$ whoami

Armado Reniery Rodas

Ing. Informática / MSc GTI

Consultor en Seg. Inf.

ITIL v4 – C)PTE – C)PEH – ISO 27k

OWASP Chapter Leader - San Pedro Sula

Disclaimer

WARNING! Toda la información incluida en este medio tiene fines educativos y profesionales, en ningún caso OWASP, ni yo somos responsables del mal uso de esta información.

OSINT

Técnicas de Reconocimiento en un Test de Intrusión

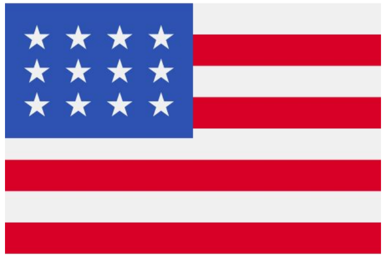
Objetivos

- ❑ Conocer sobre la investigación en fuentes abiertas (OSINT).
- ❑ Mostrar la importancia del uso de OSINT durante la etapa de Reconocimiento, en una Prueba de Intrusión.
- ❑ Demostrar cómo realizar Reconocimiento de nuestro objetivo, haciendo uso de OSINT.

¿Te has preguntado qué tan grande es Internet?

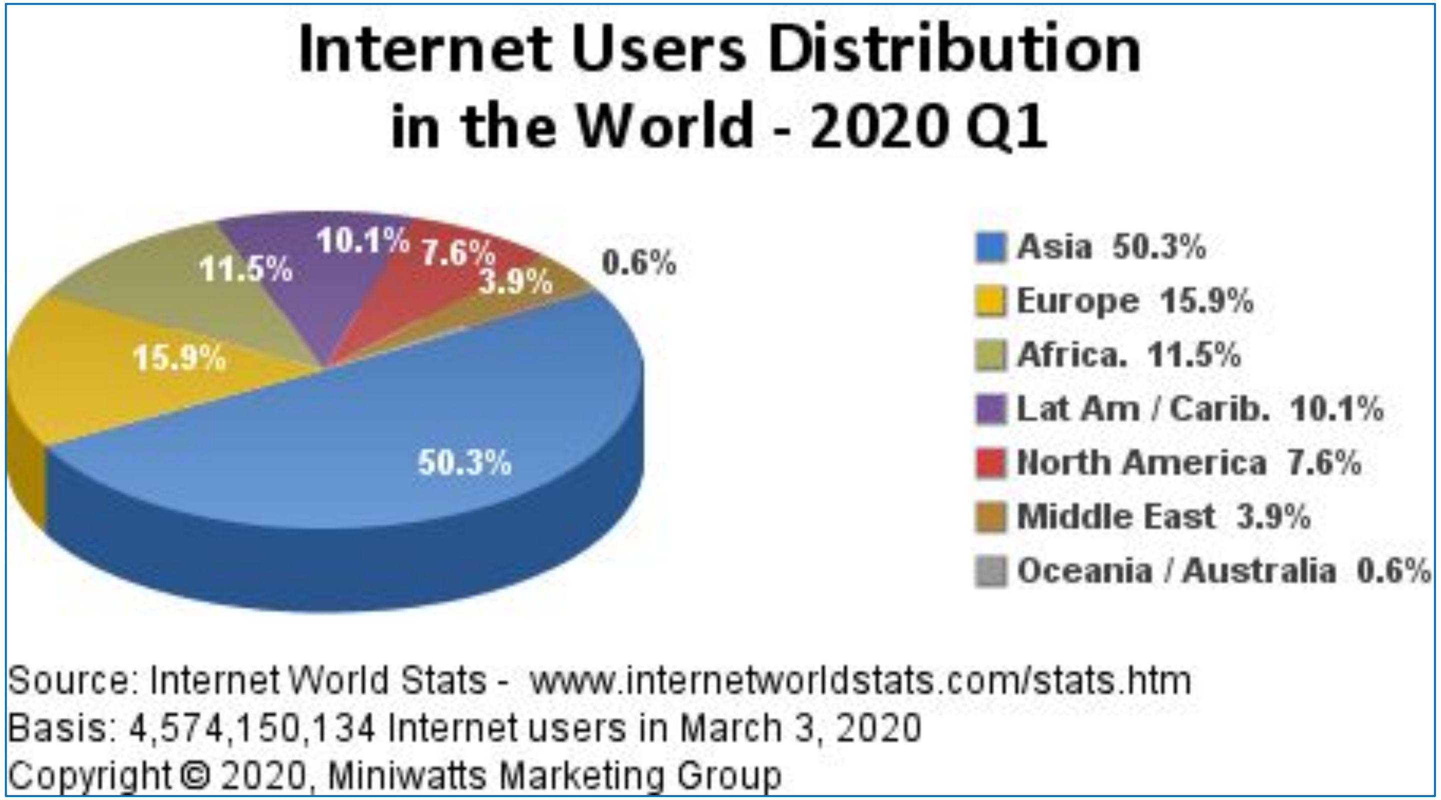
Y… ¿Qué tan expuesta está tu información?

Un poco de historia…



- ❑ 1969
- ❑ ARPANET

Estadística…



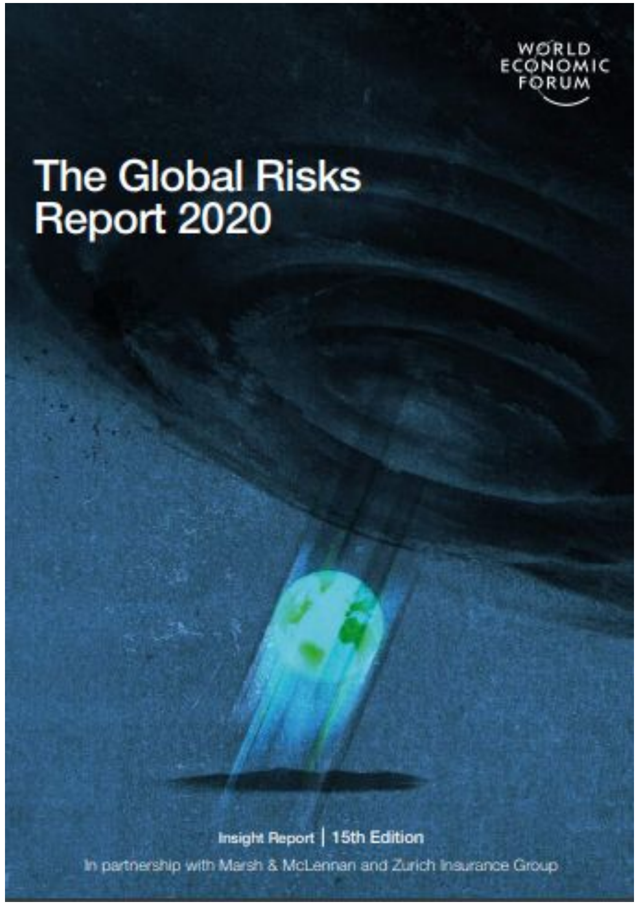
Internet Users Distribution in the World - 2020 Q1

Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 4,574,150,134 Internet users in March 3, 2020
Copyright © 2020, Miniwatts Marketing Group

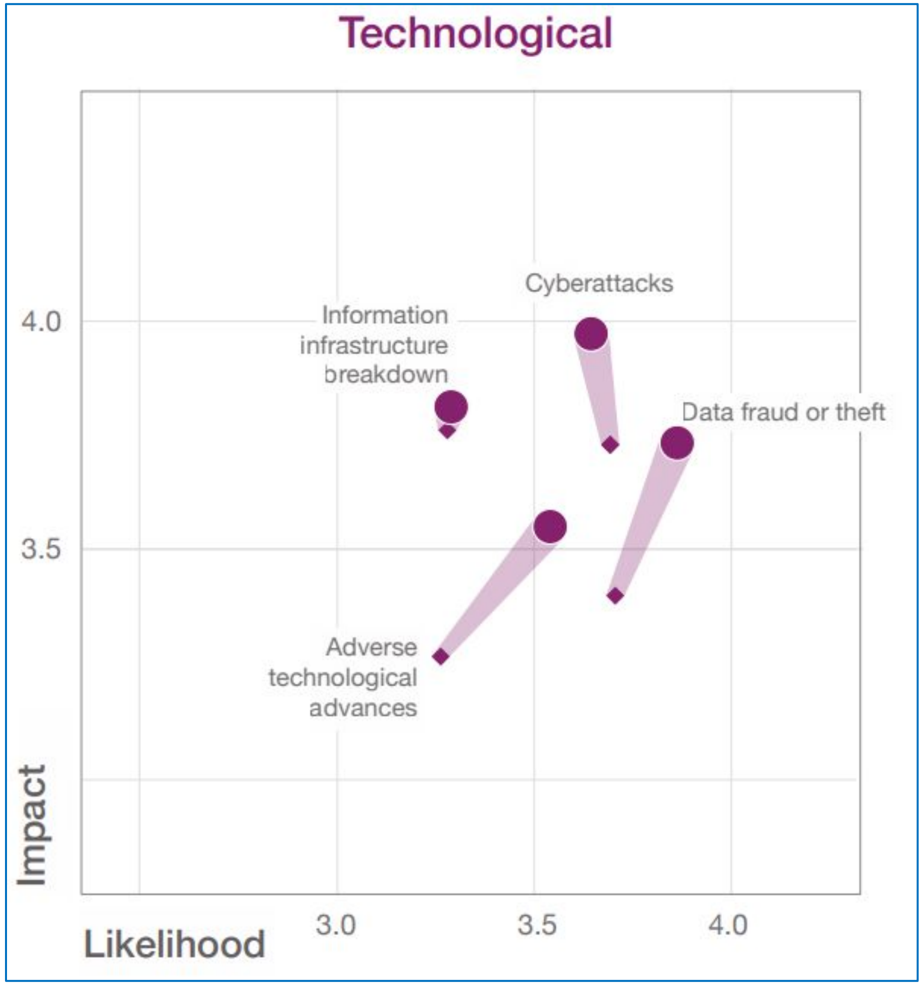
Fuente: Internet World Stats

- □ 4,574,150,134

¿Qué hay de los Riesgos?

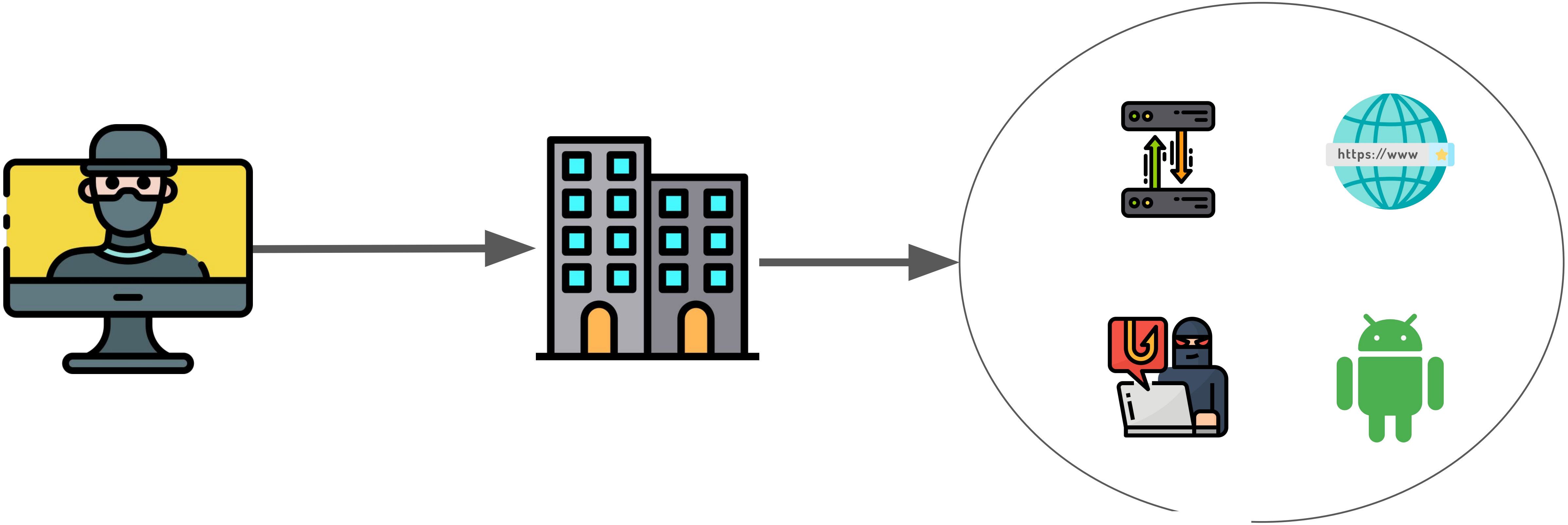

WORLD ECONOMIC FORUM
The Global Risks Report 2020
Insight Report | 15th Edition
In partnership with Marsh & McLennan and Zurich Insurance Group

