Challenge 12

http://192.168.2.11/sqli/admin1/ [Level: Advanced]

- Login as admin to obtain the flag

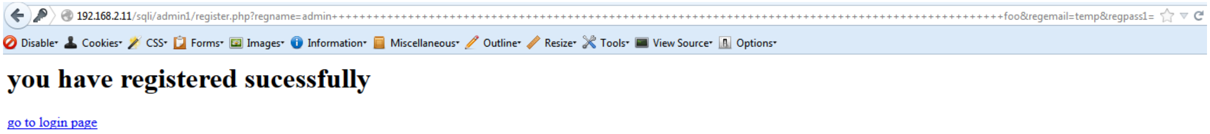
  Note: The application has a registration page but does not let you register as admin as that user already exist.

  Read about mysql truncation issue and that mysql ignores the trailing spaces when doing a string comparison:

  http://www.suspekt.org/2008/08/18/mysql-and-sql-column-truncation-vulnerabilities/

  You need to register a user with name:

  - admin<followed by lots of space which basically fills out the field length defined for username field in database><followed by some characters>
  - e.g. "admin   foo"



Now login with the username 'admin' and the password you set for the crafted username.