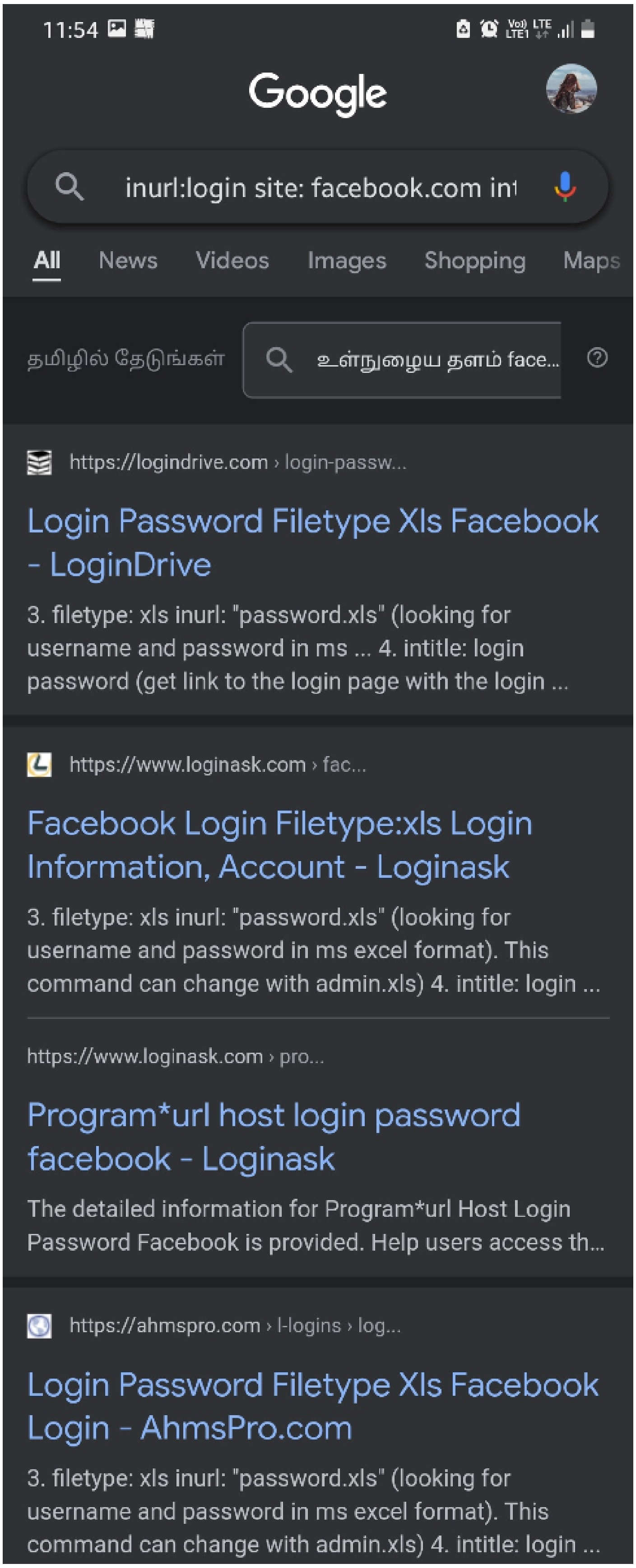
Day 2 assignment

INFORMATION GATHERING:

1.Google dorking:



11:54

Google

inurl:login site: facebook.com int

All News Videos Images Shopping Maps

தமிழில் தேடுங்கள் உள்நுழைய தளம் face...

https://logindrive.com › login-passw...

Login Password Filetype Xls Facebook - LoginDrive

3. filetype: xls inurl: "password.xls" (looking for username and password in ms ... 4. intitle: login password (get link to the login page with the login ...

https://www.loginask.com › fac...

Facebook Login Filetype:xls Login Information, Account - Loginask

3. filetype: xls inurl: "password.xls" (looking for username and password in ms excel format). This command can change with admin.xls) 4. intitle: login ...

https://www.loginask.com › pro...