Fuente: World Economic Forum



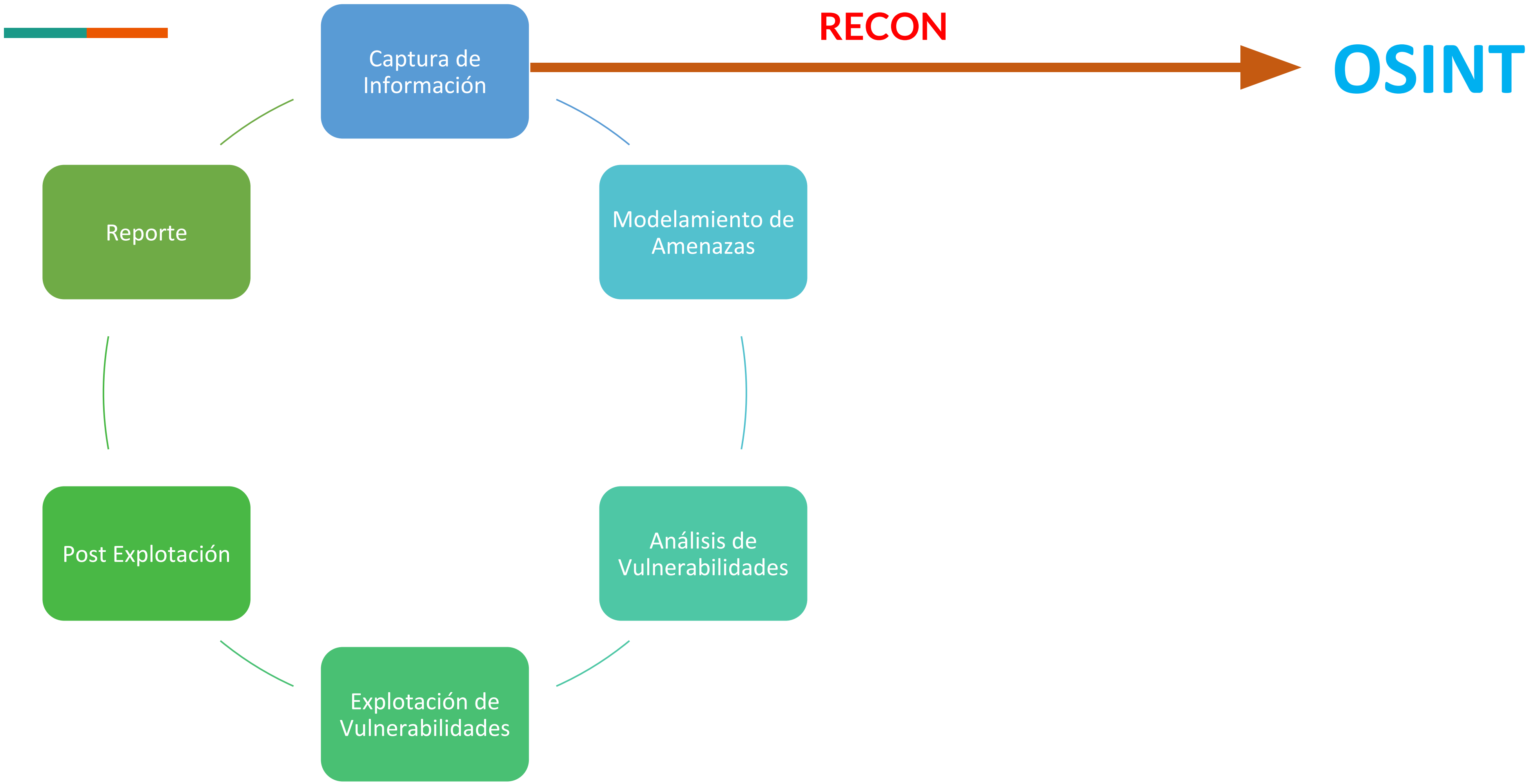
Test de Intrusión

hackerone

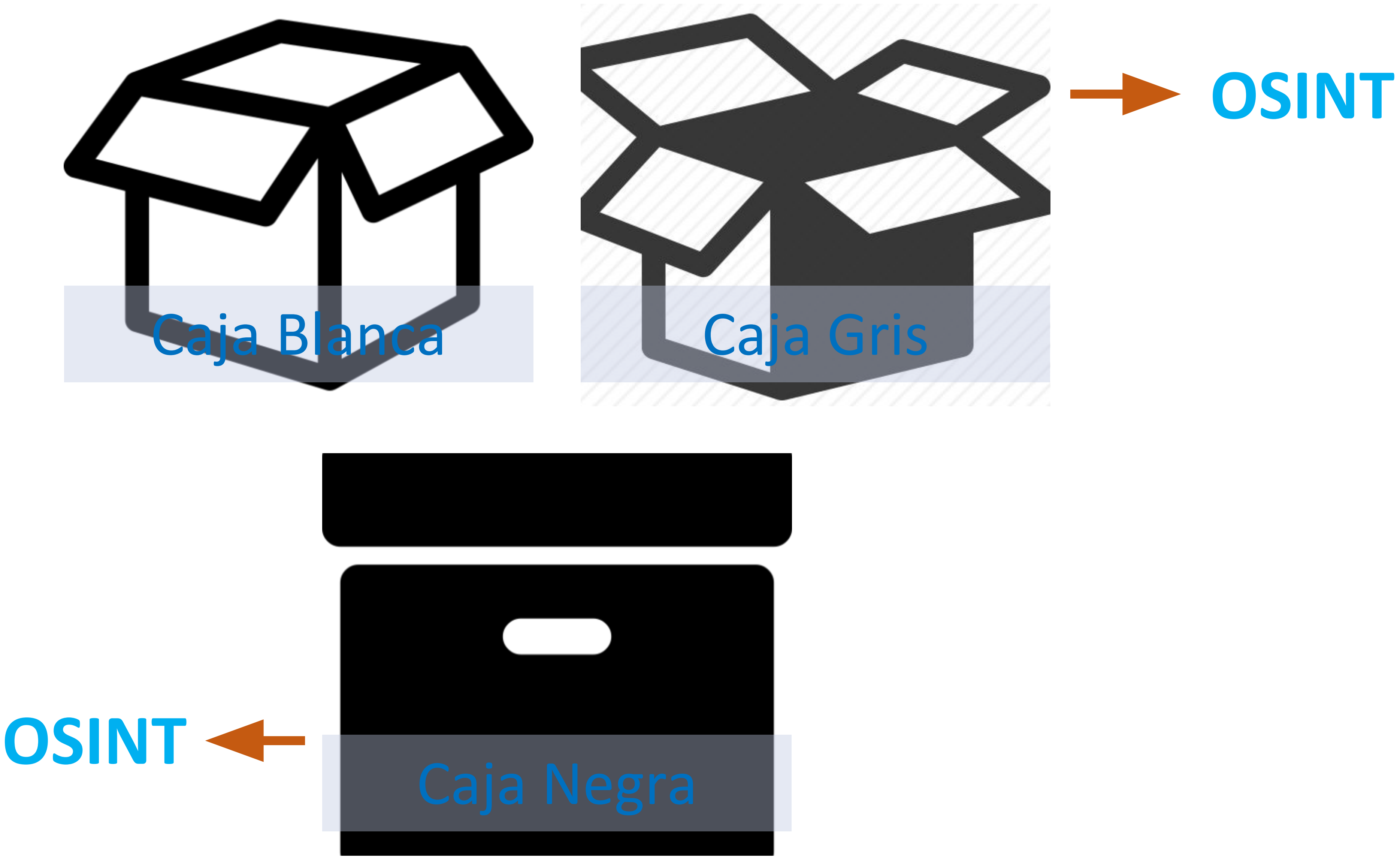


bugcrowd

Fases


Captura de Información
Modelamiento de Amenazas
Análisis de Vulnerabilidades
Explotación de Vulnerabilidades
Post Explotación
Reporte
RECON
OSINT

Tipos



Caja Blanca

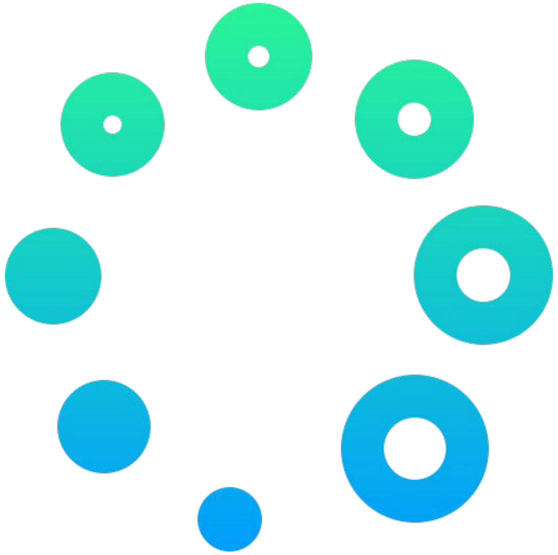
Caja Gris

OSINT

Caja Negra

OSINT

Pero…¿Qué es OSINT? 🙄



OSINT (Open Source Intelligence)

Sistema para recopilar información de **fuentes abiertas**.

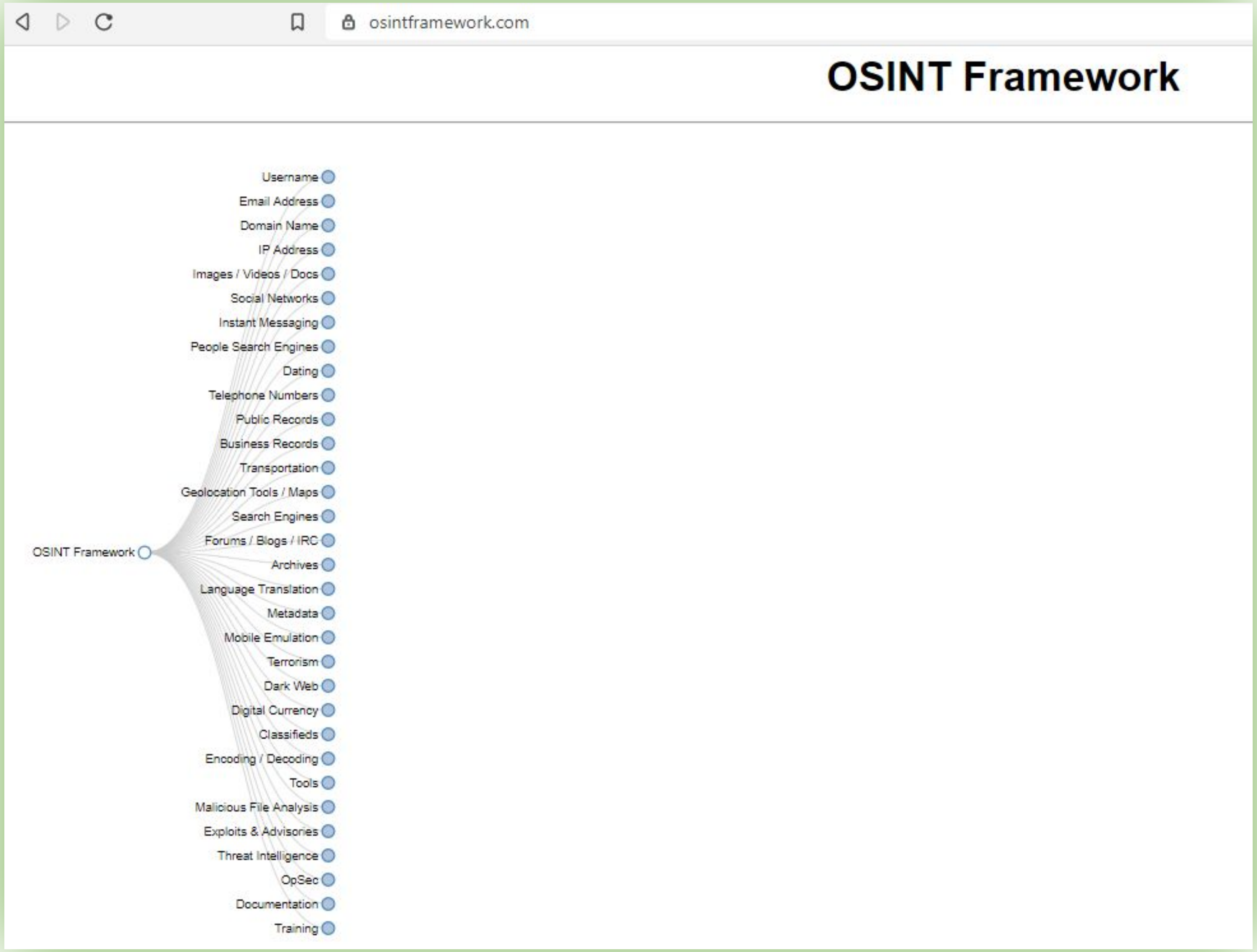
Fuentes abiertas: Cualquier vía de la que podamos obtener datos y que sea accesible y pública.

