# 简介

应用程序在向后台数据库传递SQL（Structured Query Language，结构化查询语句）查询时，如果为攻击者提供了影响该查询的能力，就会引发SQL注入。

一个正常的PHP数据查询语句：

$conn = mysql\_connection($host, $username, $password)

$query = “select \* from users where user=’admin’ and passwd=’”

$query = $query.$\_GET[“passwd”].”’”；

$result = mysql\_query($query);

这里查询语句中的passwd是根据用户输入设定的，没有做任何的限定，攻击者可以利用这个修改查询语句。

# 原理

# 测试