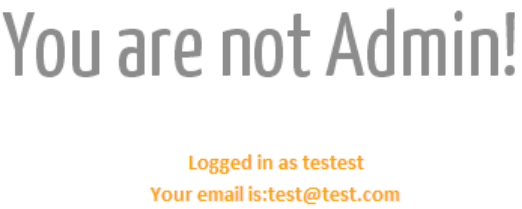
Challenge 13

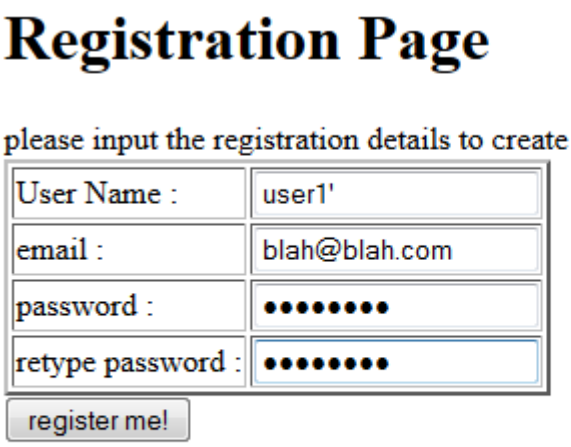
http://192.168.2.11/sqli/admin2/ [Level: Advanced]

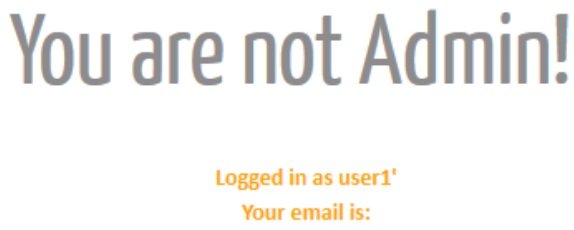
- Login as admin to obtain the flag

Note that after you login, you get displayed your registered email:



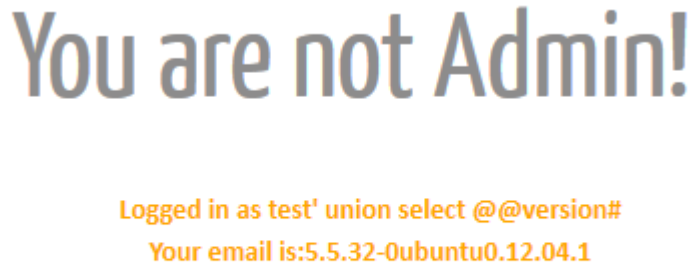
You will also find that although the registration page or login page is not vulnerable to SQL Injection, if you register with a crafted name (username with single quite in it), the email is not displayed, possibly because of 2nd order SQL Injection:





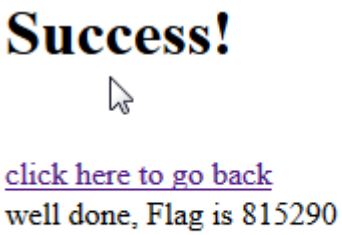
Let's start playing by registering crafted username and see if we can pull out data from back-end database:

test' union select @@version#



test' union select password from users #

This gives you the first password which is the password for admin user. Login as admin



Further reading:

- http://www.esecforte.com/blog/second-order-sql-injection/
- http://stackoverflow.com/questions/12952187/how-do-i-demonstrate-a-second-order-sql-injection