Program*url host login password facebook - Loginask

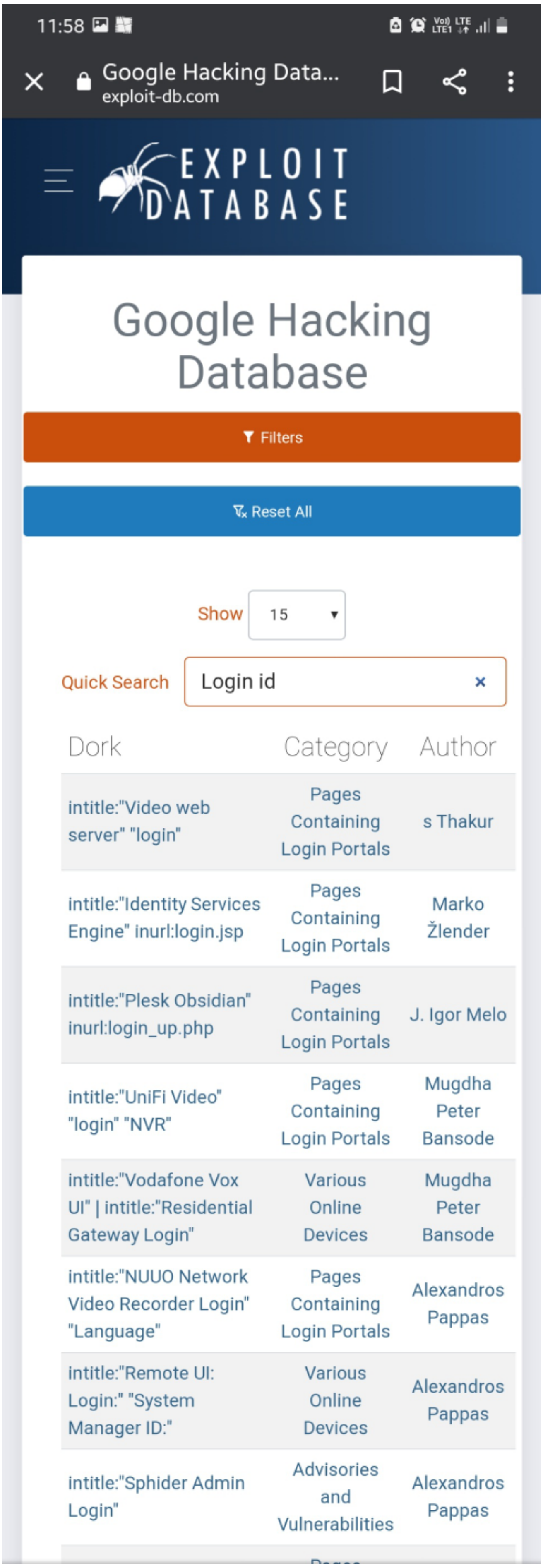
The detailed information for Program*url Host Login Password Facebook is provided. Help users access th...

https://ahmspro.com › l-logins › log...

Login Password Filetype Xls Facebook Login - AhmsPro.com

3. filetype: xls inurl: "password.xls" (looking for username and password in ms excel format). This command can change with admin.xls) 4. intitle: login ...

2.google hacking database :