Fuente: **https://ciberpatrulla.com/osint-framework/**

hunter
censys
SHODAN
in
Google
crt.sh
bing
View
Uploads
Info
Stats
Tools
WIGLE.NET
All the networks. Found by Everyone.
ZoomEye
Yandex

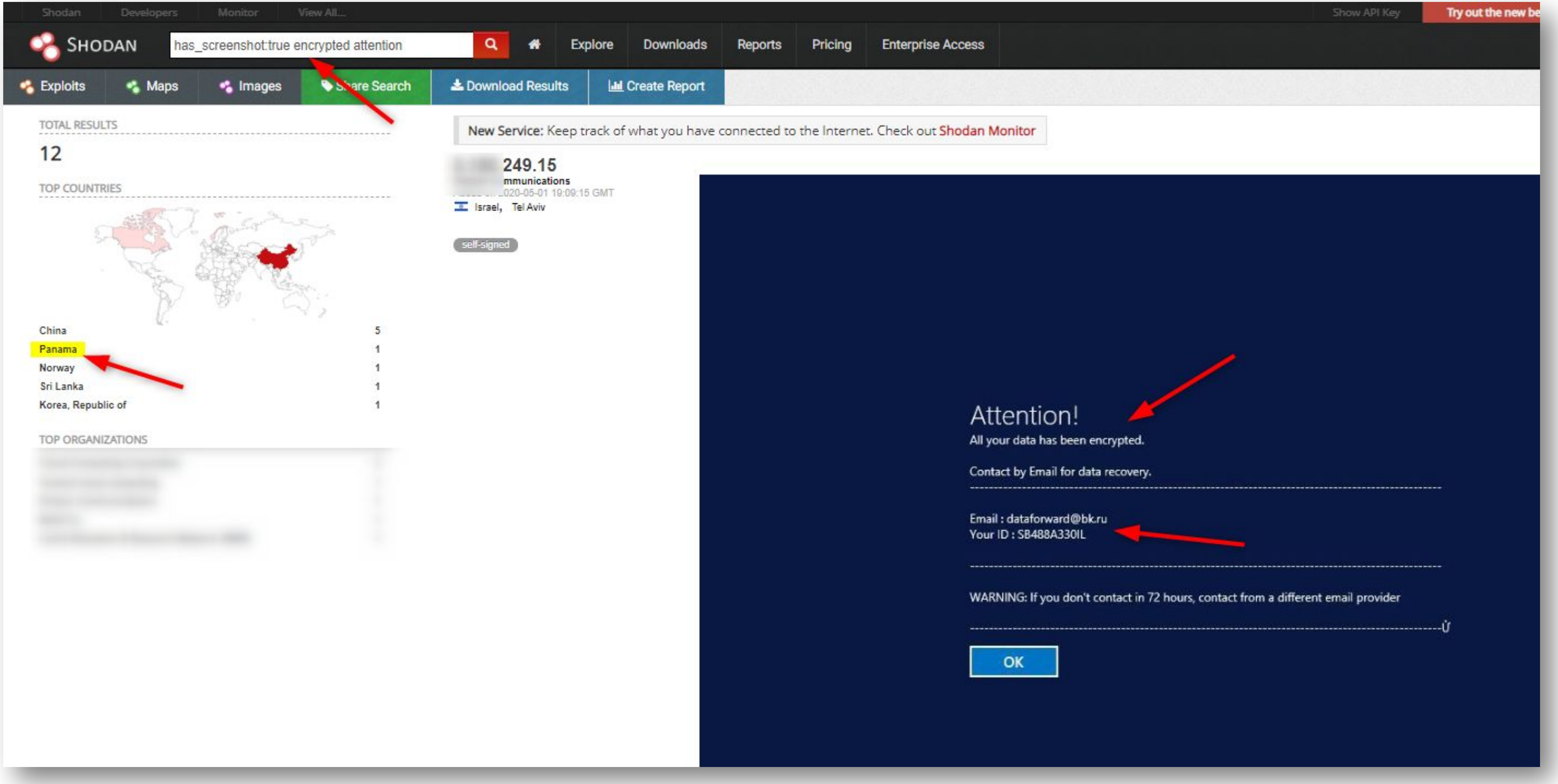
Importancia de OSINT

Información Pública o Gratuita en Internet



Fuente: https://osintframework.com/

Un pequeño ejemplo...



has_screenshot:true encrypted attention

TOTAL RESULTS

12

TOP COUNTRIES

China	5
Panama	1
Norway	1
Sri Lanka	1
Korea, Republic of	1

TOP ORGANIZATIONS

[redacted]

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

[redacted]249.15
[redacted]mmunications
[redacted]2020-05-01 19:09:15 GMT
Israel, Tel Aviv

Attention!
All your data has been encrypted.

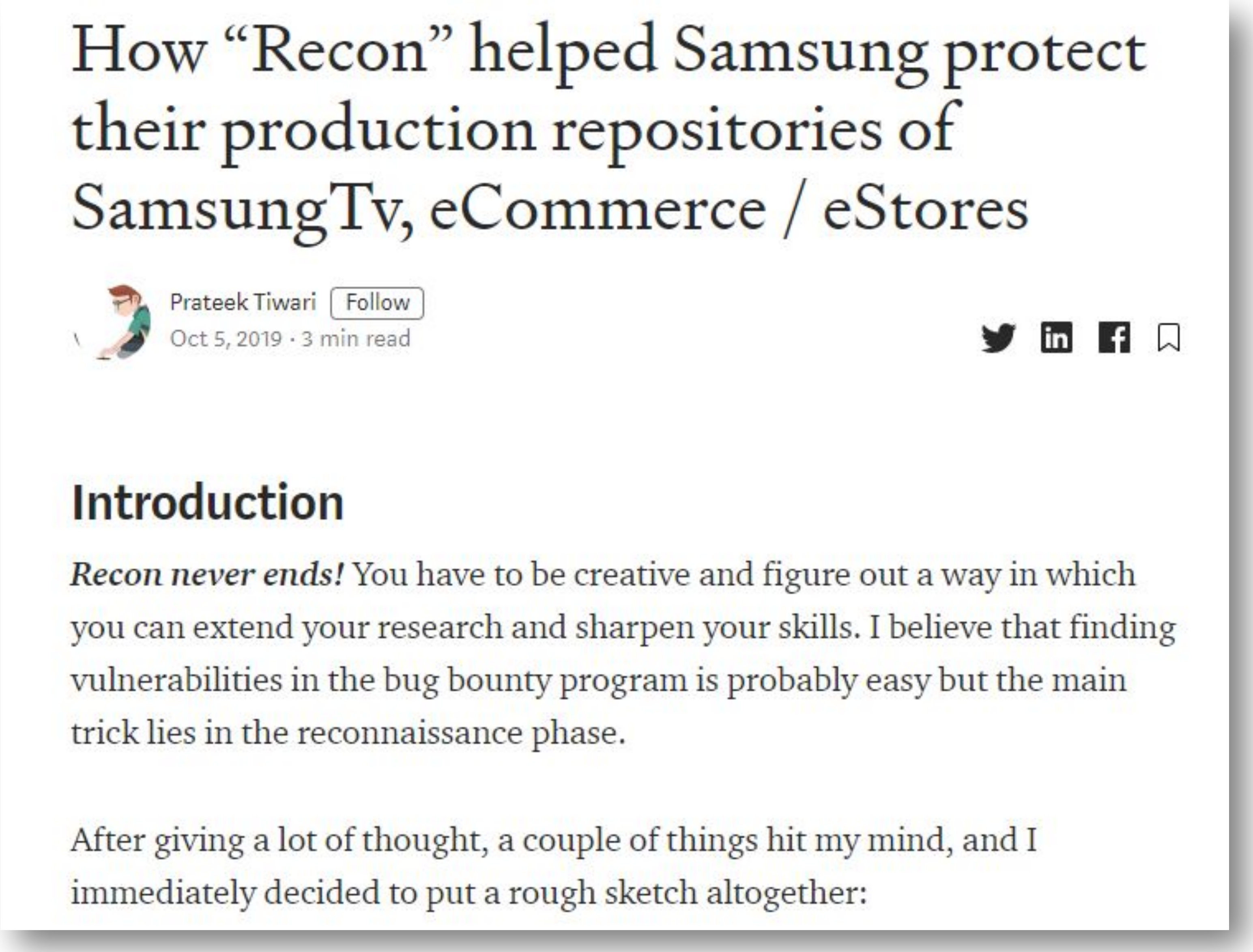
Contact by Email for data recovery.

Email : dataforward@bk.ru
Your ID : SB488A330IL

WARNING: If you don't contact in 72 hours, contact from a different email provider

Otro pequeño ejemplo...

Fuente: https://blog.usejournal.com/how-recon-helped-samsung-protect-their-production-repositories-of-samsungtv-ecommerce-estores-4c51d6ec4fdd



How "Recon" helped Samsung protect their production repositories of SamsungTv, eCommerce / eStores

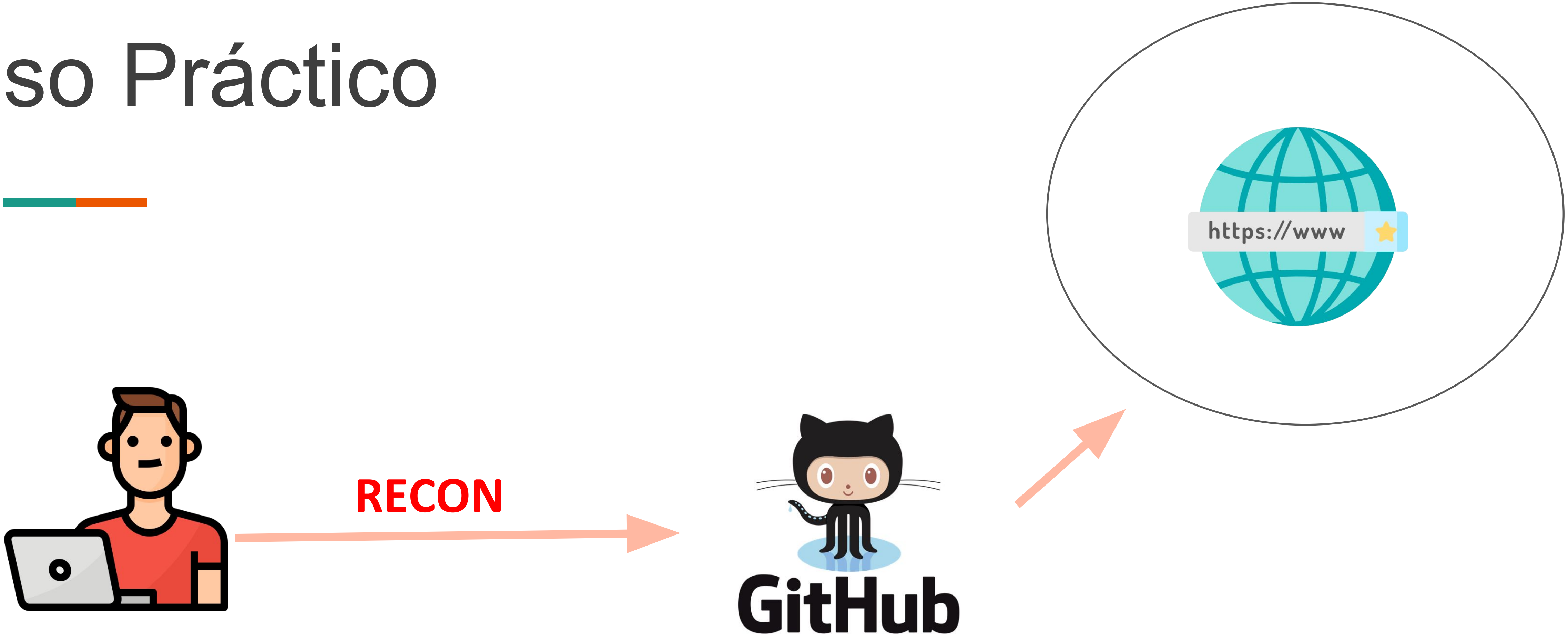
Prateek Tiwari Follow
Oct 5, 2019 · 3 min read

Introduction

Recon never ends! You have to be creative and figure out a way in which you can extend your research and sharpen your skills. I believe that finding vulnerabilities in the bug bounty program is probably easy but the main trick lies in the reconnaissance phase.

