



Recon ASRC Conference



Mike Takahashi
@TakSec



whoami

Mike Takahashi

Bug Bounty Hunter

Program Manager @ Stanford

Twitter: **@TakSec**

WeChat: **taksec**



Bug Bounty Landscape

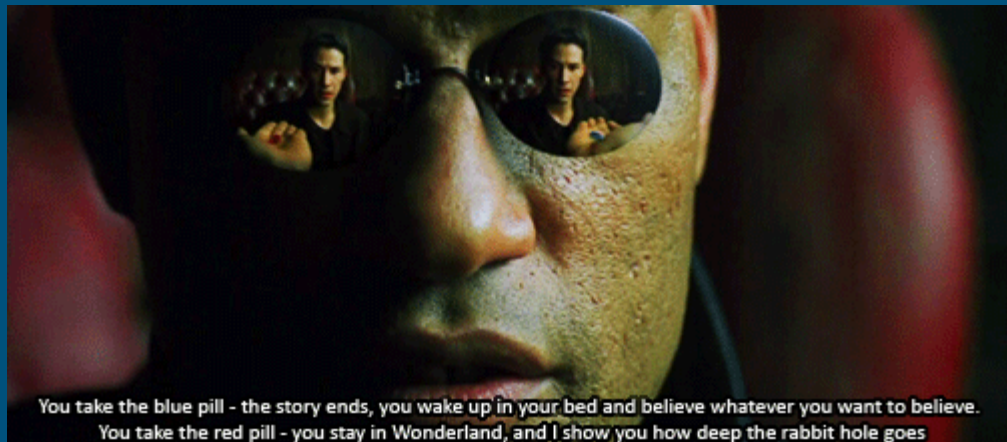
The road less traveled

Recon Recon Recon



Methodology

1. Brands
2. Subdomains
3. Mapping
4. Hack
5. Recon again!
















Acquisitions & Brands

<https://www.crunchbase.com/>

<https://en.wikipedia.org>

Footers & about us:

<https://www.alibaba.com/>

1.  Ejoy Technology acquired by Alibaba
2.  Yueke Software acquired by Alibaba
3.  AutoNavi acquired by Alibaba
4.  Kanbox acquired by Alibaba
5.  AdChina acquired by Alibaba
6.  UCWeb acquired by Alibaba
7.  Vendio acquired by Alibaba
8.  Damai.cn acquired by Alibaba
9.  Wandoujia acquired by Alibaba
10.  South China Morning Post acquired by Alibaba
11.  Umeng acquired by Alibaba
12.  Youku acquired by Alibaba
13.  AGTech Holdings acquired by Alibaba

ASNs

<https://bgp.he.net>



HURRICANE ELECTRIC
INTERNET SERVICES

Network Info Whois DNS IRR

Announced By

Origin AS	Announcement	Description
AS45102	198.11.128.0/18	Alibaba.com LLC

	yagesanitary.com , ybhhardware.com , yix.xin , ykouyada.c , yotoon.net , yuhey.com , yumi-photoelectric.com , yutehose , zdlmm.com , zhongliansteel.com , zitoys.com , zjyyfh.com ,
198.11.132.16	hsf.club
198.11.132.23	hkmeituo.com
198.11.132.52	alibabagroup.com
198.11.132.78	ent-fund.org
198.11.132.250	aishidis.com , aliexpress.com , insectchina.com , itao.com ,

Reverse Whois

<http://viewdns.info/reversewhois/>

Search unique identifier:

1. Name
2. Registered Email

alibaba-capital.net

alibaba-capital.org

alibaba-china.com.cn

alibaba-china.com

alibaba-china.net

alibaba-cloud.com

alibaba-cloud.net

alibaba-cneast.com

alibaba-corp.asia

alibaba-corp.com

alibaba-corp.net

alibaba-credit.com

alibaba-credit.mobi

alibaba-credit.net

alibaba-films.com

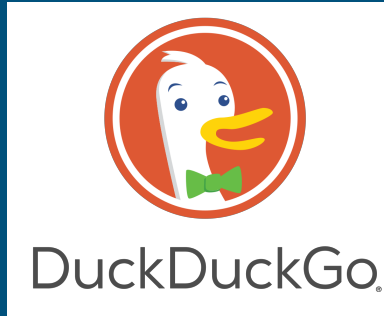
alibaba-films.net

alibaba-group.asia

alibaba-group.com

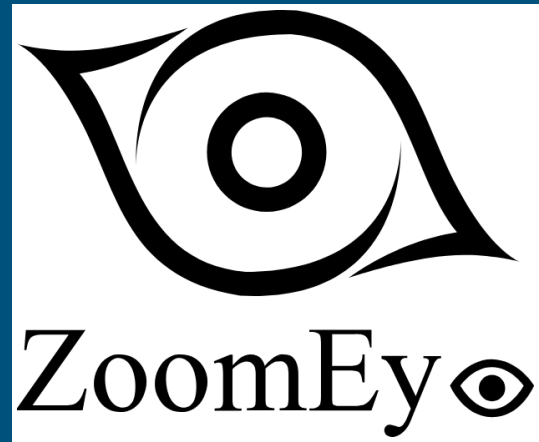
alibaba-group.net

Search Engine Dorks

The Google logo, featuring the word "Google" in its characteristic multi-colored font (blue, red, yellow, green, red, blue).The Baidu logo, featuring the word "Baidu" in a stylized font. The "Bai" is in red, "du" is in blue, and the Chinese characters "百度" are in red. A blue paw print icon is positioned between "du" and "百度".The Bing logo, featuring a green stylized "B" icon followed by the word "Bing" in a green, sans-serif font.