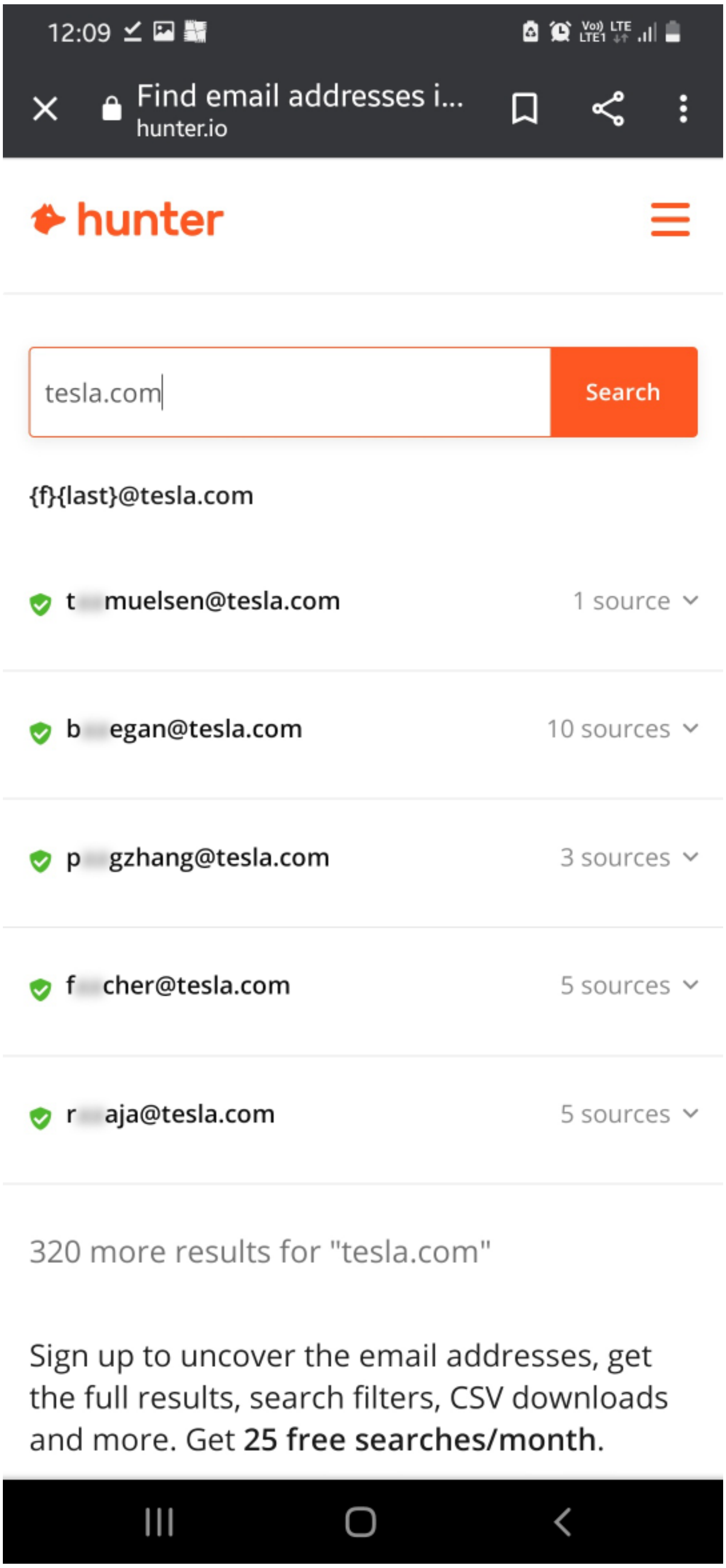
Google Hacking Database

Show 15

Quick Search Login id

Dork	Category	Author
intitle:"Video web server" "login"	Pages Containing Login Portals	s Thakur
intitle:"Identity Services Engine" inurl:login.jsp	Pages Containing Login Portals	Marko Žlender
intitle:"Plesk Obsidian" inurl:login_up.php	Pages Containing Login Portals	J. Igor Melo
intitle:"UniFi Video" "login" "NVR"	Pages Containing Login Portals	Mugdha Peter Bansode
intitle:"Vodafone Vox UI" | intitle:"Residential Gateway Login"	Various Online Devices	Mugdha Peter Bansode
intitle:"NUUO Network Video Recorder Login" "Language"	Pages Containing Login Portals	Alexandros Pappas
intitle:"Remote UI: Login:" "System Manager ID:"	Various Online Devices	Alexandros Pappas
intitle:"Sphider Admin Login"	Advisories and Vulnerabilities	Alexandros Pappas

3.finding emails using hunter.io :



{f}{last}@tesla.com

t[redacted]muelsen@tesla.com 1 source

b[redacted]egan@tesla.com 10 sources

p[redacted]gzhang@tesla.com 3 sources

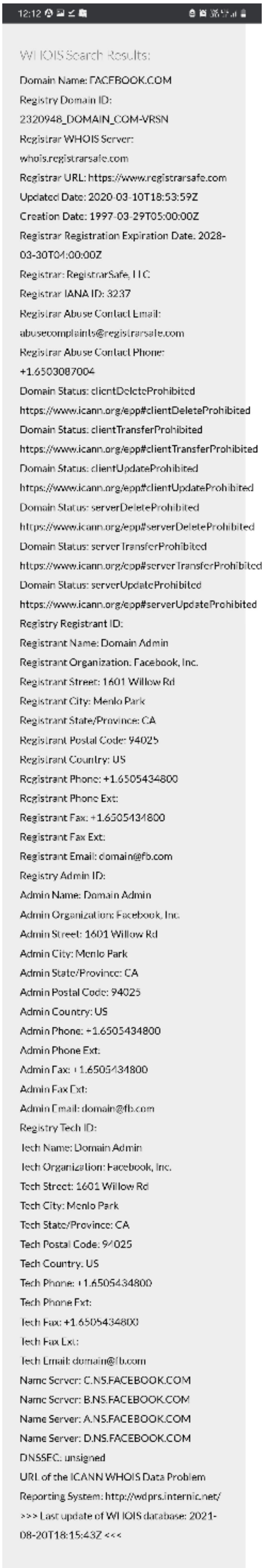
f[redacted]cher@tesla.com 5 sources

r[redacted]aja@tesla.com 5 sources

320 more results for "tesla.com"

Sign up to uncover the email addresses, get the full results, search filters, CSV downloads and more. Get **25 free searches/month**.

