Gotta catch'em all!

Finding subdomains like a god

> whoami

six2dez

> screenfetch

Name: Alexis Fernández

Location: Madrid, España

Occupation: Pentester & Bug Hunter

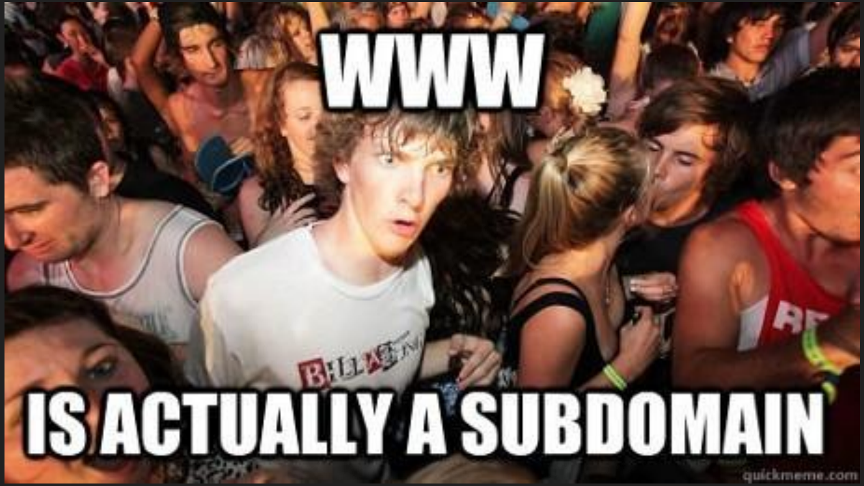
Website: pentestbook.six2dez.com

Projects: reconFTW & OneListForAll

> startx

INTRO

- Increase the attack surface
- Essential part of recon
- Descriptive words
- Related to functionality
- Obsolete forgotten subdomains
- Takeovers
- Subdomain != Website
- Special characters: '-' '.'



PASSIVE

- Third party services
- Domain collectors
- Scrapers or official clients
- Free and paid
- API keys
- Data limits / month
- + 60 similar services

PASSIVE: TOOLS & SOURCES

Tools

Amass (~60)

Subfinder (~40)

Findomain free (~15)

Assetfinder (~9)

Gau/Gauplus (3)

Waybackurls (3)

Crobat/SonarSearch - FDNS (1)

Sources

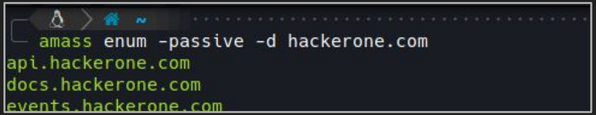
General:

- Censys
- Spyse
- SecurityTrails
- PassiveTotal

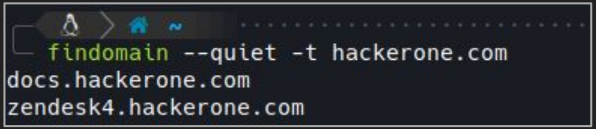
Specific:

- GitHub
- WaybackMachine
- Facebook
- CloudFlare
- VirusTotal

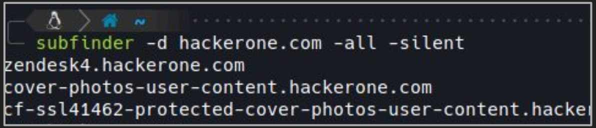
PASSIVE: EXAMPLES



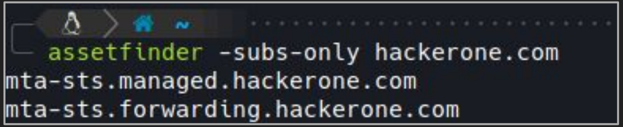
```
amass enum -passive -d hackerone.com
api.hackerone.com
docs.hackerone.com
events.hackerone.com
```