After giving a lot of thought, a couple of things hit my mind, and I immediately decided to put a rough sketch altogether:

Caso Práctico

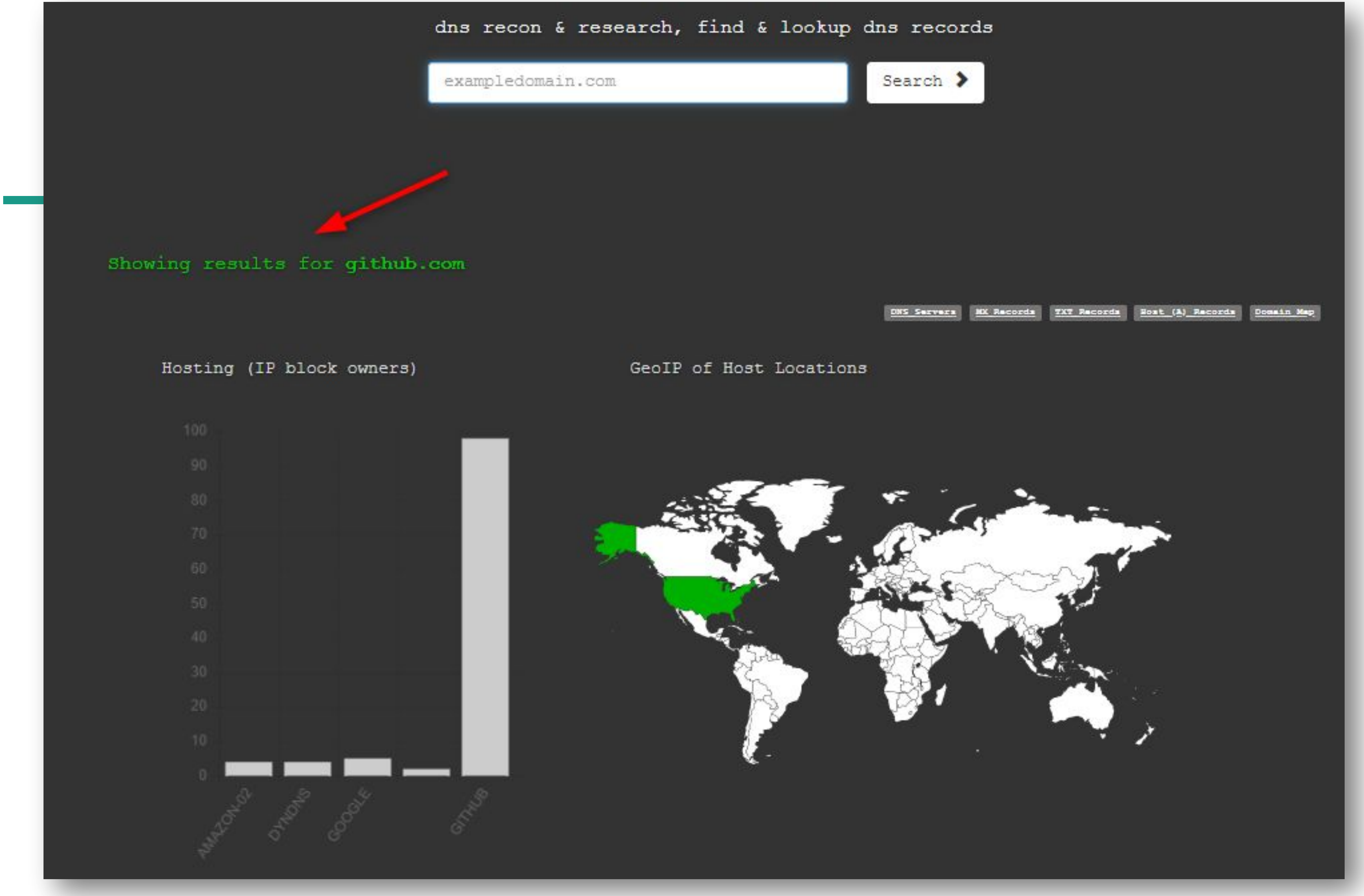


Target: https://github.com/

Objetivo: *Subdominios y Direcciones IP*

Tools

- ❑ https://dnsdumpster.com/
- ❑ https://crt.sh/
- ❑ Google Dorks (Google Hacking)
- ❑ https://rapiddns.io/
- ❑ https://censys.io/

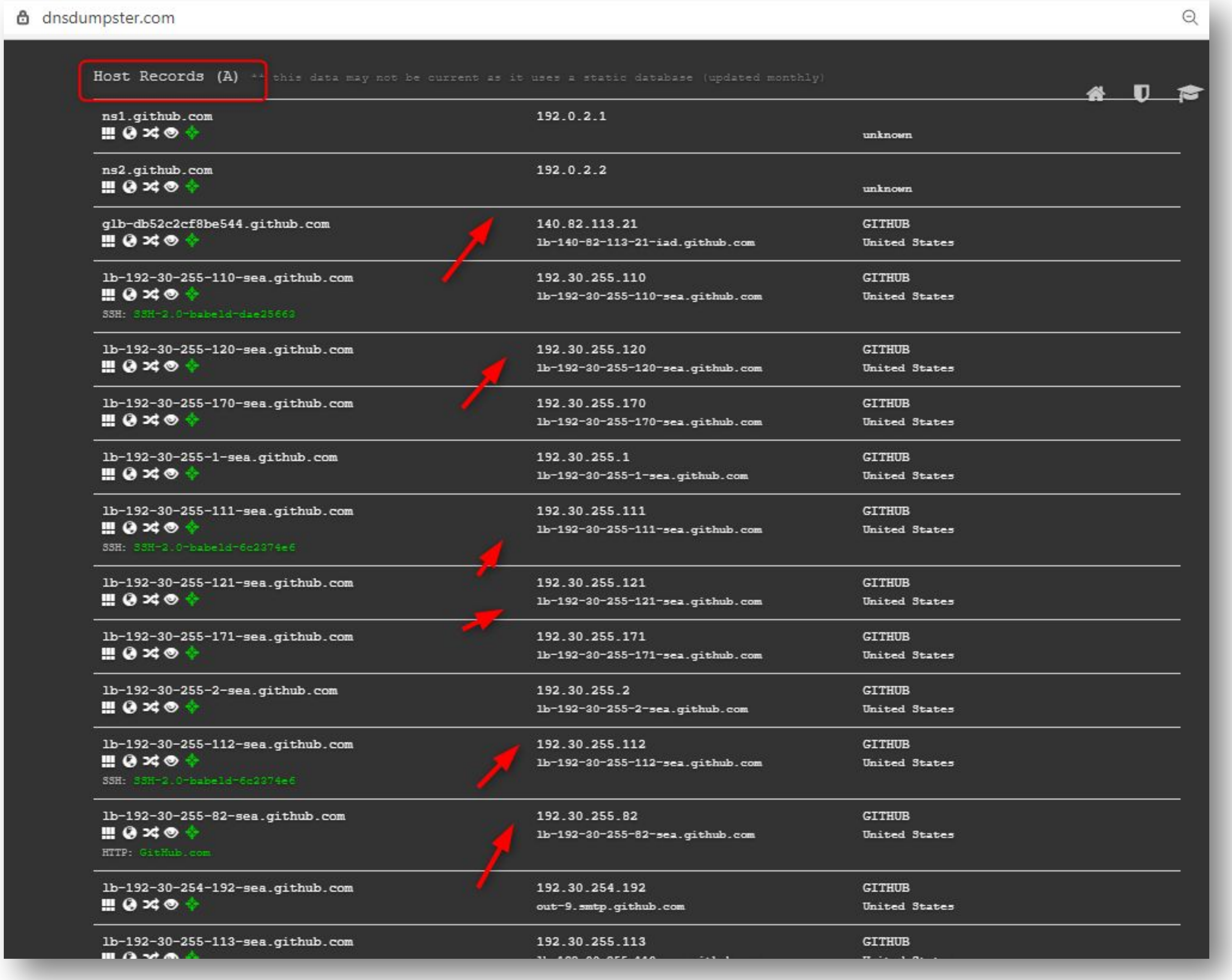


dns recon & research, find & lookup dns records

Showing results for github.com

Hosting (IP block owners)