GHDB: <https://www.exploit-db.com/google-hacking-database/>

Search Engines for Servers



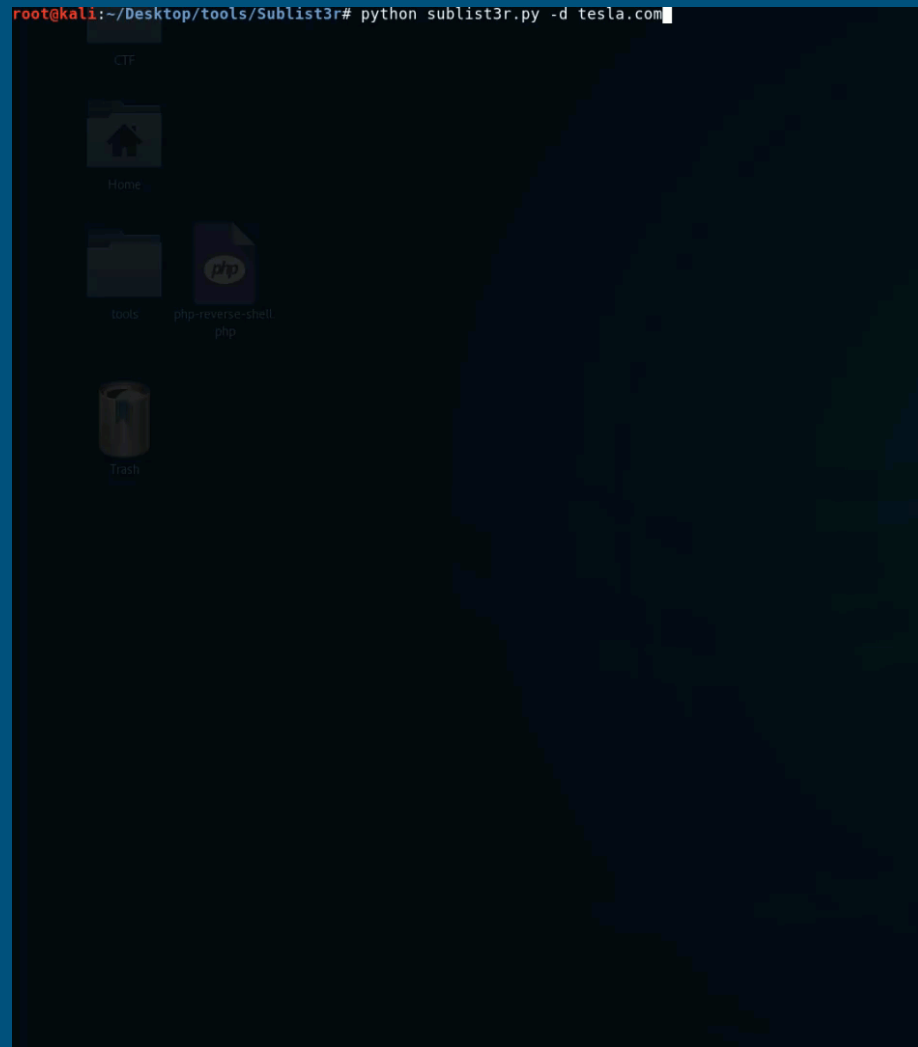
Subdomain Discovery

<https://dnsdumpster.com/>

Subfinder

Amass

Aquatone



Subdomain Bruteforcing

subbrute

massdns

subfinder

All.txt - JHaddix



Fingerprinting

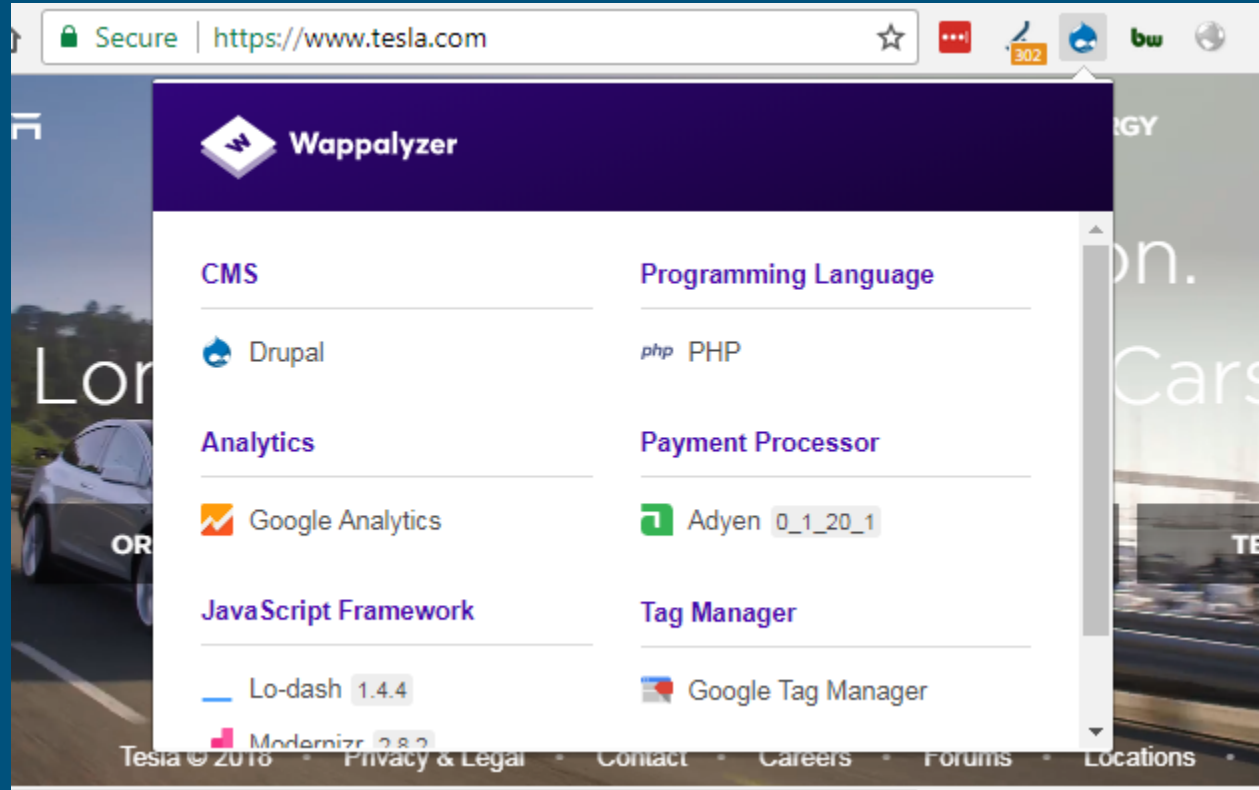
Wappalyzer