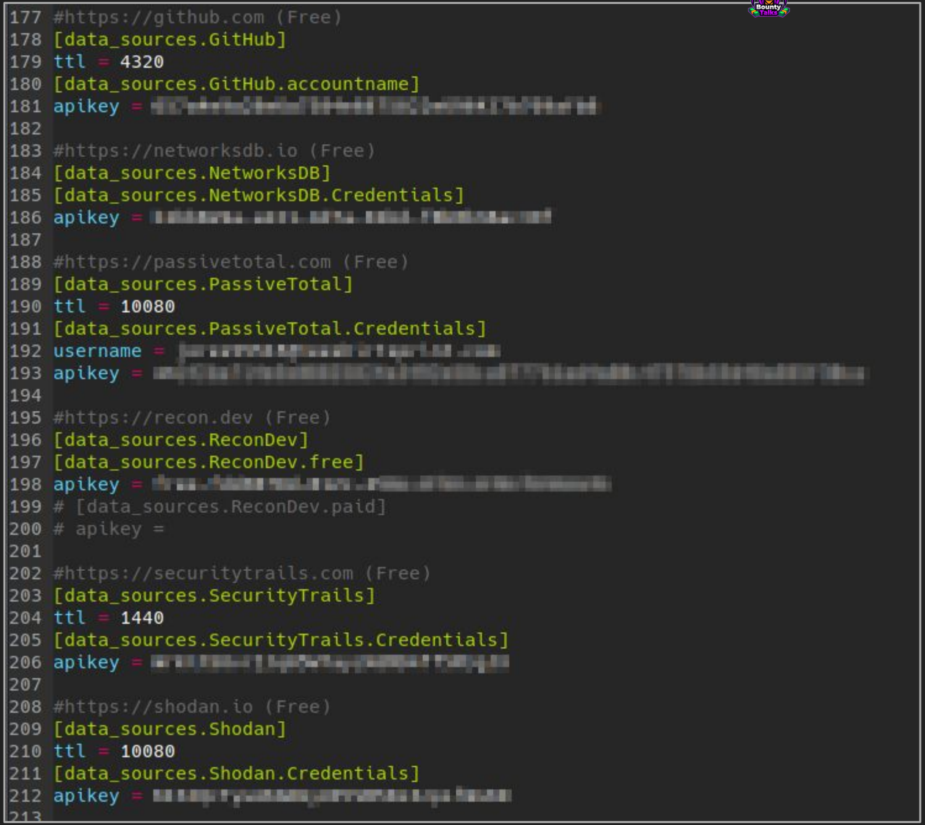
```
findomain --quiet -t hackerone.com
docs.hackerone.com
zendesk4.hackerone.com
```



```
subfinder -d hackerone.com -all -silent
zendesk4.hackerone.com
cover-photos-user-content.hackerone.com
cf-ssl41462-protected-cover-photos-user-content.hacke
```



```
assetfinder -subs-only hackerone.com
mta-sts.managed.hackerone.com
mta-sts.forwarding.hackerone.com
```



```
#https://github.com (Free)
[data_sources.GitHub]
ttl = 4320
[data_sources.GitHub.accountname]
apikey = [redacted]

#https://networksdb.io (Free)
[data_sources.NetworksDB]
[data_sources.NetworksDB.Credentials]
apikey = [redacted]

#https://passivetotal.com (Free)
[data_sources.PassiveTotal]
ttl = 10080
[data_sources.PassiveTotal.Credentials]
username = [redacted]
apikey = [redacted]

#https://recon.dev (Free)
[data_sources.ReconDev]
[data_sources.ReconDev.free]
apikey = [redacted]
# [data_sources.ReconDev.paid]
# apikey =

#https://securitytrails.com (Free)
[data_sources.SecurityTrails]
ttl = 1440
[data_sources.SecurityTrails.Credentials]
apikey = [redacted]

#https://shodan.io (Free)
[data_sources.Shodan]
ttl = 10080
[data_sources.Shodan.Credentials]
apikey = [redacted]
```