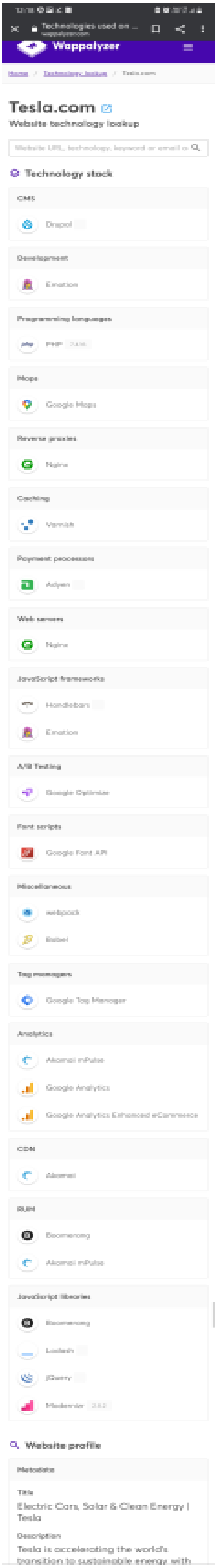
4.who is lookup :



WHOIS Search Results:

```
Domain Name: FACEBOOK.COM
Registry Domain ID:
2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server:
whois.registrarsafe.com
Registrar URL: https://www.registrarsafe.com
Updated Date: 2020-03-10T18:53:59Z
Creation Date: 1997-03-29T05:00:00Z
Registrar Registration Expiration Date: 2028-
03-30T04:00:00Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email:
abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone:
+1.6503087004
Domain Status: clientDeleteProhibited
https://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited
https://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited
https://www.icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited
https://www.icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited
https://www.icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited
https://www.icann.org/epp#serverUpdateProhibited
Registry Registrant ID:
Registrant Name: Domain Admin
Registrant Organization: Facebook, Inc.
Registrant Street: 1601 Willow Rd
Registrant City: Menlo Park
Registrant State/Province: CA
Registrant Postal Code: 94025
Registrant Country: US
Registrant Phone: +1.6505434800
Registrant Phone Ext:
Registrant Fax: +1.6505434800
Registrant Fax Ext:
Registrant Email: domain@fb.com
Registry Admin ID:
Admin Name: Domain Admin
Admin Organization: Facebook, Inc.
Admin Street: 1601 Willow Rd
Admin City: Menlo Park
Admin State/Province: CA
Admin Postal Code: 94025
Admin Country: US
Admin Phone: +1.6505434800
Admin Phone Ext:
Admin Fax: +1.6505434800
Admin Fax Ext:
Admin Email: domain@fb.com
Registry Tech ID:
Tech Name: Domain Admin
Tech Organization: Facebook, Inc.
Tech Street: 1601 Willow Rd
Tech City: Menlo Park
Tech State/Province: CA
Tech Postal Code: 94025
Tech Country: US
Tech Phone: +1.6505434800
Tech Phone Ext:
Tech Fax: +1.6505434800
Tech Fax Ext:
Tech Email: domain@fb.com
Name Server: C.NS.FACEBOOK.COM
Name Server: B.NS.FACEBOOK.COM
Name Server: A.NS.FACEBOOK.COM
Name Server: D.NS.FACEBOOK.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem
Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2021-
08-20T18:15:43Z <<<
```

