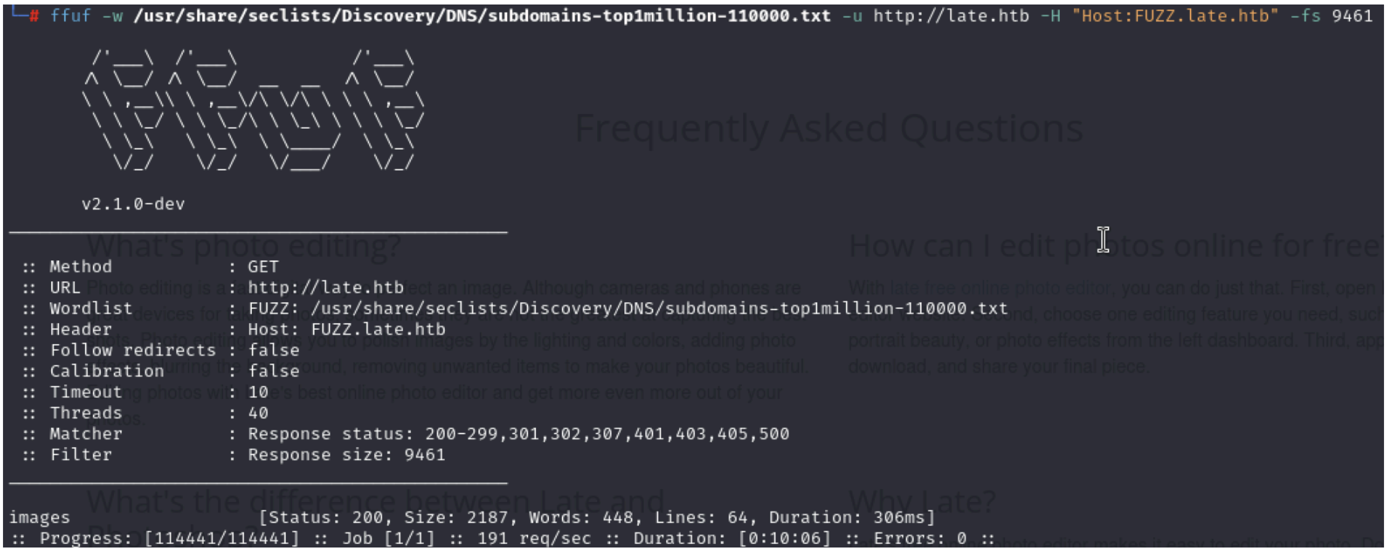
Late

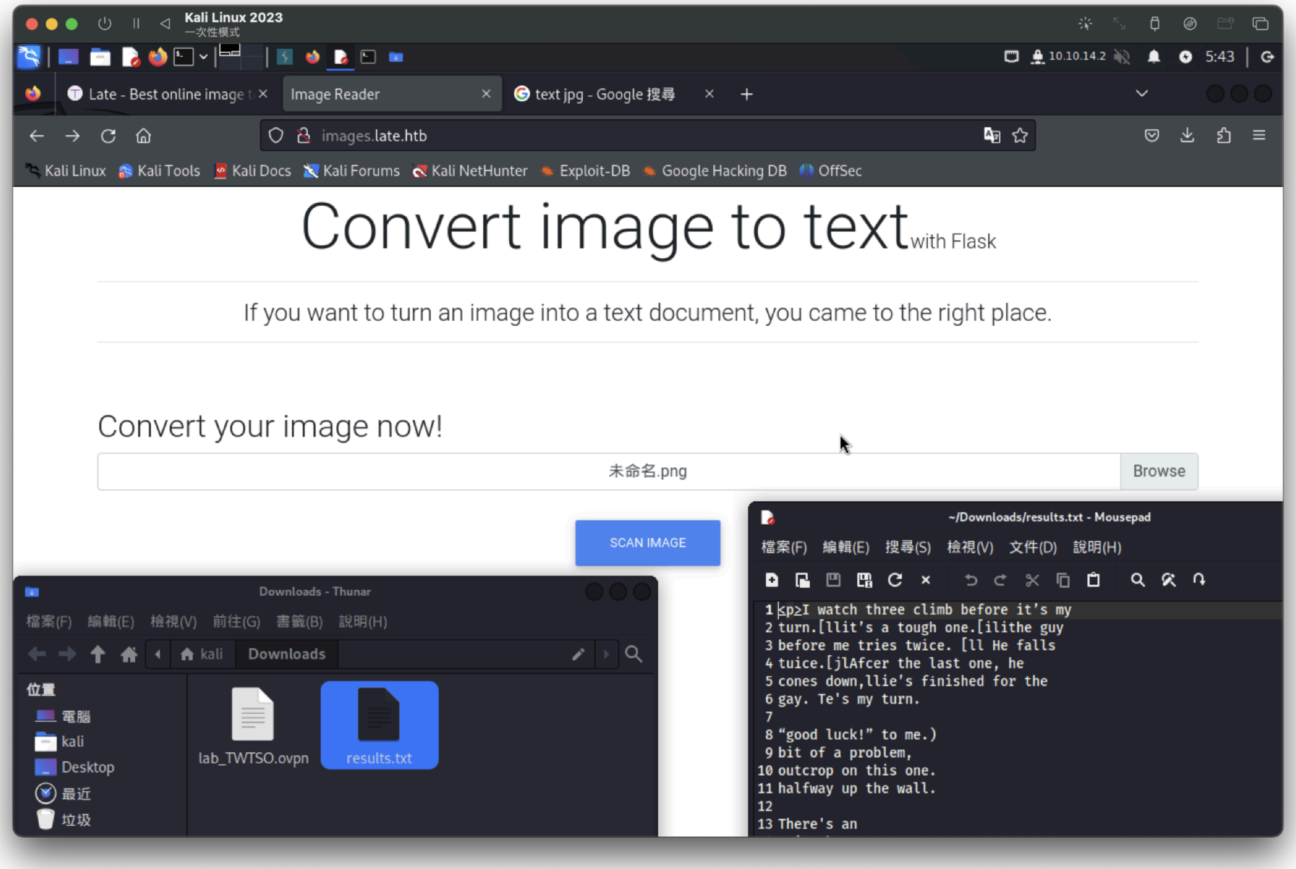
```
└─# nmap -sCV -p 22,80 -A 10.10.11.156
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 04:44 PDT
Nmap scan report for 10.10.11.156
Host is up (0.22s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 02:5e:29:0e:a3:af:4e:72:9d:a4:fe:0d:cb:5d:83:07 (RSA)
|   256 41:e1:fe:03:a5:c7:97:c4:d5:16:77:f3:41:0c:e9:fb (ECDSA)
|_  256 28:39:46:98:17:1e:46:1a:1e:a1:ab:3b:9a:57:70:48 (ED25519)
80/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Late - Best online image tools
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (96%), Linux 5.0 - 5.5 (96%), Linux 4.15 - 5.8 (95%), Linux 3.1 (95%), Linux 3.2 (95%), Linux 5.3 - 5.4 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), Linux 2.6.32 (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   267.38 ms 10.10.14.1
2   267.54 ms 10.10.11.156

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.81 seconds
```