Amass config file

PASSIVE: PROS & CONS

PROS

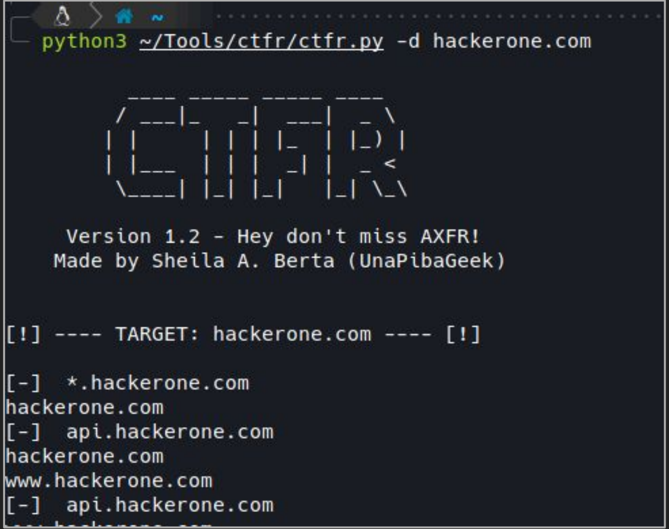
- Large number of results
- Fast
- Easy
- Basis for future steps

CONS

- Outdated information
- Signup process in every service
- Tool Settings
- Duplicates per service
- Payment services
- Token spend / request

CERTIFICATE TRANSPARENCY

- Passive source
- Contains the certificate information
- Certification authorities use CT to detect frauds
- Sources
  - https://certificate.transparency.dev/
  - https://crt.sh/
- Tools:
  - ctfr (https://github.com/UnaPibaGeek/ctfr)
  - subcert (https://github.com/A3h1nt/Subcert)
  - crtfinder(https://github.com/eslam3kl/crtfinder)
- Pros/cons
  - Free and up-to-date
  - Just sites with certs



```
python3 ~/Tools/ctfr/ctfr.py -d hackerone.com

          ____ _____ _____ ____
         / ___|_   _|  ___|  _ \
        | |     | | | |_  | |_) |
        | |___  | | |  _| |  _ <
         \____| |_| |_|   |_| \_\

     Version 1.2 - Hey don't miss AXFR!
    Made by Sheila A. Berta (UnaPibaGeek)


[!] ---- TARGET: hackerone.com ---- [!]

[-]  *.hackerone.com
hackerone.com
[-]  api.hackerone.com
hackerone.com
www.hackerone.com
[-]  api.hackerone.com
```

BRUTE FORCE

Wordlists usage to get subdomains by DNS resolution.

Tools:

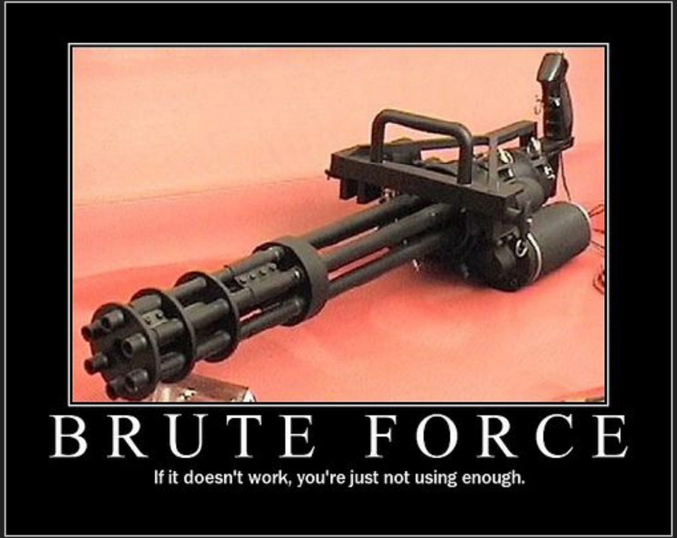
- puredns (https://github.com/d3mondev/puredns)
- shuffledns (https://github.com/projectdiscovery/shuffledns)

Wordlists:

- Assetnote (https://wordlists-cdn.assetnote.io/data/manual/best-dns-wordlist.txt)
- SecLists (https://github.com/danielmiessler/SecLists/blob/master/Discovery/DNS/sortedcombined-knock-dnsrecon-fierce-reconng.txt)

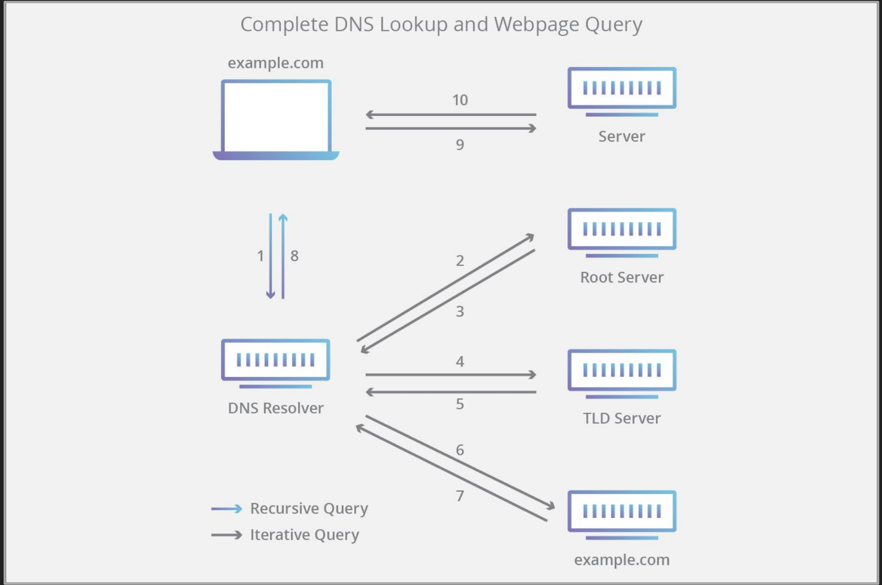
Pros/cons:

- Valuable results (not indexed yet)
- Bandwidth bottleneck (better on VPS) and bans.



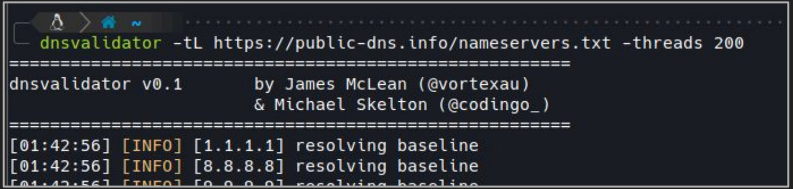
BRUTE FORCE: DNS RESOLUTION

- We request to a DNS resolver to resolve the request
- We do not interact directly with the target
- Known DNS resolvers limits:
  - Google (1500 rps)
  - CloudFlare (Dinamic ~300 rps)
  - Quad9 (Bruteforce not allowed)
  - OpenDNS (Bruteforce not allowed)
  - Comodo (No specified)
  - AlternateDNS (Dinamic ~100 rps)



