Challenge 10

http://192.168.2.11/sqli/sql8/ [Level: Advanced]

- Which parameter is vulnerable?

  Sort_results

- Provide test case to confirm the sql injection vulnerability

  True case:

  sort_results=(select 1)

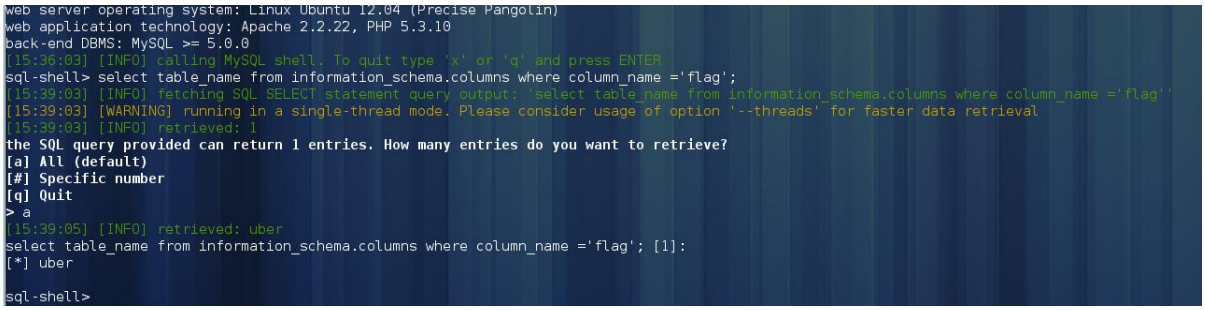
  False case:

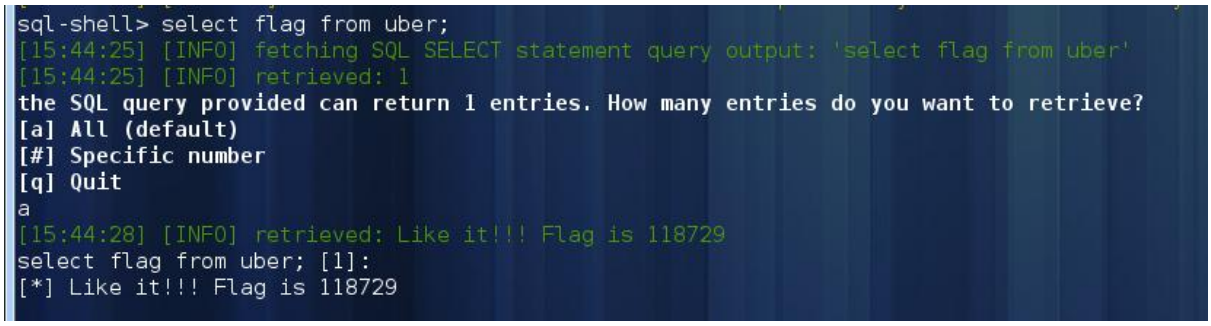
  sort_results=(select 1,2)

  Read more about this here:

  http://www.notsosecure.com/blog/2008/08/01/injection-in-order-by-clause/

- Obtain the database username and flag.





Further reading:

http://www.tuxz.net/blog/archives/2010/11/21/sql_injection__exploiting_the_order_by_clause/

http://www.gremwell.com/exploiting_sql_injection_in_order_by_on_oracle