一般目錄爆破無啥東西
找到vhost



```
└─# ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -u http://late.htb -H "Host:FUZZ.late.htb" -fs 9461

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://late.htb
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.late.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 9461
________________________________________________

images                  [Status: 200, Size: 2187, Words: 448, Lines: 64, Duration: 306ms]
:: Progress: [114441/114441] :: Job [1/1] :: 191 req/sec :: Duration: [0:10:06] :: Errors: 0 ::
```

上傳有文字圖片，會直接轉成文字



Convert image to text with Flask

If you want to turn an image into a text document, you came to the right place.

Convert your image now!

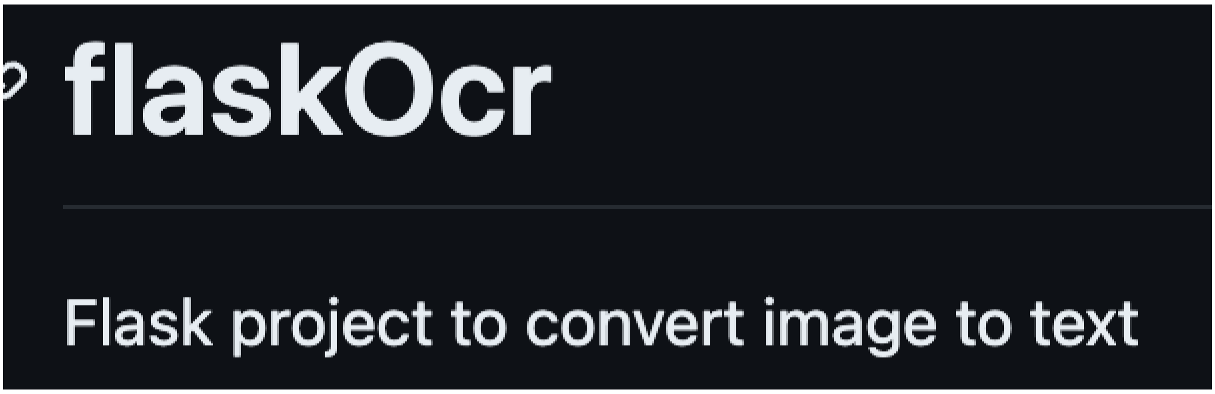
未命名.png | Browse

SCAN IMAGE

Downloads - Thunar
檔案(F) 編輯(E) 檢視(V) 前往(G) 書籤(B) 說明(H)
kali
Downloads
位置
電腦
kali
Desktop
最近
垃圾
lab_TWTSO.ovpn
results.txt
~/Downloads/results.txt - Mousepad
檔案(F) 編輯(E) 搜尋(S) 檢視(V) 文件(D) 說明(H)

```
<p>I watch three climb before it's my
turn.[llit's a tough one.[ilithe guy
before me tries twice. [ll He falls
tuice.[jlAfcer the last one, he
cones down,llie's finished for the
gay. Te's my turn.

"good luck!" to me.)
bit of a problem,
outcrop on this one.
halfway up the wall.

There's an
```

Convert image to textwith Flask
使用orc



flaskOcr

Flask project to convert image to text

Flask為python撰寫，可以嘗試SSTI攻擊