Web enum

Thursday, August 4, 2022

9:17 PM

# Assetfinder

# <https://github.com/tomnomnom/assetfinder>

./assetfinder tesla.com

suppliers.tesla.com

auth.tesla.com

tesla.com

[www.tesla.com](http://www.tesla.com)

b.ns.vps1.e.tesla.com.cn

digitalassets-accounts.tesla.com

issues.teslamotors.com

o1.emailo.tesla.com.cn

[www.c-us.teslamotors.cn](http://www.c-us.teslamotors.cn)

ir.tesla.com

tesla.cn

link.tesla.com

[www.film-blogs.teslamotors.cn](http://www.film-blogs.teslamotors.cn)

[www.ns10-dl.teslamotors.cn](http://www.ns10-dl.teslamotors.cn)

tinton.site

teslastore.us

epc.tesla.com

tesler-ai.work

teslacdpna0.tesla.com

[www.teslamotors.com](http://www.teslamotors.com)

suppliers.teslamotors.com

bankdramowadabkil.gq

events-b.mb.manwardpress.com

service.tesla.com

iplogger.org

[www.tesla.cn](http://www.tesla.cn)

cloudinary.com

sso.tesla.com

pay.tesla.com

shop.tesla.com

# AMASS

amass intel -d owasp.org -whois

# Httprobe

▶ cat recon/example/domains.txt

example.com

example.edu

example.net

▶ cat recon/example/domains.txt | httprobe

<http://example.com>

<http://example.net>

<http://example.edu>

<https://example.com>

<https://example.edu>

<https://example.net>

cat domains.txt | httprobe -p http:81 -p https:8443

You can set the concurrency level with the -c flag:

cat domains.txt | httprobe -c 50

You can change the timeout by using the -t flag and specifying a timeout in milliseconds:

cat domains.txt | httprobe -t 20000

# gowitness - a golang, web screenshot utility

<https://github.com/sensepost/gowitness>

# Auto recon

<https://github.com/TCM-Course-Resources/Practical-Ethical-Hacking-Resources/blob/master/bash/webrecon.sh>