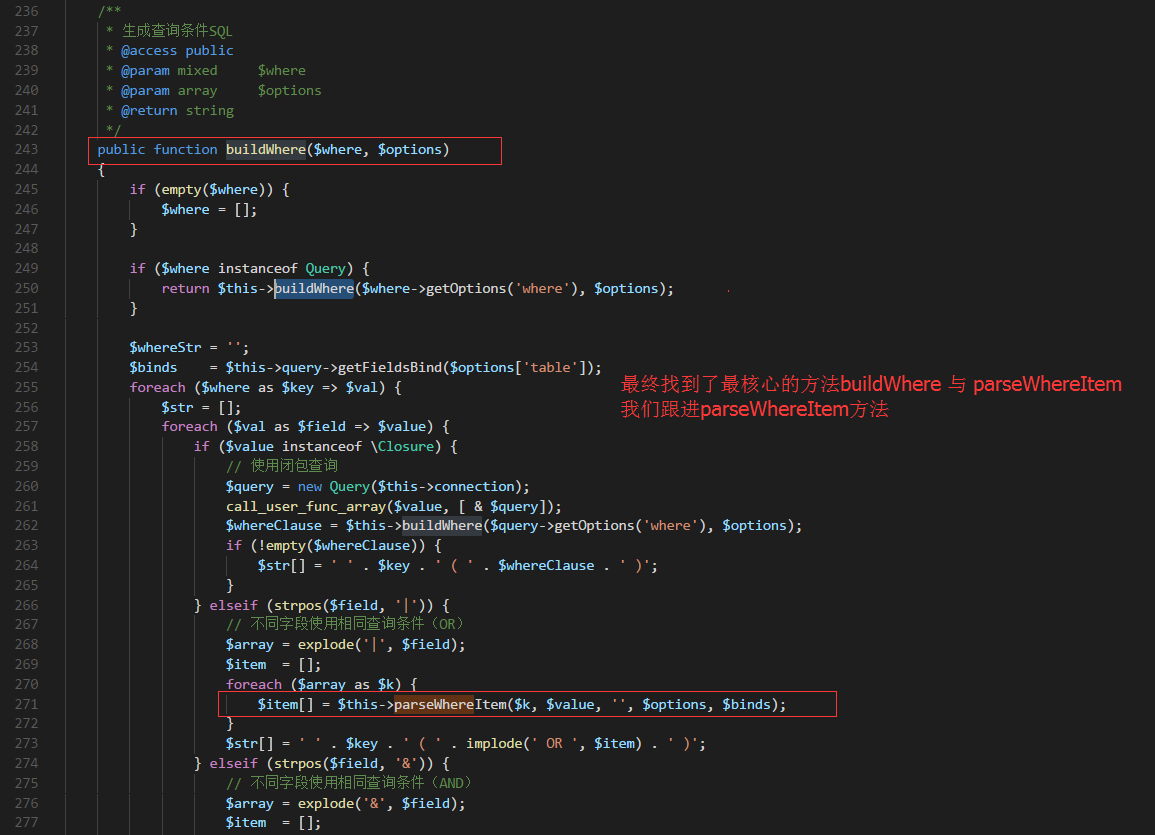




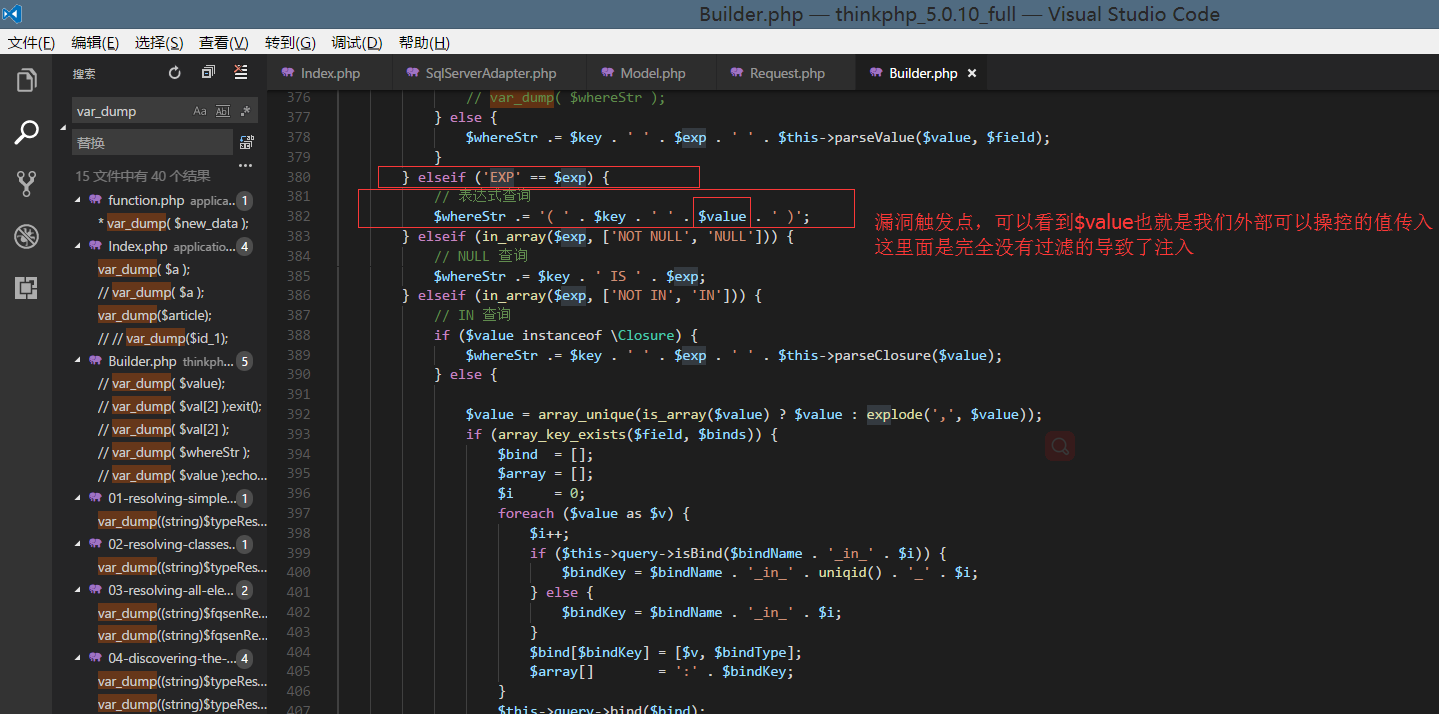












建议：使用exp表达式的时候不要让外部可操控就是一个注入。