5. Website technology using wappalyzer:



Home / Technology lookup / Tesla.com

Tesla.com

Website technology lookup

Technology stack

CMS

- Drupal

Development

- Emotion

Programming languages

- PHP 7.4.16

Maps

- Google Maps

Reverse proxies

- Nginx

Caching

- Varnish

Payment processors

- Adyen

Web servers

- Nginx

JavaScript frameworks

- Handlebars
- Emotion

A/B Testing

- Google Optimize

Font scripts

- Google Font API

Miscellaneous

- webpack
- Babel

Tag managers

- Google Tag Manager

Analytics

- Akamai mPulse
- Google Analytics
- Google Analytics Enhanced eCommerce

CDN

- Akamai

RUM

- Boomerang
- Akamai mPulse

JavaScript libraries

- Boomerang
- Lodash
- jQuery
- Modernizr 2.6.2

Website profile

Metadata

Title

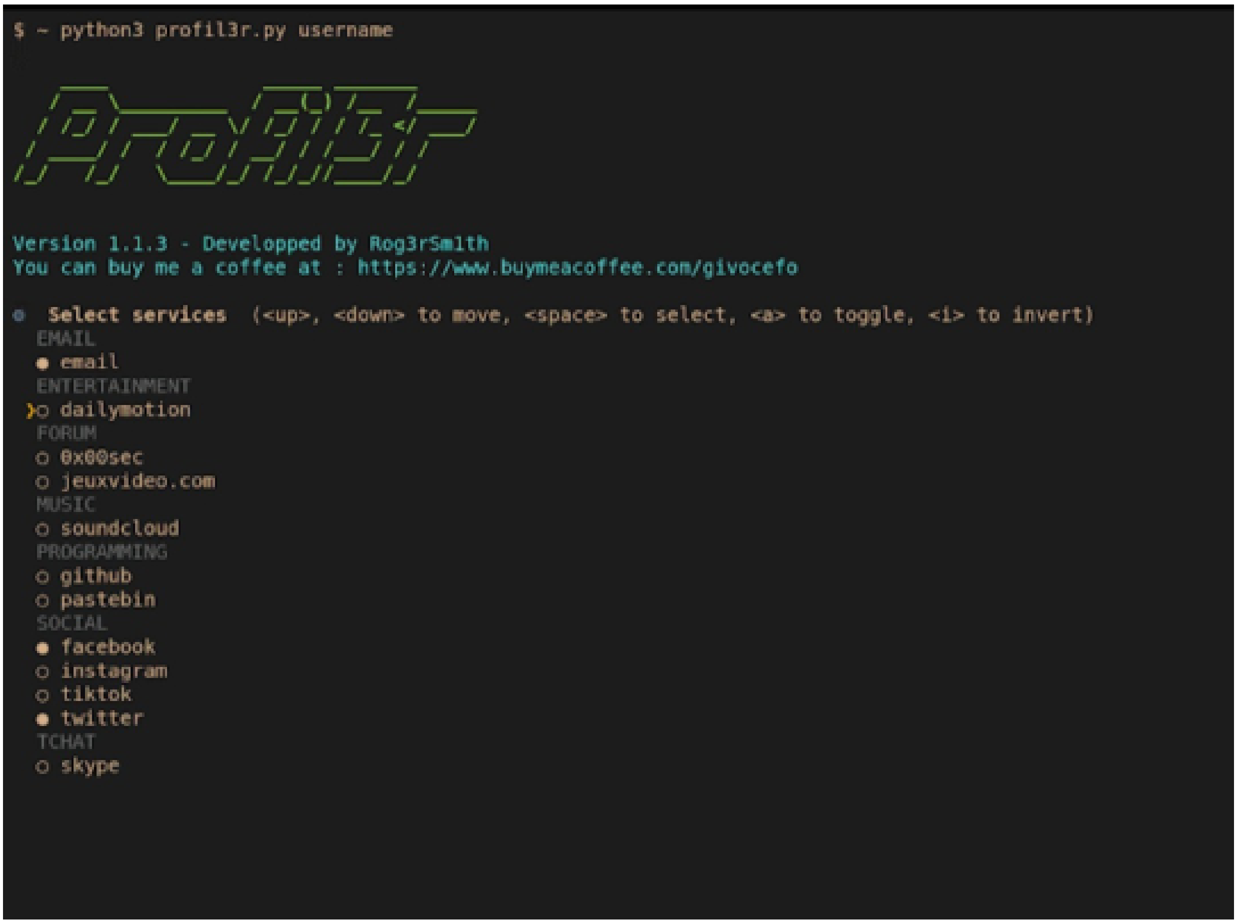
Electric Cars, Solar & Clean Energy | Tesla