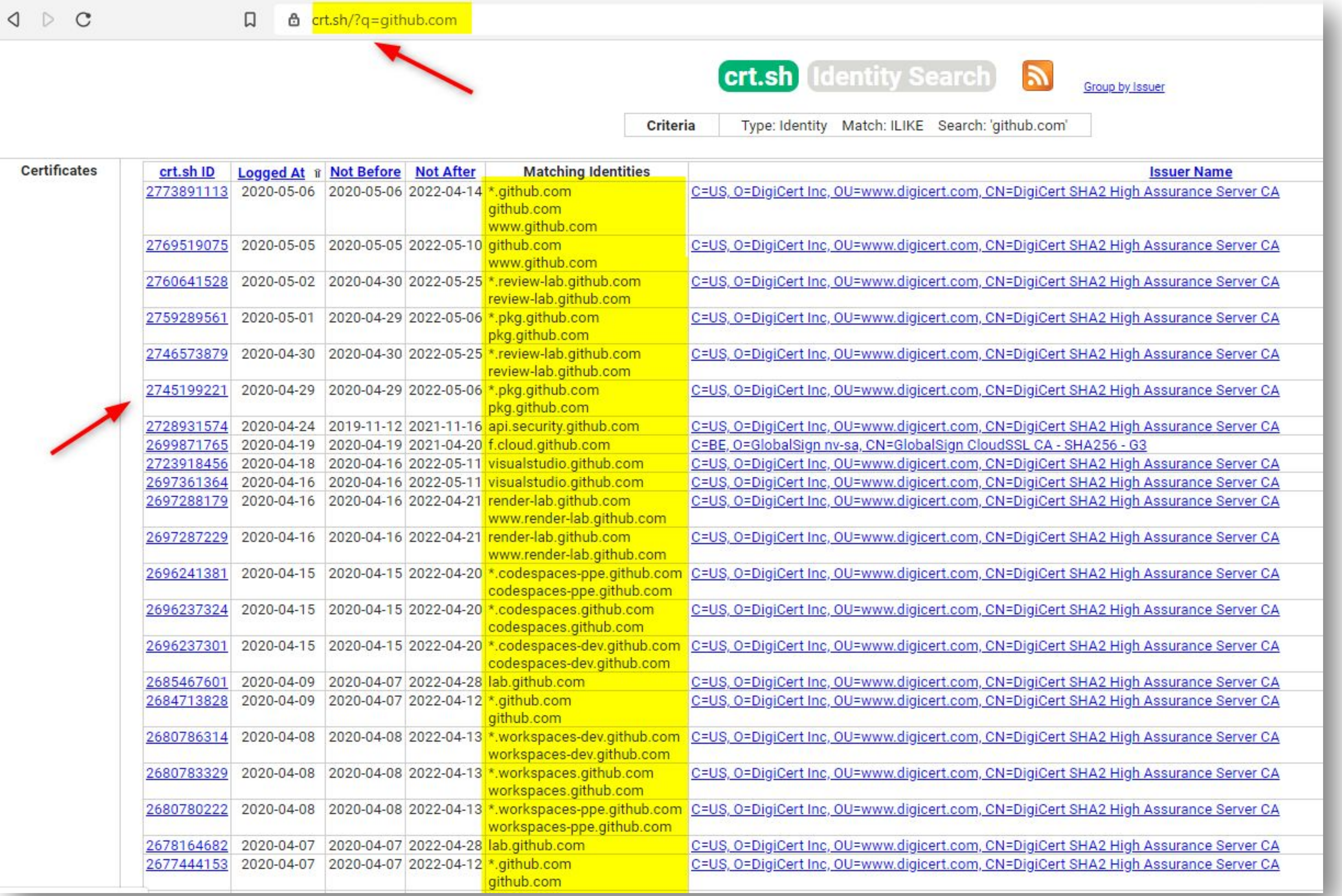
GeoIP of Host Locations



dnsdumpster.com

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

ns1.github.com	192.0.2.1	unknown
ns2.github.com	192.0.2.2	unknown
glb-db52c2cf8be544.github.com	140.82.113.21 lb-140-82-113-21-iad.github.com	GITHUB United States
lb-192-30-255-110-sea.github.com SSH: SSH-2.0-babeld-dae25663	192.30.255.110 lb-192-30-255-110-sea.github.com	GITHUB United States
lb-192-30-255-120-sea.github.com	192.30.255.120 lb-192-30-255-120-sea.github.com	GITHUB United States
lb-192-30-255-170-sea.github.com	192.30.255.170 lb-192-30-255-170-sea.github.com	GITHUB United States
lb-192-30-255-1-sea.github.com	192.30.255.1 lb-192-30-255-1-sea.github.com	GITHUB United States
lb-192-30-255-111-sea.github.com SSH: SSH-2.0-babeld-6c2374e6	192.30.255.111 lb-192-30-255-111-sea.github.com	GITHUB United States
lb-192-30-255-121-sea.github.com	192.30.255.121 lb-192-30-255-121-sea.github.com	GITHUB United States
lb-192-30-255-171-sea.github.com	192.30.255.171 lb-192-30-255-171-sea.github.com	GITHUB United States
lb-192-30-255-2-sea.github.com	192.30.255.2 lb-192-30-255-2-sea.github.com	GITHUB United States
lb-192-30-255-112-sea.github.com SSH: SSH-2.0-babeld-6c2374e6	192.30.255.112 lb-192-30-255-112-sea.github.com	GITHUB United States
lb-192-30-255-82-sea.github.com HTTP: GitHub.com	192.30.255.82 lb-192-30-255-82-sea.github.com	GITHUB United States
lb-192-30-254-192-sea.github.com	192.30.254.192 out-9.smtp.github.com	GITHUB United States
lb-192-30-255-113-sea.github.com	192.30.255.113	GITHUB

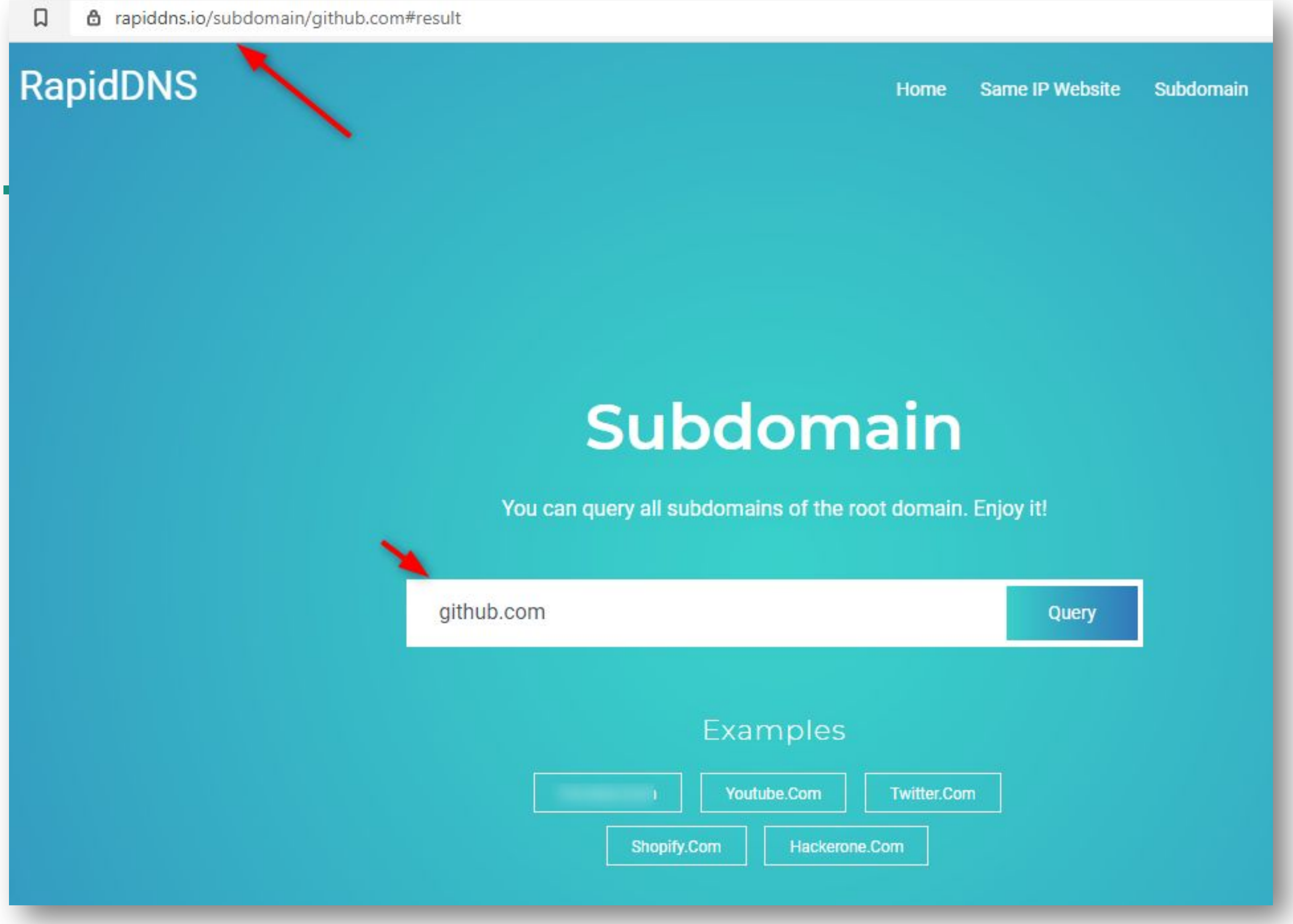


crt.sh/?q=github.com

Criteria Type: Identity Match: ILIKE Search: 'github.com'

Certificates

crt.sh ID	Logged At ⇑	Not Before	Not After	Matching Identities	Issuer Name
2773891113	2020-05-06	2020-05-06	2022-04-14	*.github.com github.com www.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2769519075	2020-05-05	2020-05-05	2022-05-10	github.com www.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2760641528	2020-05-02	2020-04-30	2022-05-25	*.review-lab.github.com review-lab.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2759289561	2020-05-01	2020-04-29	2022-05-06	*.pkg.github.com pkg.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2746573879	2020-04-30	2020-04-30	2022-05-25	*.review-lab.github.com review-lab.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2745199221	2020-04-29	2020-04-29	2022-05-06	*.pkg.github.com pkg.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2728931574	2020-04-24	2019-11-12	2021-11-16	api.security.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2699871765	2020-04-19	2020-04-19	2021-04-20	f.cloud.github.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
2723918456	2020-04-18	2020-04-16	2022-05-11	visualstudio.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2697361364	2020-04-16	2020-04-16	2022-05-11	visualstudio.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2697288179	2020-04-16	2020-04-16	2022-04-21	render-lab.github.com www.render-lab.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2697287229	2020-04-16	2020-04-16	2022-04-21	render-lab.github.com www.render-lab.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2696241381	2020-04-15	2020-04-15	2022-04-20	*.codespaces-ppe.github.com codespaces-ppe.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2696237324	2020-04-15	2020-04-15	2022-04-20	*.codespaces.github.com codespaces.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2696237301	2020-04-15	2020-04-15	2022-04-20	*.codespaces-dev.github.com codespaces-dev.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2685467601	2020-04-09	2020-04-07	2022-04-28	lab.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2684713828	2020-04-09	2020-04-07	2022-04-12	*.github.com github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2680786314	2020-04-08	2020-04-08	2022-04-13	*.workspaces-dev.github.com workspaces-dev.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2680783329	2020-04-08	2020-04-08	2022-04-13	*.workspaces.github.com workspaces.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2680780222	2020-04-08	2020-04-08	2022-04-13	*.workspaces-ppe.github.com workspaces-ppe.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2678164682	2020-04-07	2020-04-07	2022-04-28	lab.github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2677444153	2020-04-07	2020-04-07	2022-04-12	*.github.com github.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA



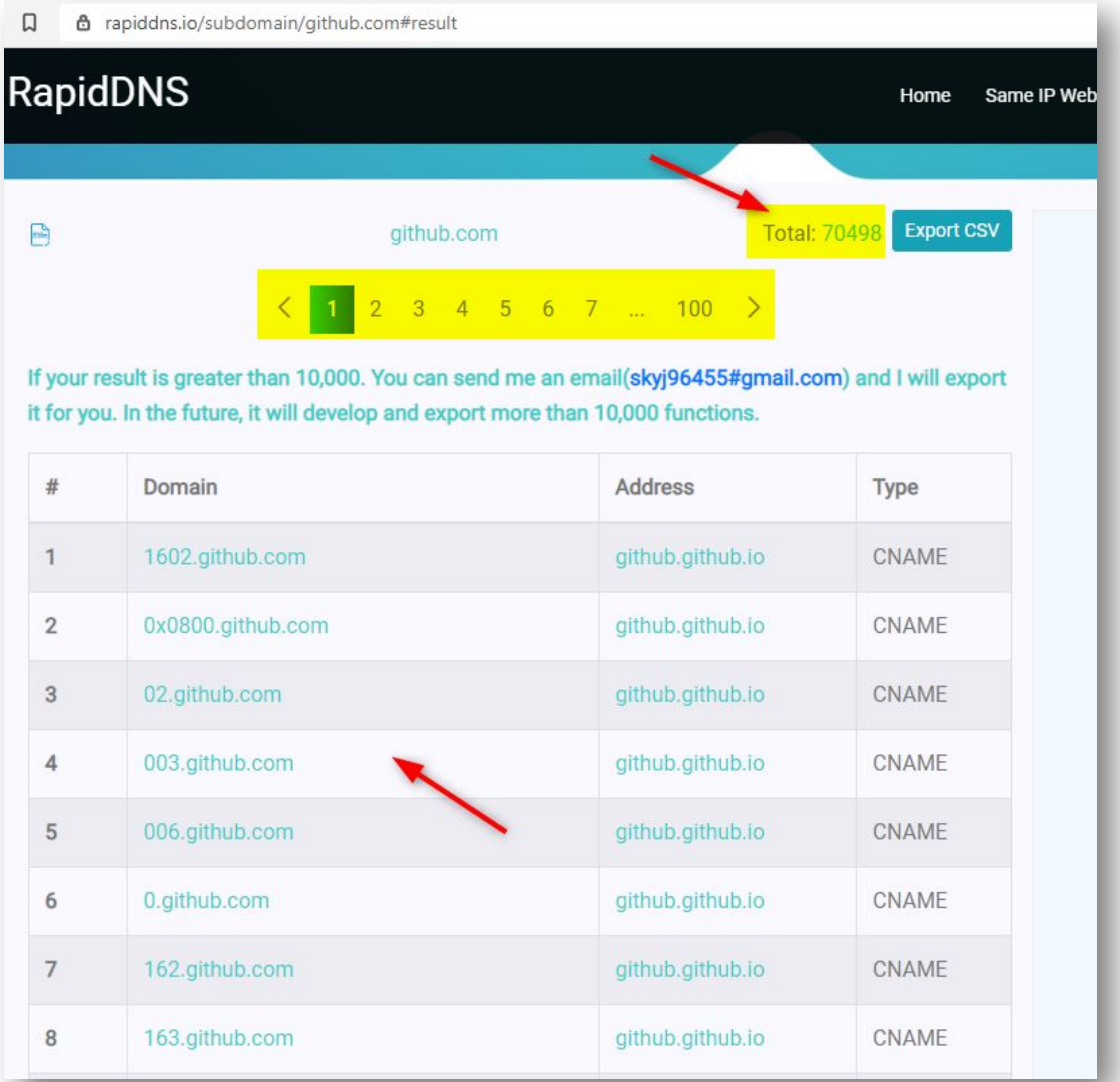
rapiddns.io/subdomain/github.com#result

RapidDNS

Subdomain

You can query all subdomains of the root domain. Enjoy it!