BRUTE FORCE: RESOLVERS

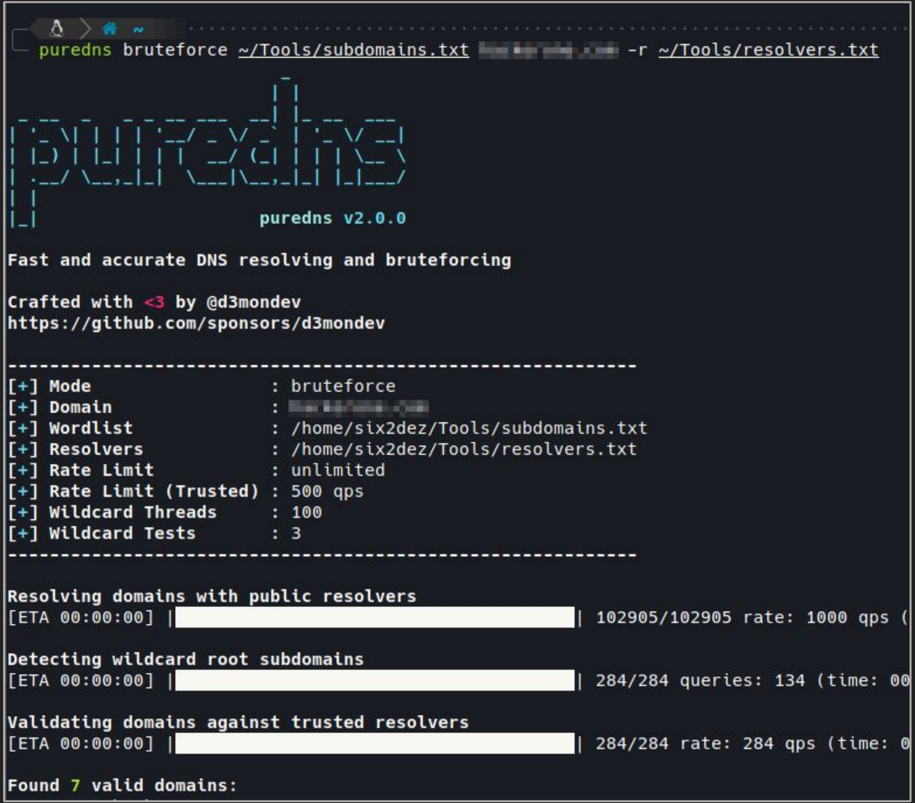
- List of public resolvers:
  - dnsvalidator (https://github.com/vortexau/dnsvalidator)



```
dnsvalidator -tL https://public-dns.info/nameservers.txt -threads 200
============================================================
dnsvalidator v0.1        by James McLean (@vortexau)
                         & Michael Skelton (@codingo_)
============================================================
[01:42:56] [INFO] [1.1.1.1] resolving baseline
[01:42:56] [INFO] [8.8.8.8] resolving baseline
[01:42:56] [INFO] [9.9.9.9] resolving baseline
```

- DNS resolution with new resolvers:
  - Maximum speed> 3000 rps
  - Better from VPS
- Double check with trusted resolvers:
  - Speed <400 rps

Without double-checking there are false positives



```
puredns bruteforce ~/Tools/subdomains.txt [redacted] -r ~/Tools/resolvers.txt

                      _
                     | |
 _ __  _   _ _ __ ___  __| |_ __  ___
| '_ \| | | | '__/ _ \/ _` | '_ \/ __|
| |_) | |_| | | |  __/ (_| | | | \__ \
| .__/ \__,_|_|  \___|\__,_|_| |_|___/
| |
|_|                       puredns v2.0.0

Fast and accurate DNS resolving and bruteforcing

Crafted with <3 by @d3mondev
https://github.com/sponsors/d3mondev

------------------------------------------------------------
[+] Mode                 : bruteforce
[+] Domain               : [redacted]
[+] Wordlist             : /home/six2dez/Tools/subdomains.txt
[+] Resolvers            : /home/six2dez/Tools/resolvers.txt
[+] Rate Limit           : unlimited
[+] Rate Limit (Trusted) : 500 qps
[+] Wildcard Threads     : 100
[+] Wildcard Tests       : 3
------------------------------------------------------------

Resolving domains with public resolvers
[ETA 00:00:00] |                                      | 102905/102905 rate: 1000 qps (

Detecting wildcard root subdomains
[ETA 00:00:00] |                                      | 284/284 queries: 134 (time: 00

Validating domains against trusted resolvers
[ETA 00:00:00] |                                      | 284/284 rate: 284 qps (time: 0

Found 7 valid domains:
```

