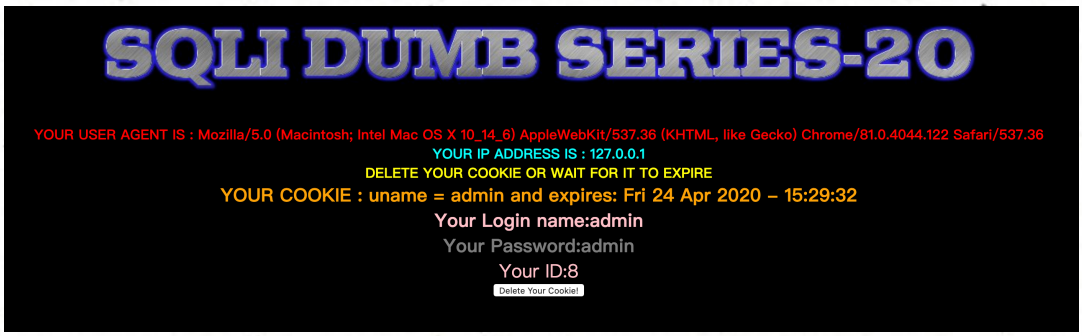
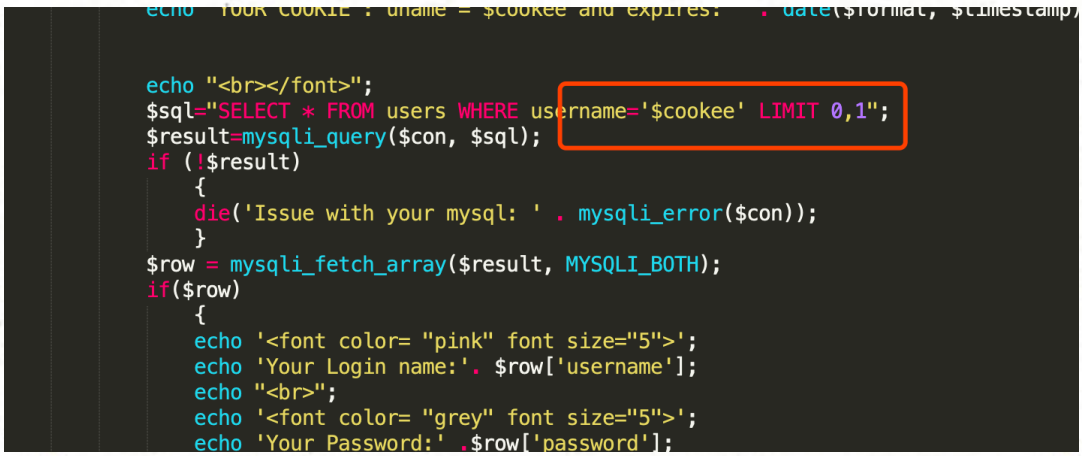
admin admin登录后

