Challenge 8

http://192.168.2.11/sqli/sql6/ [Level: Intermediate]

- Which parameter is vulnerable

  Message parameter is vulnerable

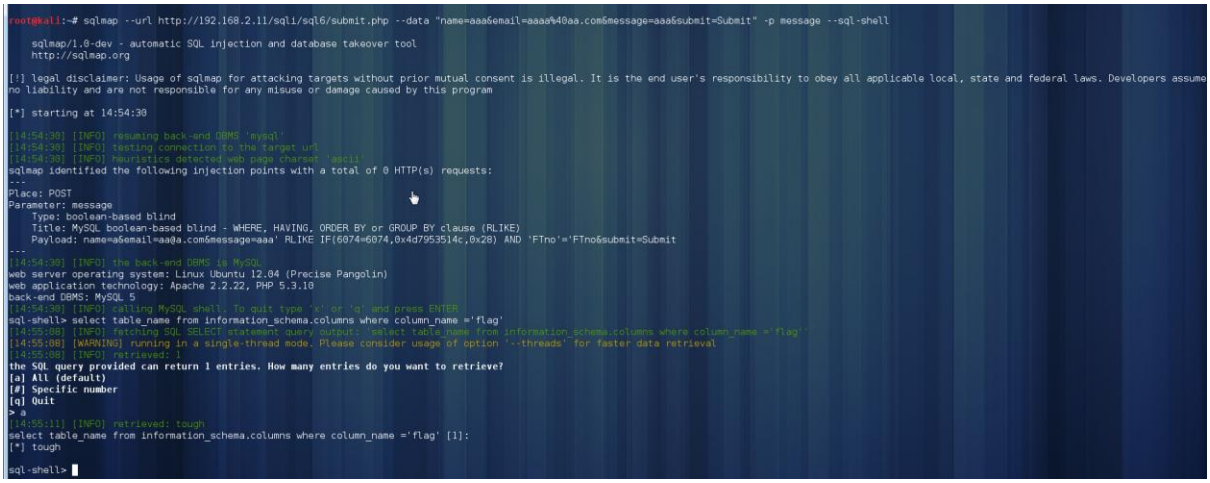
- List techniques by which SQL Injection can be exploited

  Time delay functions benchmark() or sleep()

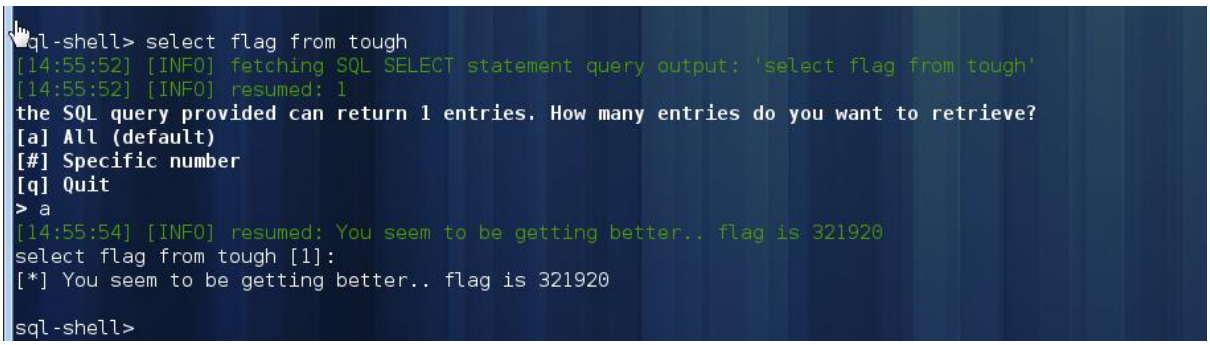
  You can use TRUE and ERROR technique described here:

  http://www.notsosecure.com/blog/2008/05/26/if-query-data-manipulation/

- Obtain the table which contains the column flag



- Obtain the flag



Further reading:

http://www.slideshare.net/matt_presson/timebased-blind-sql-injection

http://hakipedia.com/index.php/SQL_Injection#MySQL_BENCHMARK

http://www.notsosecure.com/blog/2008/05/26/if-query-data-manipulation/