Description

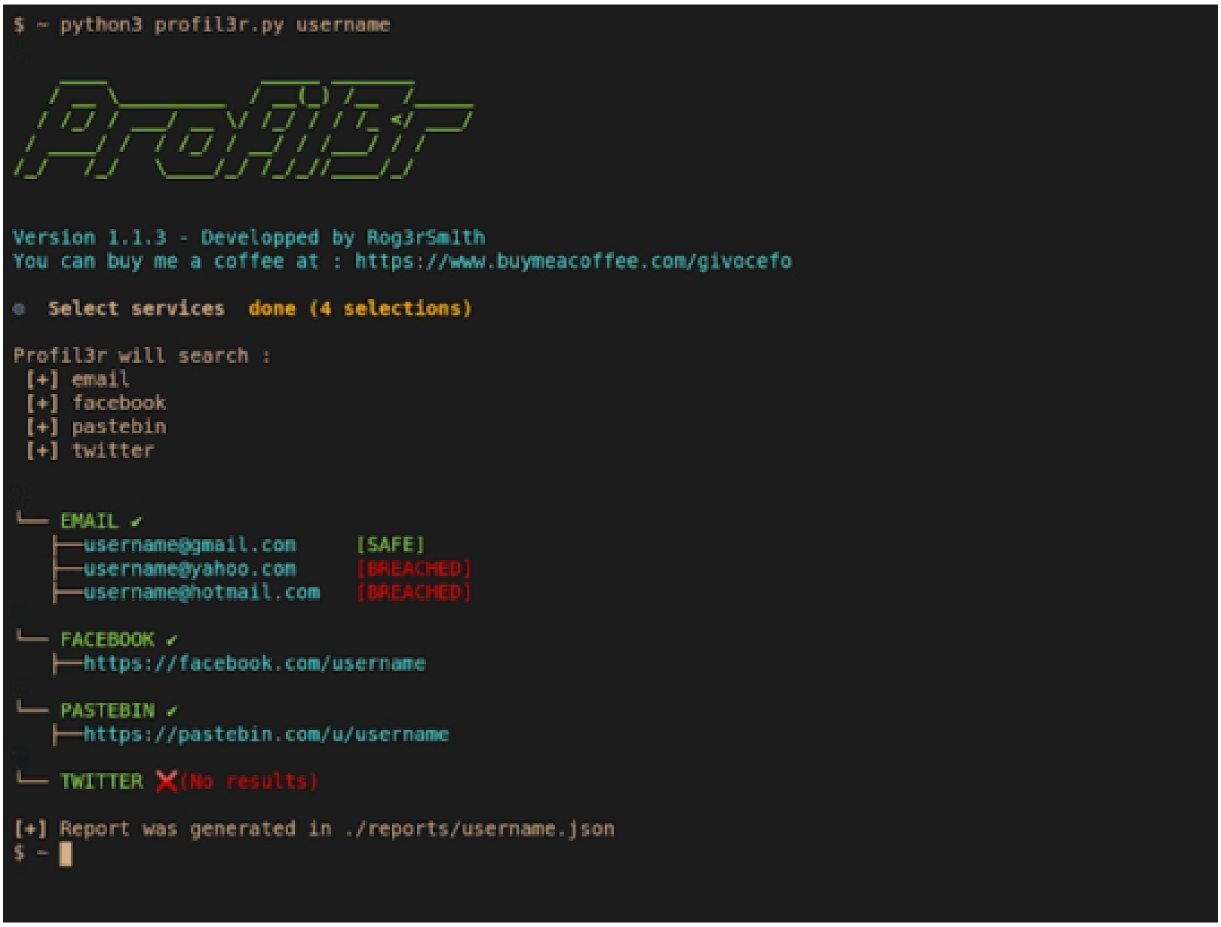
Tesla is accelerating the world's transition to sustainable energy with

6. Profil3r :

Example:



