

# 封神台SQL注入-延时注入

原创



VIP文章 炎鳳先生



于 2020-10-05 12:47:20 发布



189



收藏

分类专栏: [Web安全微专业](#) [渗透](#) [黑客](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_40941912/article/details/108927685](https://blog.csdn.net/qq_40941912/article/details/108927685)

版权

## 一、原理

所谓的盲注就是在服务器没有错误回显的时候完成的注入攻击。

服务器没有错误回显, 对于攻击者来说缺少了非常重要的“调试信息”。

- 布尔盲注
  - 布尔很明显True跟False, 也就是说它只会根据你的注入信息返回True跟False, 也就没有了之前的报错信息
- 时间盲注
  - 界面返回值只有一种, true 无论输入任何值 返回情况都会按正常的来处理。加入特定的时间函数, 通过查看web页面返回的时间差来判断注入的语句是否正确

相关函数

length() => 返回(字符串)长度的数值

substr([],[A],[B]) => 返回[]值中, [A]开始[B]位后的字符值

ascii() => 通过数值返回(此处内容)的阿斯克码

sleep()

if(expr1.expr2,expr3) =>判断语句, 第一个正确执行2, 错误执行3

## 二、作业

### (一) SQL注入-延时盲注 Rank 1

页面原始URL: <http://inject2.lab.aqlab.cn:81/Pass-13/index.php?id=1>

任务:

通过延时注入获得flag。

对该页面进行GET传参, 传参名为id

我们发现，在这个页面，无论传入怎样的参数，页面始终都不会变化，我们无法从页面变化得知数据库是否执行了我们的传参

## 全学院SQL注入靶场

s-01  
s-02  
s-03  
s-04  
s-05  
s-06  
s-07  
s-08  
s-09  
s-10  
s-11  
s-12  
s-13  
s-14  
s-15  
s-16

### 本关考点:

延时注入（一）

### 任务

通过延时注入获得flag。

对该页面进行GET传参，传参名为id

### 数据库查询语句:

```
select *from news where id="9" and 1=2 --qwe"
```

### 查询结果:

有数据

通过sleep函数确定存在时间盲注

传入，等待四秒后页面才返回，确定存在盲注

```
" and
```