github.com

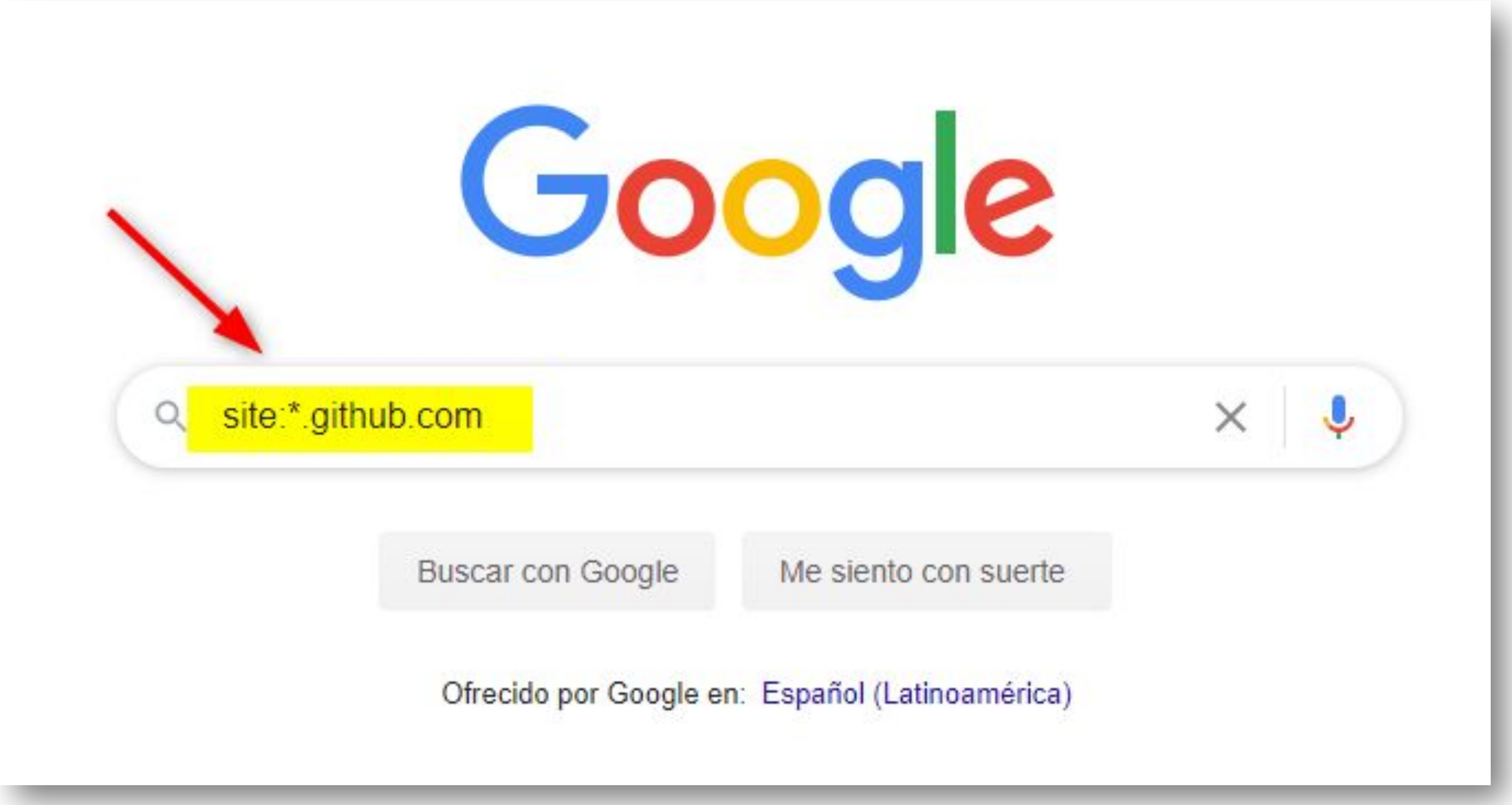


github.com

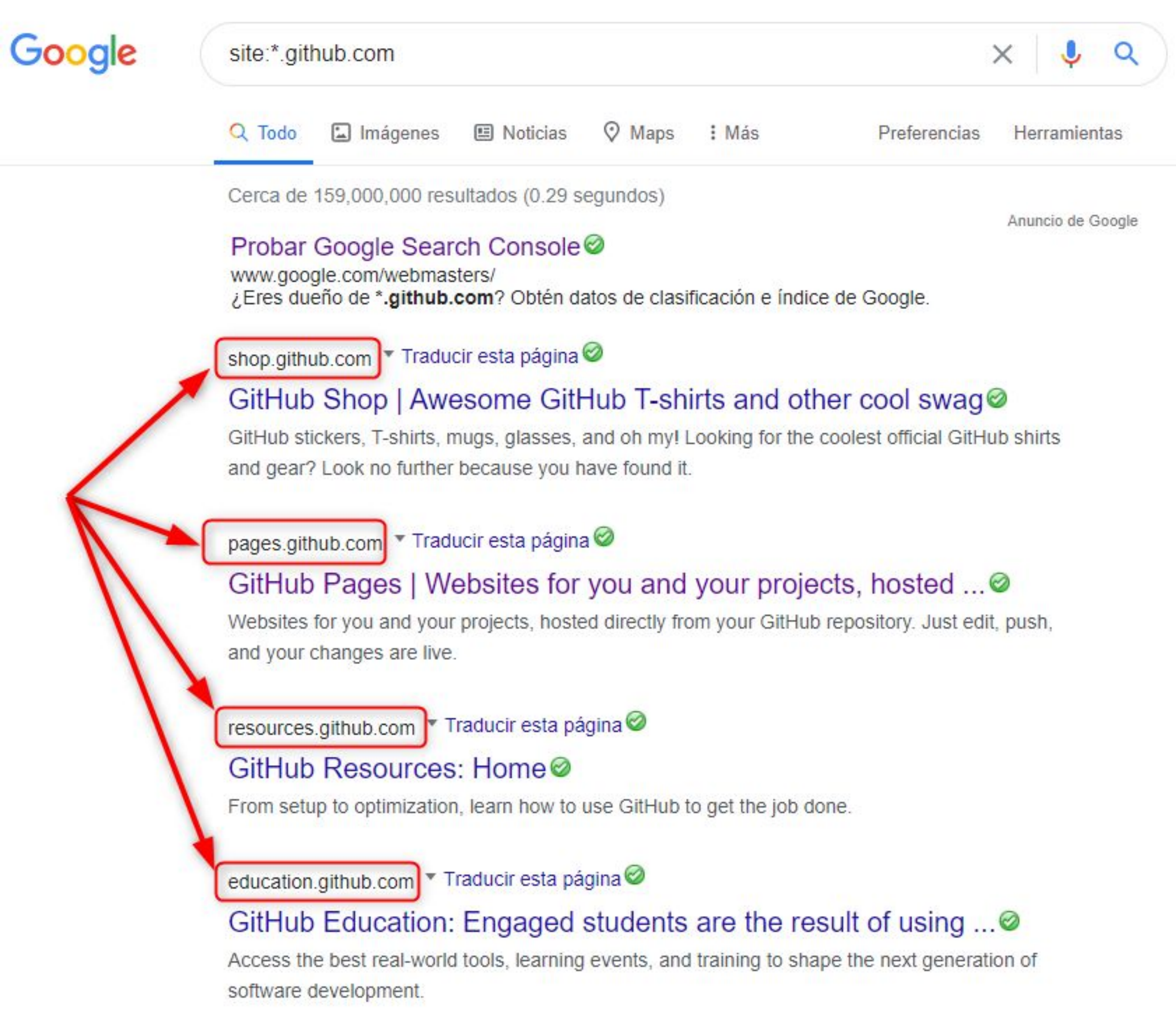
Total: 70498

If your result is greater than 10,000. You can send me an email(skyj96455#gmail.com) and I will export it for you. In the future, it will develop and export more than 10,000 functions.

#	Domain	Address	Type
1	1602.github.com	github.github.io	CNAME
2	0x0800.github.com	github.github.io	CNAME
3	02.github.com	github.github.io	CNAME
4	003.github.com	github.github.io	CNAME
5	006.github.com	github.github.io	CNAME
6	0.github.com	github.github.io	CNAME
7	162.github.com	github.github.io	CNAME
8	163.github.com	github.github.io	CNAME



site:*.github.com



Cerca de 159,000,000 resultados (0.29 segundos)

Anuncio de Google

Probar Google Search Console

www.google.com/webmasters/

¿Eres dueño de *.**github.com**? Obtén datos de clasificación e índice de Google.

shop.github.com ▾ Traducir esta página

GitHub Shop | Awesome GitHub T-shirts and other cool swag

GitHub stickers, T-shirts, mugs, glasses, and oh my! Looking for the coolest official GitHub shirts and gear? Look no further because you have found it.

pages.github.com ▾ Traducir esta página

GitHub Pages | Websites for you and your projects, hosted ...

Websites for you and your projects, hosted directly from your GitHub repository. Just edit, push, and your changes are live.

resources.github.com ▾ Traducir esta página

GitHub Resources: Home

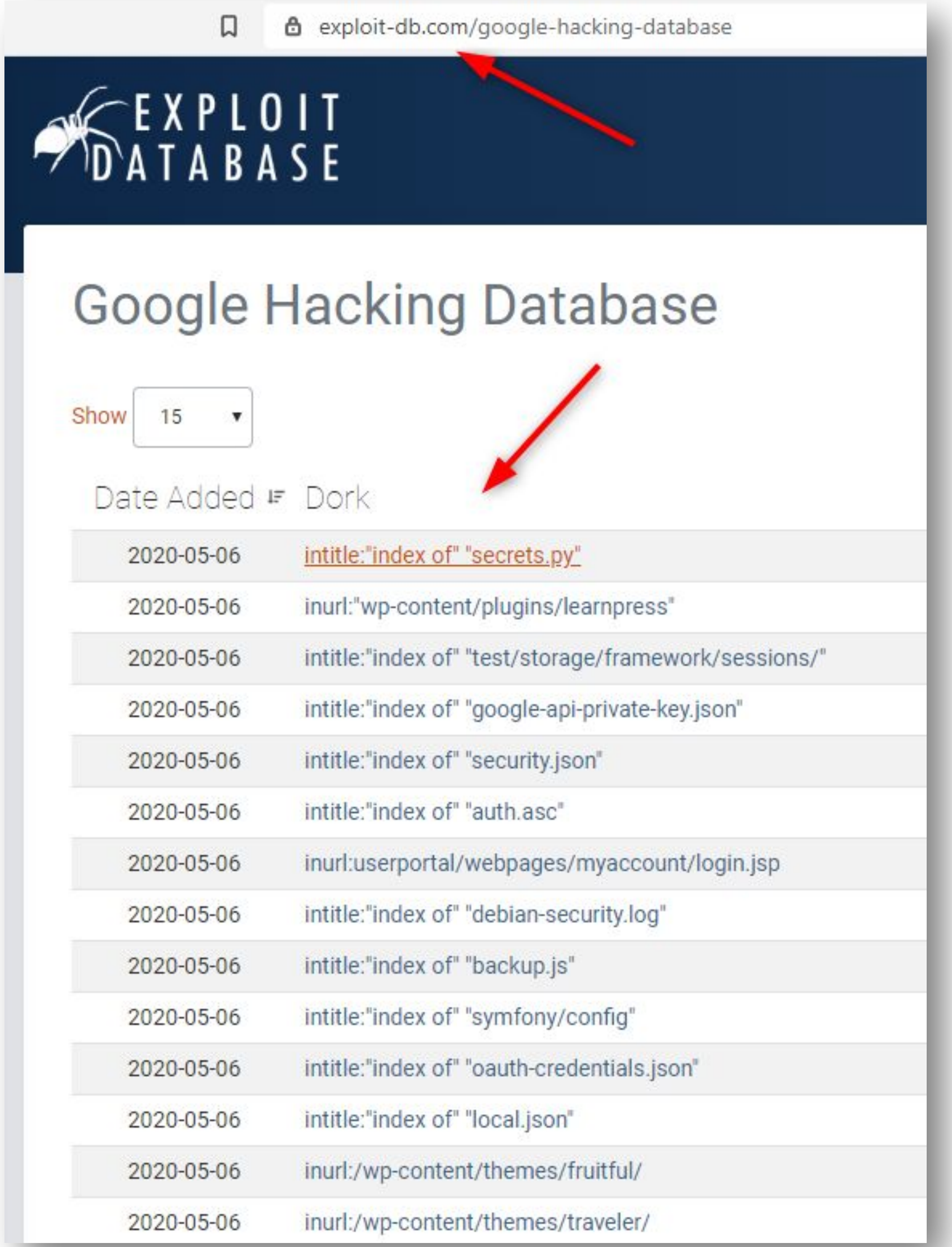
From setup to optimization, learn how to use GitHub to get the job done.