PERMUTATIONS AND ALTERATIONS

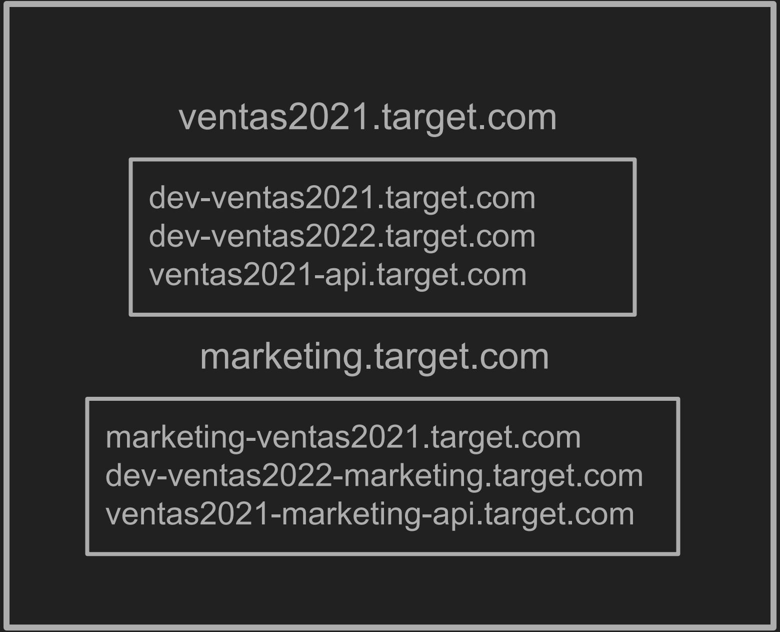
Generation of dictionaries based on already found subdomains and a list of permutations.

- Increase and decrease numbers
- Levels of depth
- Use of '.' and '-' to concatenate
- Using previous results as iterations

Pros/cons:

- Valuable results
- Disk space, bandwidth bottleneck (better in VPS), bans.

Tool:
gotator (https://github.com/Josue87/gotator)



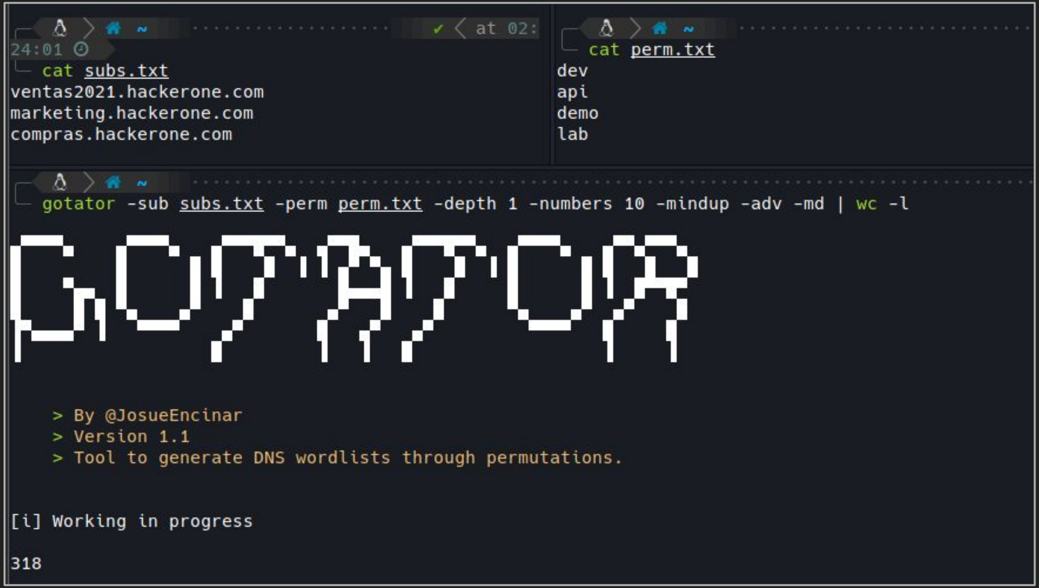
ventas2021.target.com

dev-ventas2021.target.com
dev-ventas2022.target.com
ventas2021-api.target.com

marketing.target.com

marketing-ventas2021.target.com
dev-ventas2022-marketing.target.com
ventas2021-marketing-api.target.com