Builtwith

Vulners

WPScan

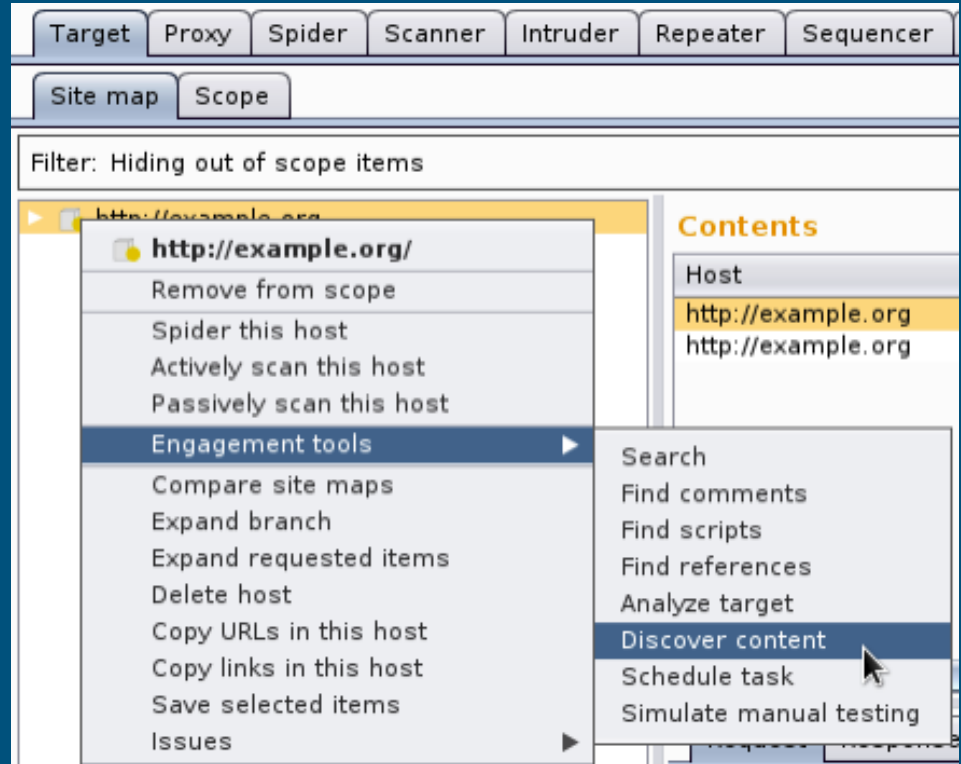
droopescan



Mapping

Directory brute forcing:

- GoBuster
- Burp Discover Content
- Search engine dorks



Found a bug, now what?



Recon Again!

Same vuln on other domains/subdomains

Search engine dorks

Bug * Recon = \$\$\$

Questions?

Thank you

Twitter: @TakSec

WeChat: **taksec**