education.github.com ▾ Traducir esta página

GitHub Education: Engaged students are the result of using ...

Access the best real-world tools, learning events, and training to shape the next generation of software development.

Más Google Dorks :V



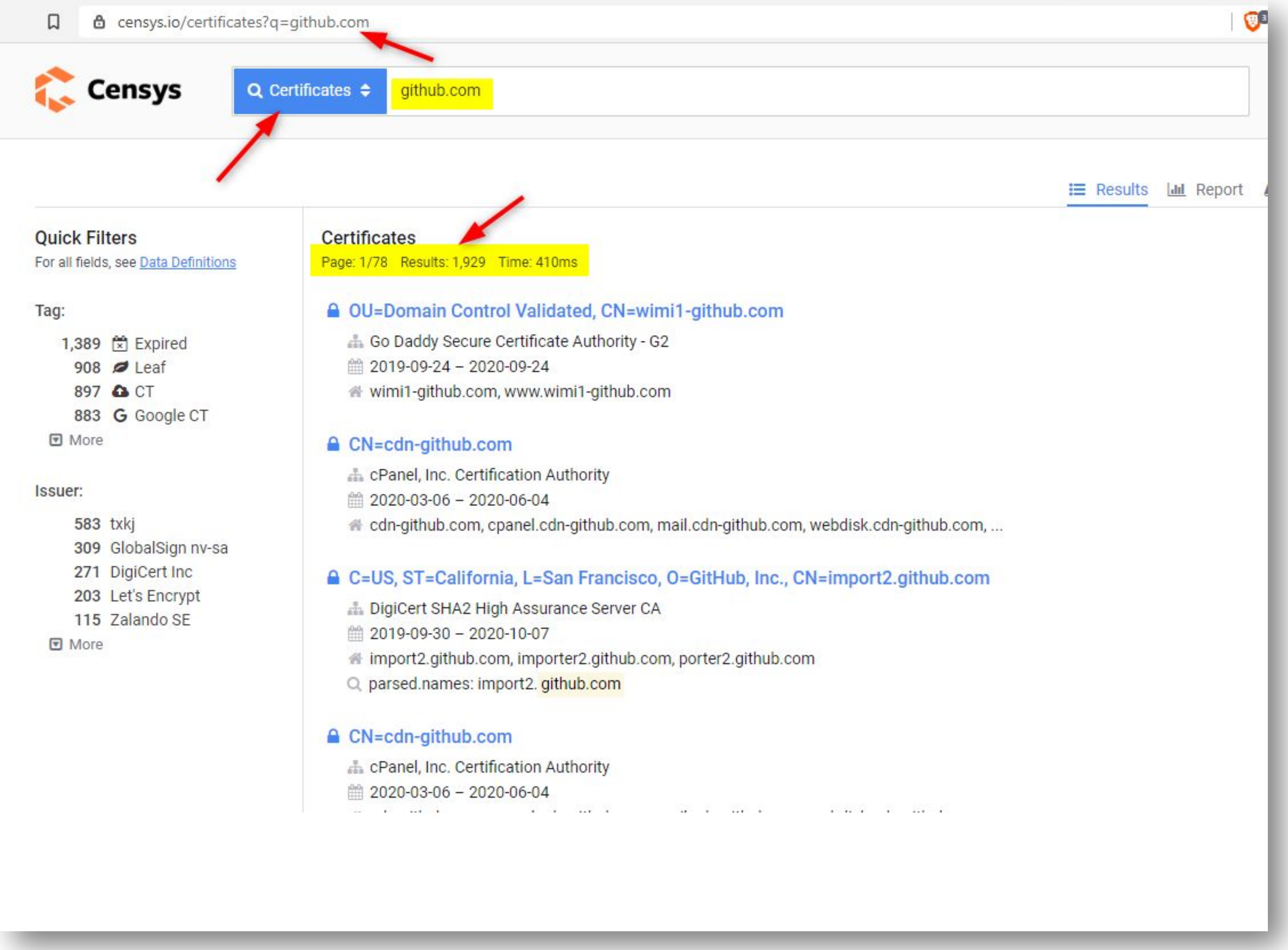
exploit-db.com/google-hacking-database

EXPLOIT DATABASE

Google Hacking Database

Show 15

Date Added	Dork
2020-05-06	intitle:"index of" "secrets.py"
2020-05-06	inurl:"wp-content/plugins/learnpress"
2020-05-06	intitle:"index of" "test/storage/framework/sessions/"
2020-05-06	intitle:"index of" "google-api-private-key.json"
2020-05-06	intitle:"index of" "security.json"
2020-05-06	intitle:"index of" "auth.asc"
2020-05-06	inurl:userportal/webpages/myaccount/login.jsp
2020-05-06	intitle:"index of" "debian-security.log"
2020-05-06	intitle:"index of" "backup.js"
2020-05-06	intitle:"index of" "symfony/config"
2020-05-06	intitle:"index of" "oauth-credentials.json"
2020-05-06	intitle:"index of" "local.json"
2020-05-06	inurl:/wp-content/themes/fruitful/
2020-05-06	inurl:/wp-content/themes/traveler/



Quick Filters

For all fields, see Data Definitions

Tag:

1,389	Expired
908	Leaf
897	CT
883	Google CT

More

Issuer:

583	txkj
309	GlobalSign nv-sa
271	DigiCert Inc
203	Let's Encrypt
115	Zalando SE

More

Certificates

Page: 1/78 Results: 1,929 Time: 410ms

OU=Domain Control Validated, CN=wimi1-github.com

Go Daddy Secure Certificate Authority - G2

2019-09-24 – 2020-09-24

wimi1-github.com, www.wimi1-github.com

CN=cdn-github.com

cPanel, Inc. Certification Authority

2020-03-06 – 2020-06-04

cdn-github.com, cpanel.cdn-github.com, mail.cdn-github.com, webdisk.cdn-github.com, ...