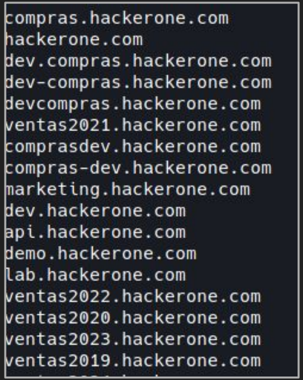
GOTATOR EXAMPLES



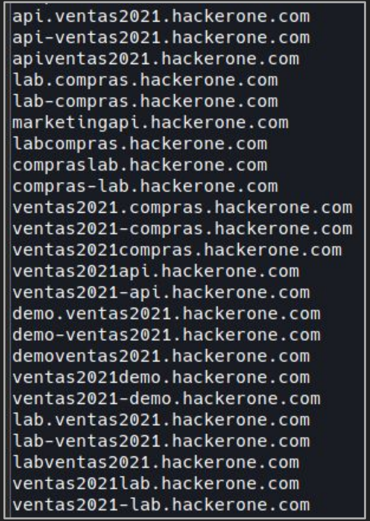
```
 ~                                    ✓ < at 02:
24:01
└ cat subs.txt
ventas2021.hackerone.com
marketing.hackerone.com
compras.hackerone.com
```

```
 ~
└ cat perm.txt
dev
api
demo
lab
```

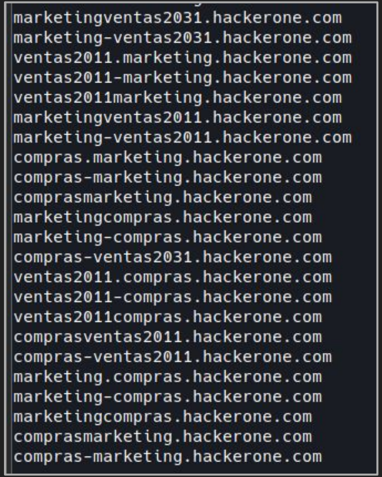
```
 ~
└ gotator -sub subs.txt -perm perm.txt -depth 1 -numbers 10 -mindup -adv -md | wc -l

GOTATOR

    > By @JosueEncinar
    > Version 1.1
    > Tool to generate DNS wordlists through permutations.


[i] Working in progress

318
```



```
compras.hackerone.com
hackerone.com
dev.compras.hackerone.com
dev-compras.hackerone.com
devcompras.hackerone.com
ventas2021.hackerone.com
comprasdev.hackerone.com
compras-dev.hackerone.com
marketing.hackerone.com
dev.hackerone.com
api.hackerone.com
demo.hackerone.com
lab.hackerone.com
ventas2022.hackerone.com
ventas2020.hackerone.com
ventas2023.hackerone.com
ventas2019.hackerone.com
```



```
api.ventas2021.hackerone.com
api-ventas2021.hackerone.com
apiventas2021.hackerone.com
lab.compras.hackerone.com
lab-compras.hackerone.com
marketingapi.hackerone.com
labcompras.hackerone.com
compraslab.hackerone.com
compras-lab.hackerone.com
ventas2021.compras.hackerone.com
ventas2021-compras.hackerone.com
ventas2021compras.hackerone.com
ventas2021api.hackerone.com
ventas2021-api.hackerone.com
demo.ventas2021.hackerone.com
demo-ventas2021.hackerone.com
demoventas2021.hackerone.com
ventas2021demo.hackerone.com
ventas2021-demo.hackerone.com
lab.ventas2021.hackerone.com
lab-ventas2021.hackerone.com
labventas2021.hackerone.com
ventas2021lab.hackerone.com
ventas2021-lab.hackerone.com
```