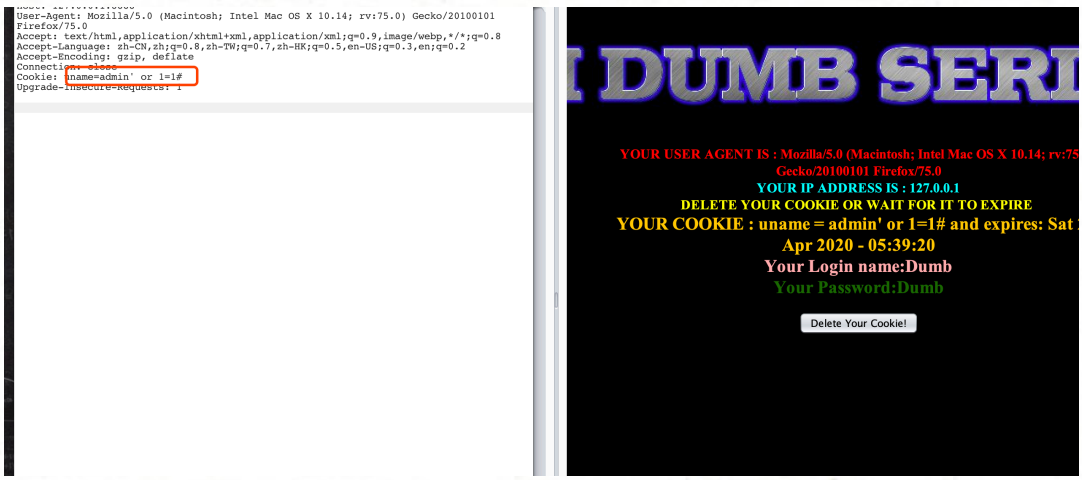


看源码发现username和password一样被check了，但是回显了cookie的信息，因此没准可以用cookie注入

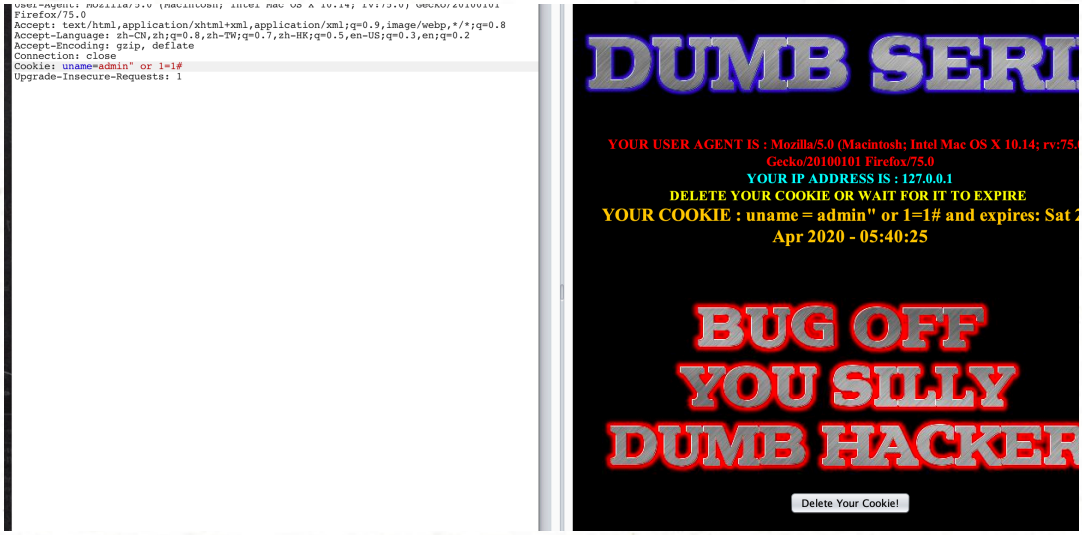


```
echo "<br></font>";
$sql="SELECT * FROM users WHERE username='$cookee' LIMIT 0,1";
$result=mysqli_query($con, $sql);
if (!$result)
    {
    die('Issue with your mysql: ' . mysqli_error($con));
    }
$row = mysqli_fetch_array($result, MYSQLI_BOTH);
if($row)
    {
    echo '<font color= "pink" font size="5">';
    echo 'Your Login name:'. $row['username'];
    echo "<br>";
    echo '<font color= "grey" font size="5">';
    echo 'Your Password:' .$row['password'];
```