C=US, ST=California, L=San Francisco, O=GitHub, Inc., CN=import2.github.com

DigiCert SHA2 High Assurance Server CA

2019-09-30 – 2020-10-07

import2.github.com, importer2.github.com, porter2.github.com

parsed.names: import2. github.com

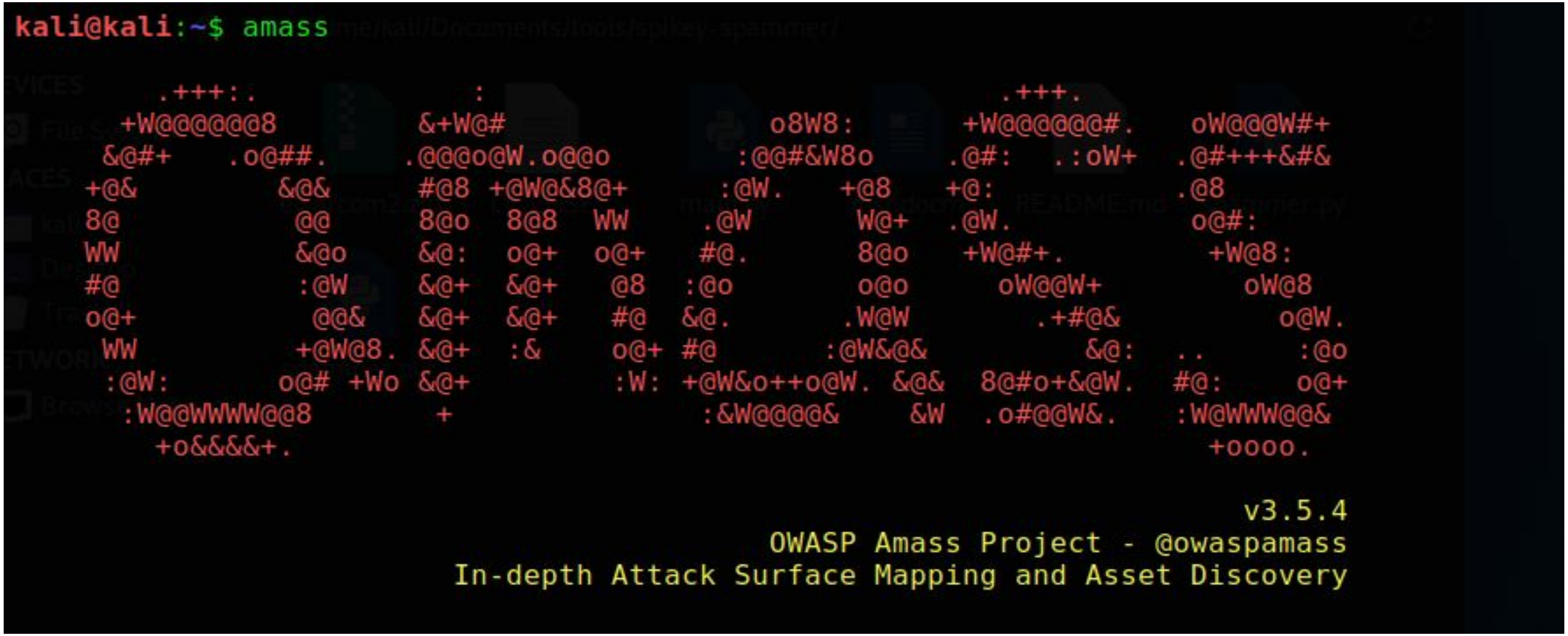
CN=cdn-github.com

cPanel, Inc. Certification Authority

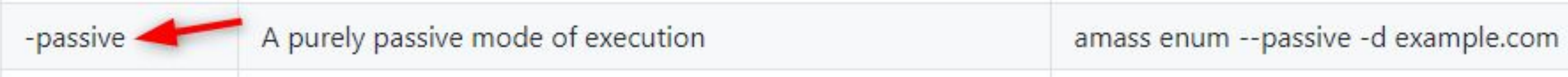
2020-03-06 – 2020-06-04

$ # Y la línea de comandos [¿?]😟

OWASP Amass



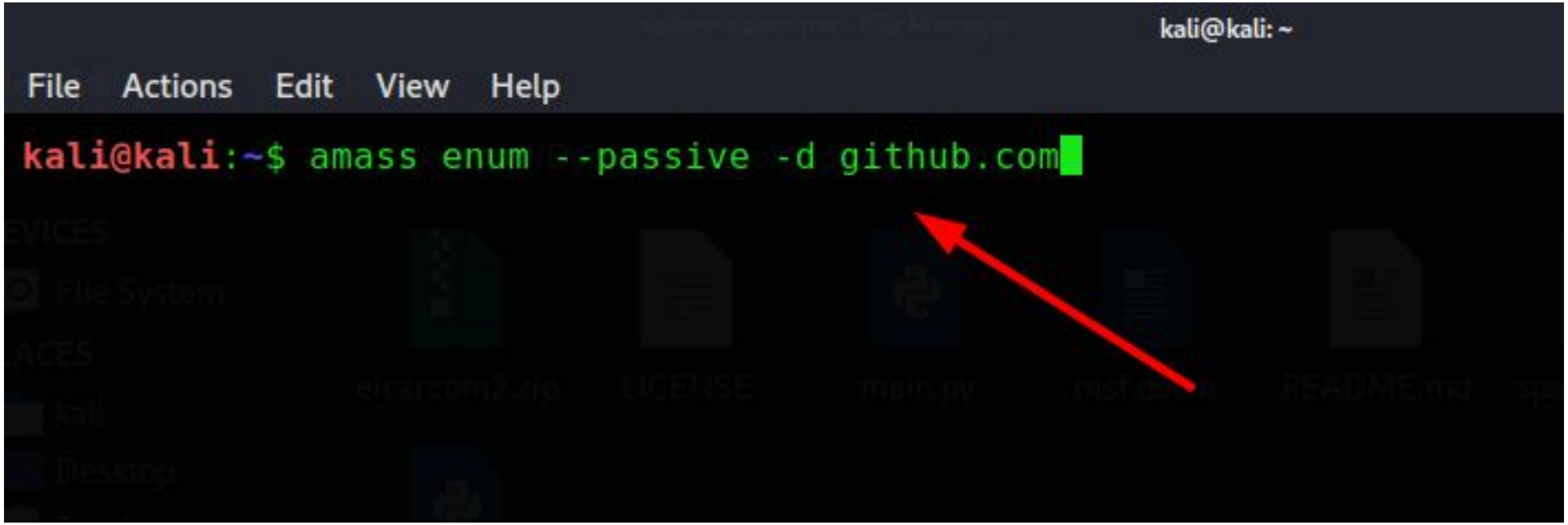
```
kali@kali:~$ amass

        .+++:.            :                             .+++.
      +W@@@@@@8        &+W@#               o8W8:      +W@@@@@@#.   oW@@@W#+
     &@#+   .o@##.    .@@@o@W.o@@o       :@@#&W8o    .@#:  .:oW+  .@#+++&#&
    +@&        &@&     #@8 +@W@&8@+     :@W.   +@8   +@:          .@8
    8@          @@     8@o  8@8  WW    .@W      W@+  .@W.          o@#:
    WW          &@o    &@:  o@+  o@+   #@.      8@o   +W@#+.        +W@8:
    #@          :@W    &@+  &@+   @8  :@o       o@o     oW@@W+        oW@8
    o@+          @@&   &@+  &@+   #@  &@.      .W@W       .+#@&         o@W.
     WW         +@W@8. &@+  :&    o@+ #@      :@W&@&         &@:  ..     :@o
     :@W:      o@# +Wo &@+        :W: +@W&o++o@W. &@&  8@#o+&@W.  #@:    o@+
      :W@@WWWW@@8       +              :&W@@@@&    &W  .o#@@W&.   :W@WWW@@&
        +o&&&&+.                                                    +oooo.

                                                                      v3.5.4
                                           OWASP Amass Project - @owaspamass
                         In-depth Attack Surface Mapping and Asset Discovery
```



-passive	A purely passive mode of execution	amass enum --passive -d example.com

Fuente: https://github.com/OWASP/Amass

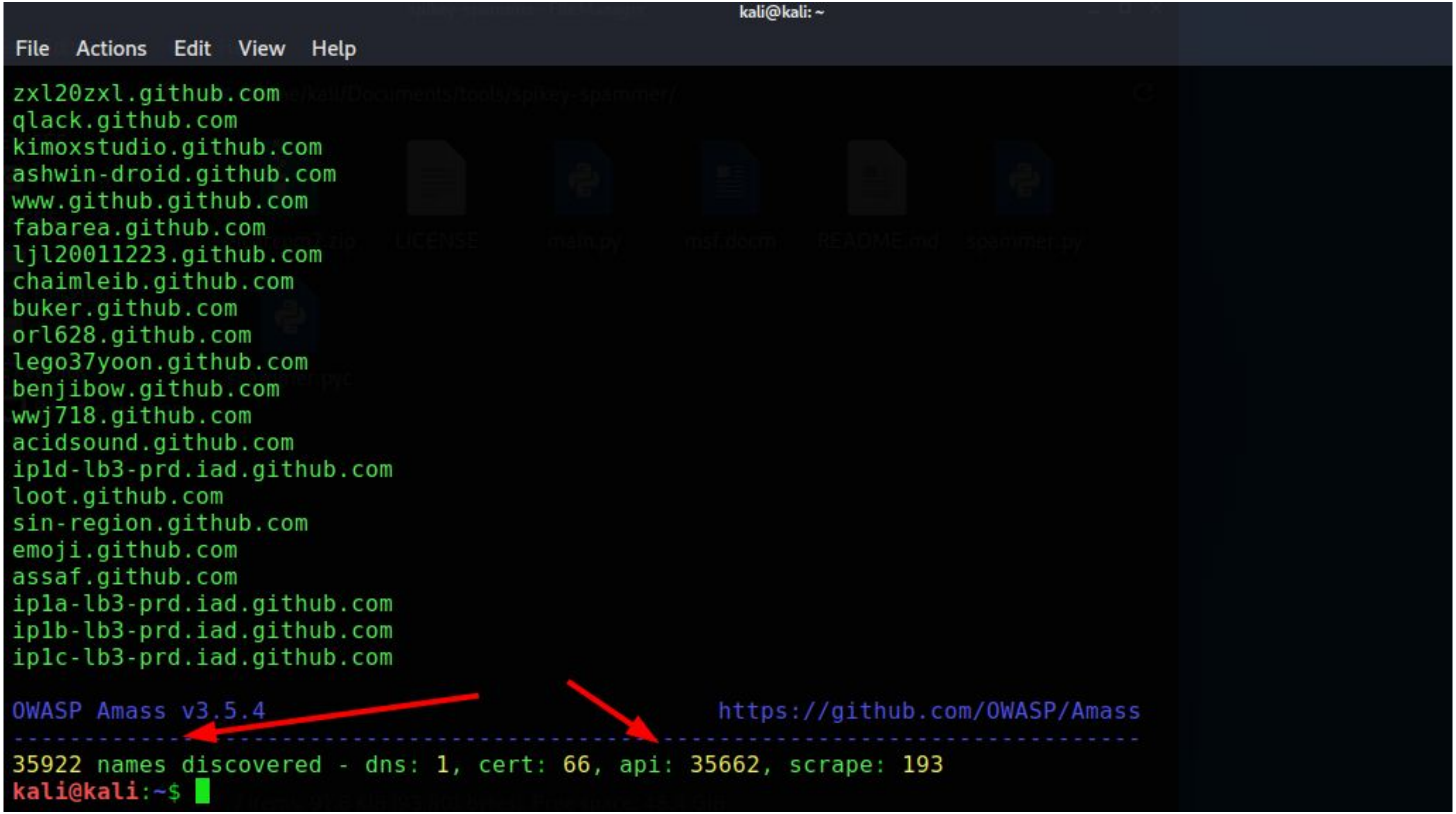
OWASP Amass



```
kali@kali:~$ amass enum --passive -d github.com
```

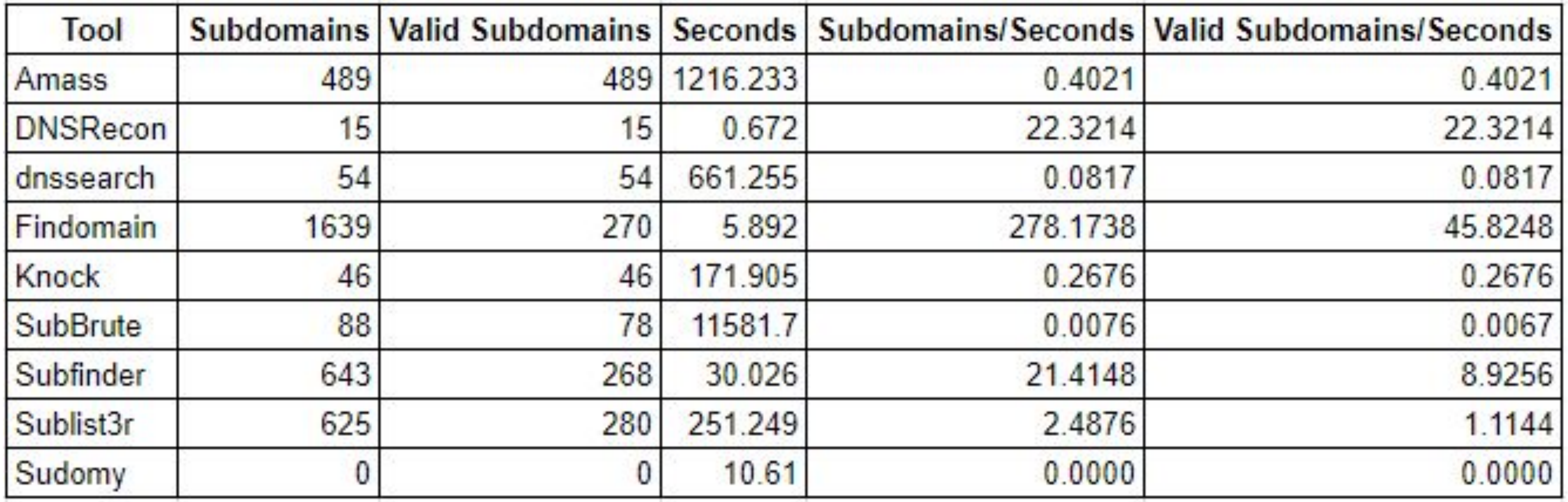
Fuente: https://github.com/OWASP/Amass

OWASP Amass



```
zxl20zxl.github.com
qlack.github.com
kimoxstudio.github.com
ashwin-droid.github.com
www.github.github.com
fabarea.github.com
ljl20011223.github.com
chaimleib.github.com
buker.github.com
orl628.github.com
lego37yoon.github.com
benjibow.github.com
wwj718.github.com
acidsound.github.com
ipld-lb3-prd.iad.github.com
loot.github.com
sin-region.github.com
emoji.github.com
assaf.github.com
ipla-lb3-prd.iad.github.com
iplb-lb3-prd.iad.github.com
iplc-lb3-prd.iad.github.com

OWASP Amass v3.5.4                              https://github.com/OWASP/Amass
--------------------------------------------------------------------------------
35922 names discovered - dns: 1, cert: 66, api: 35662, scrape: 193
kali@kali:~$
```

Otras Tools



Tool	Subdomains	Valid Subdomains	Seconds	Subdomains/Seconds	Valid Subdomains/Seconds
Amass	489	489	1216.233	0.4021	0.4021
DNSRecon	15	15	0.672	22.3214	22.3214
dnssearch	54	54	661.255	0.0817	0.0817
Findomain	1639	270	5.892	278.1738	45.8248
Knock	46	46	171.905	0.2676	0.2676
SubBrute	88	78	11581.7	0.0076	0.0067
Subfinder	643	268	30.026	21.4148	8.9256
Sublist3r	625	280	251.249	2.4876	1.1144
Sudomy	0	0	10.61	0.0000	0.0000

Fuente:
https://medium.com/@ricardoiramar/subdomain-enumeration-tools-evaluation-57d4ec02d69e

Recomendaciones

LIVE RECON
WITH NAHAMSEC
TWITCH.TV/NAHAMSEC
05/03/2020
11:00AM PST | 07:00PM UTC | 12:30AM IST
+ SPECIAL GUEST
JAMES KETTLE
@ALBINOWAX

LIVE RECON
WITH NAHAMSEC
TWITCH.TV/NAHAMSEC
04/26/2020
11:00AM PDT | 06:00PM UTC | 11:30PM IST
+ SPECIAL GUEST
MAYONAISE

Otras Recomendaciones...

OWASP LATAM@HOME
CONFERENCIAS Y TALLERES
LIGHTYEAR

Gracias! Hackers...