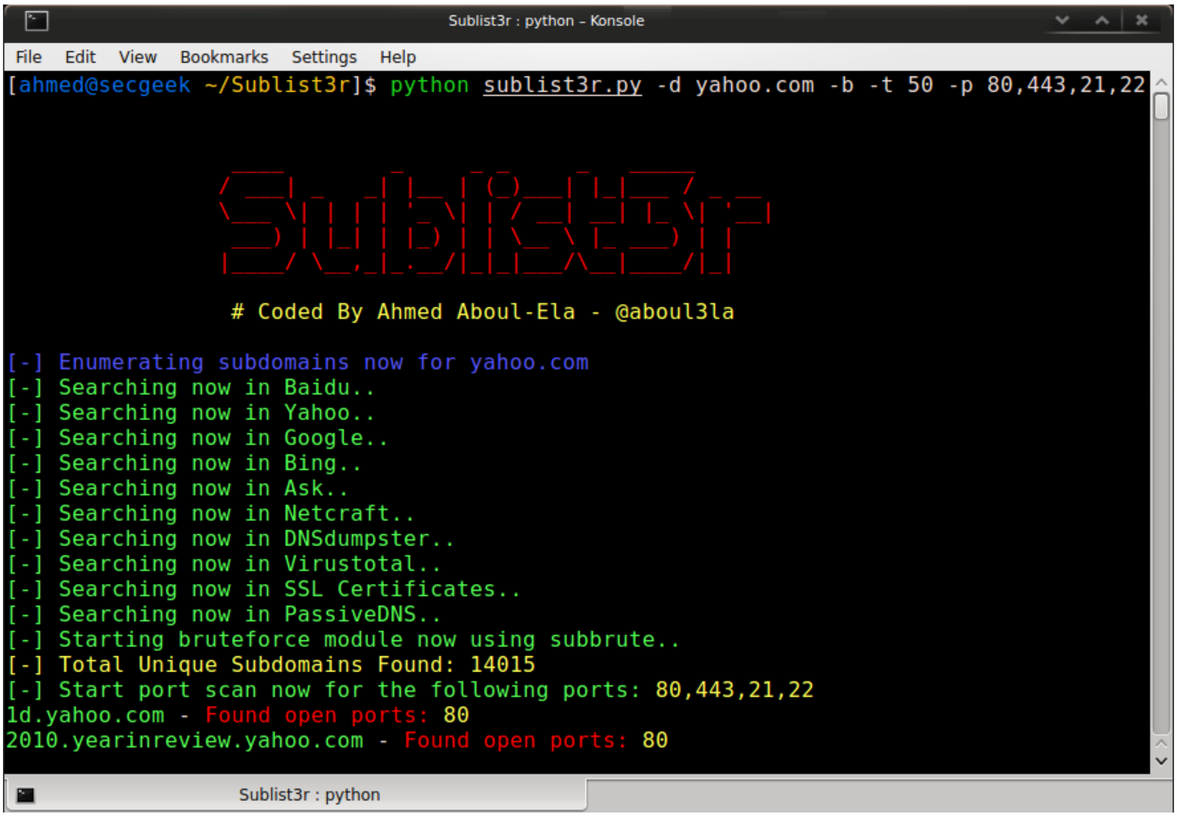
```
$ ~ python3 profil3r.py username

Version 1.1.3 - Developped by Rog3rSm1th
You can buy me a coffee at : https://www.buymeacoffee.com/givocefo

  Select services  (<up>, <down> to move, <space> to select, <a> to toggle, <i> to invert)
   EMAIL
   ● email
   ENTERTAINMENT
  ❯○ dailymotion
   FORUM
   ○ 0x00sec
   ○ jeuxvideo.com
   MUSIC
   ○ soundcloud
   PROGRAMMING
   ○ github
   ○ pastebin
   SOCIAL
   ● facebook
   ○ instagram
   ○ tiktok
   ● twitter
   TCHAT
   ○ skype
```



```
$ ~ python3 profil3r.py username

Version 1.1.3 - Developped by Rog3rSm1th
You can buy me a coffee at : https://www.buymeacoffee.com/givocefo

●  Select services  done (4 selections)

Profil3r will search :
  [+] email
  [+] facebook
  [+] pastebin
  [+] twitter


└── EMAIL ✓
    ├──username@gmail.com      [SAFE]
    ├──username@yahoo.com      [BREACHED]
    ├──username@hotmail.com    [BREACHED]

└── FACEBOOK ✓
    ├──https://facebook.com/username

└── PASTEBIN ✓
    ├──https://pastebin.com/u/username

└── TWITTER ✗(No results)

[+] Report was generated in ./reports/username.json
$ ~ █
```

7.sublis3r :

Example:

