

来自一个一周就写了一题的菜鸡。

其实表面上是这样，其实还是尝试了很多的。xss我自己都被hack8次了，submit就不行。。

web--sqli--1:

118.89.111.179:3000/?id=1&code=ydqrct37

新标签页

x



Django Admin

x



《You I

```
substr(md5($_GET["code"]),0,4) === bf3f
array(1) { ["word"] => string(7) "welcome" }
```

- 然后搞一个1-1试一下，就发现是数字型注入了。
- 一个回显位，然后依次爆库爆表等等得到tablename=f1111111g
columnname=f14444444g 然后拿flag。

哦对了，这个code脚本也要说，就是取样然后md5对比一哈

```
1 import hashlib
2 import random
3
4 def rstring(i):
5     string=''
6
7     ran=random.sample('abcdefghijklmnopqrstuvwxyz123456789',i)
8     return string.join(ran)
9
10 def md5(thing):
11     return hashlib.new('md5',thing.encode('utf-8')).hexdigest()
12
13 for x in range(1000000):
14     randomstring=rstring(8)
15     target=md5(randomstring)
16     if target[:4]=='bf3f': #tablename=f1111111g
17         columnname=f14444444g
18         print(randomstring)
19         break
20     else:
21         print('第%d次失败'%x)
```

