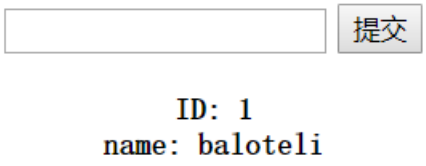
CTF实验吧-简单的sql注入【SQL注入关键词绕过】

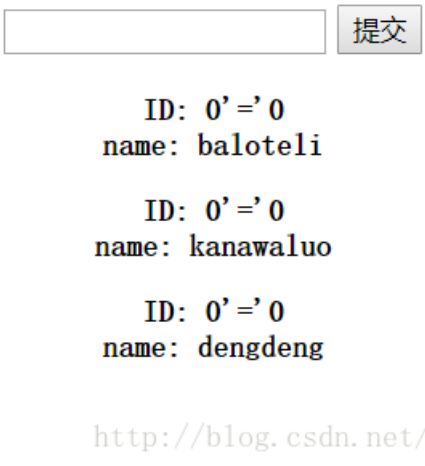
原创

Sp4rkW 于 2017-07-21 16:32:07 发布 1904 收藏 2
文章标签： ctf web 实验吧 sql注入

首先尝试性的试了一个1，



然后试了一下0'='0，将所有值输出看看



这也证明了"没有被题目给过滤掉

接下来开始尝试and语句准备试出其表名，按实验吧的习惯，一般都是存在flag表的flag字段中，不过还是尝试一下

然而，报错，and，select，from等词汇均被忽略了

试了一些方法，均不可解决，下面方法参考了实验吧作者双眼皮的双子座和pcat的思路，侵删

第一种：

```
1' unionunion  selectselect  flag fromfrom  flag wherewhere  '1'='1
```

重复加空格重复

第二种：

/*!关键字*/ 即可越过忽略保留关键字

以上两种方法均可测试存在flag表，flag字段，而答案也确实在其中，，，不愧是实验吧，老套路，哈哈哈

不过还是很好奇，这种忽略的手法是什么，为什么这样就能跳过忽略保留关键字，欢迎大佬指教！