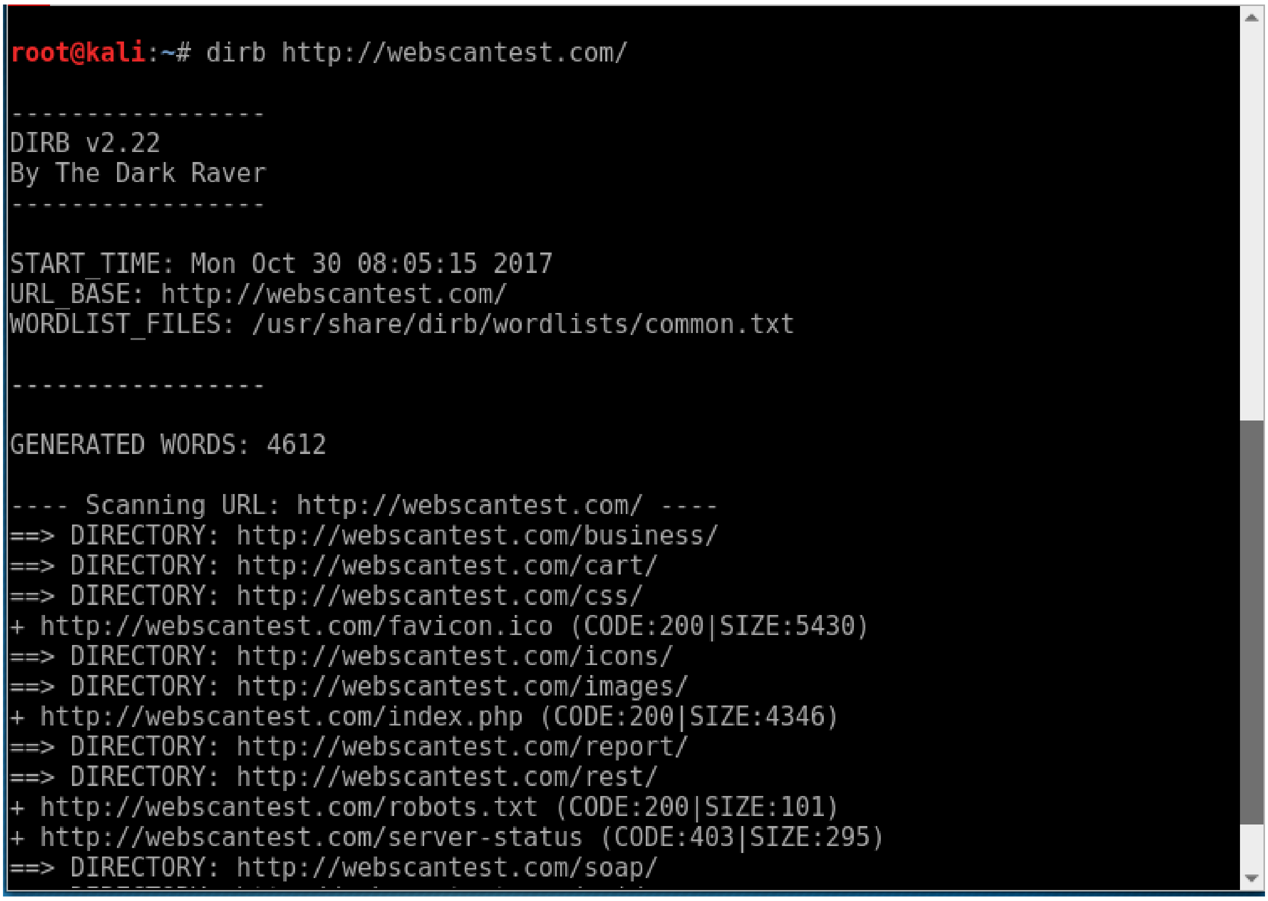


```
[ahmed@secgeek ~/Sublist3r]$ python sublist3r.py -d yahoo.com -b -t 50 -p 80,443,21,22

                  # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for yahoo.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Starting bruteforce module now using subbrute..
[-] Total Unique Subdomains Found: 14015
[-] Start port scan now for the following ports: 80,443,21,22
1d.yahoo.com - Found open ports: 80
2010.yearinreview.yahoo.com - Found open ports: 80
```

SCANNING :

1.dirb : (looking for files)

Example:



```
root@kali:~# dirb http://webscantest.com/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Oct 30 08:05:15 2017
URL_BASE: http://webscantest.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://webscantest.com/ ----
==> DIRECTORY: http://webscantest.com/business/
==> DIRECTORY: http://webscantest.com/cart/
==> DIRECTORY: http://webscantest.com/css/
+ http://webscantest.com/favicon.ico (CODE:200|SIZE:5430)
==> DIRECTORY: http://webscantest.com/icons/
==> DIRECTORY: http://webscantest.com/images/
+ http://webscantest.com/index.php (CODE:200|SIZE:4346)
==> DIRECTORY: http://webscantest.com/report/
==> DIRECTORY: http://webscantest.com/rest/
+ http://webscantest.com/robots.txt (CODE:200|SIZE:101)
+ http://webscantest.com/server-status (CODE:403|SIZE:295)
==> DIRECTORY: http://webscantest.com/soap/
```