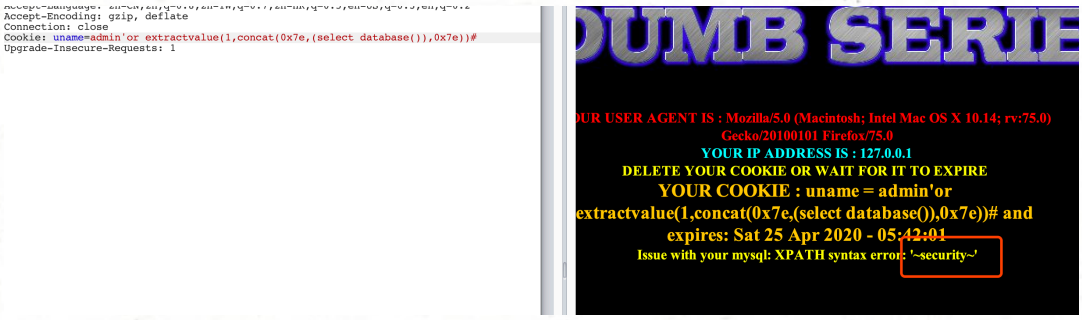
这里查询的时候用到了cookie，说明存在注入点



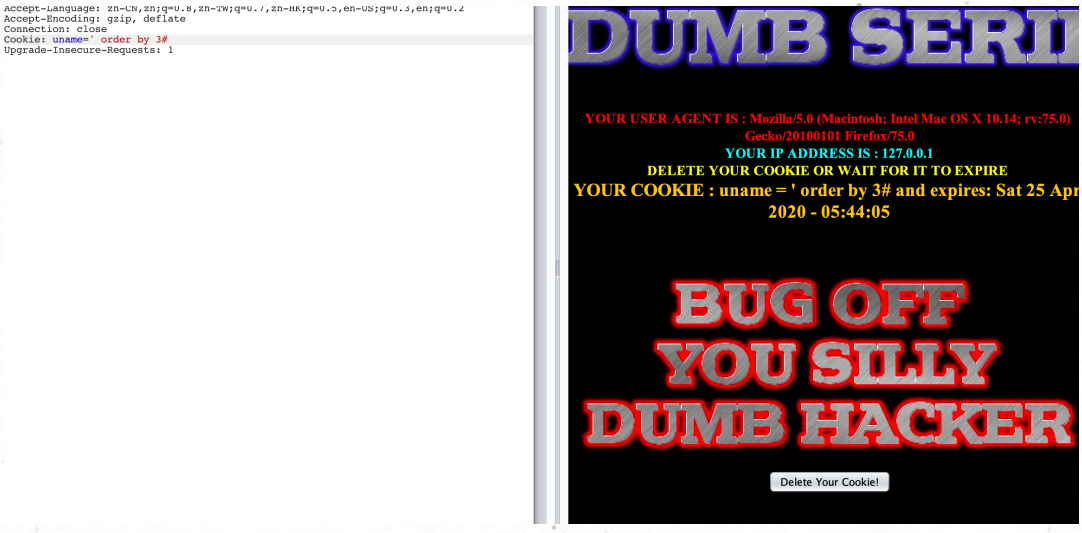
没有报错 说明是单引号型，双引号就会报错

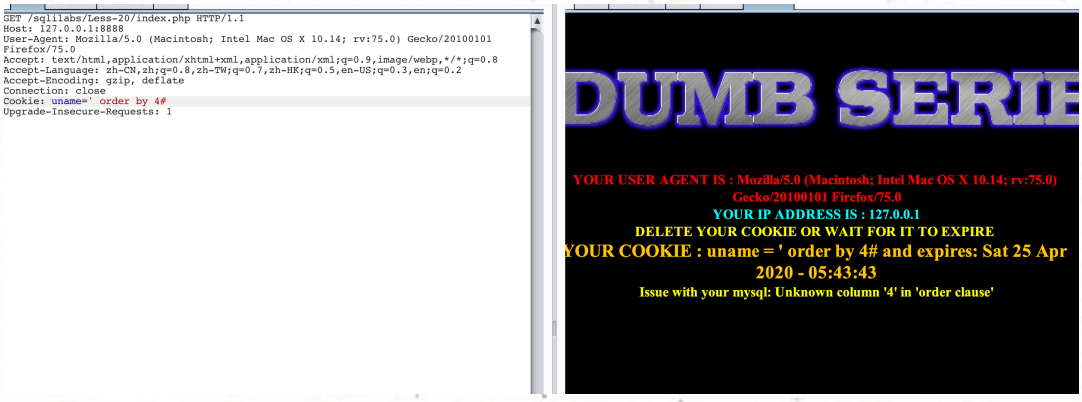


通过报错注入可以做



通过union联合查询也可以做,先用order by 测出来查询了3列





然后寻找回显位置，这个题有回显，因此可以用union联合查询