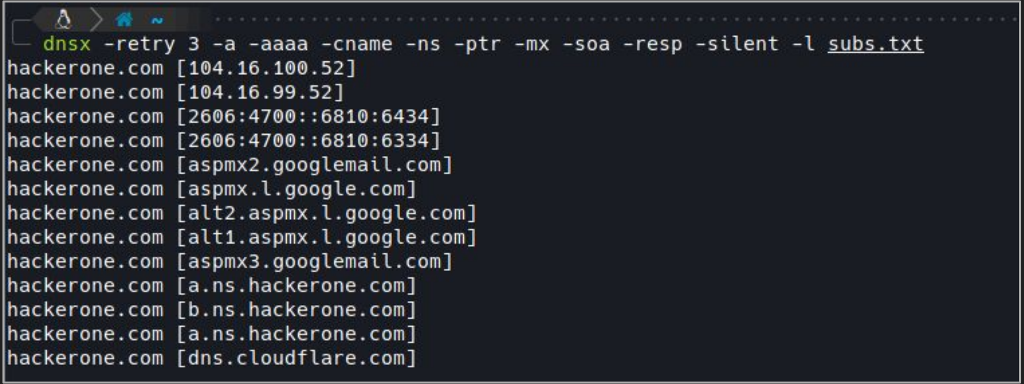
```
marketingventas2031.hackerone.com
marketing-ventas2031.hackerone.com
ventas2011.marketing.hackerone.com
ventas2011-marketing.hackerone.com
ventas2011marketing.hackerone.com
marketingventas2011.hackerone.com
marketing-ventas2011.hackerone.com
compras.marketing.hackerone.com
compras-marketing.hackerone.com
comprasmarketing.hackerone.com
marketingcompras.hackerone.com
marketing-compras.hackerone.com
compras-ventas2031.hackerone.com
ventas2011.compras.hackerone.com
ventas2011-compras.hackerone.com
ventas2011compras.hackerone.com
comprasventas2011.hackerone.com
compras-ventas2011.hackerone.com
marketing.compras.hackerone.com
marketing-compras.hackerone.com
marketingcompras.hackerone.com
comprasmarketing.hackerone.com
compras-marketing.hackerone.com
```

DNS RECORDS

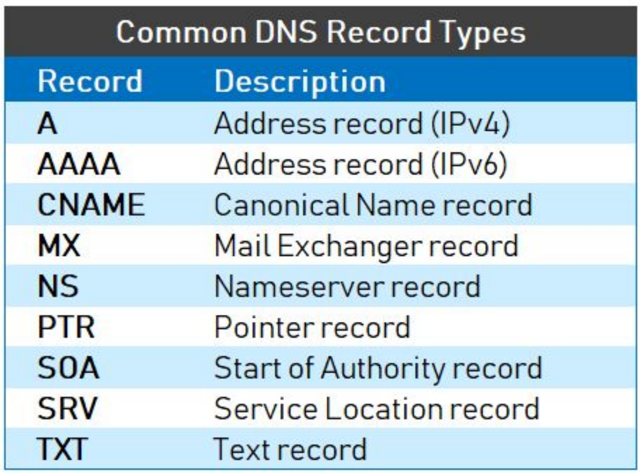
Sometimes DNS records point to subdomains that are reused for other functions.

Tool:

dnsx (https://github.com/projectdiscovery/dnsx)



```
dnsx -retry 3 -a -aaaa -cname -ns -ptr -mx -soa -resp -silent -l subs.txt
hackerone.com [104.16.100.52]
hackerone.com [104.16.99.52]
hackerone.com [2606:4700::6810:6434]
hackerone.com [2606:4700::6810:6334]
hackerone.com [aspmx2.googlemail.com]
hackerone.com [aspmx.l.google.com]
hackerone.com [alt2.aspmx.l.google.com]
hackerone.com [alt1.aspmx.l.google.com]
hackerone.com [aspmx3.googlemail.com]
hackerone.com [a.ns.hackerone.com]
hackerone.com [b.ns.hackerone.com]
hackerone.com [a.ns.hackerone.com]
hackerone.com [dns.cloudflare.com]
```



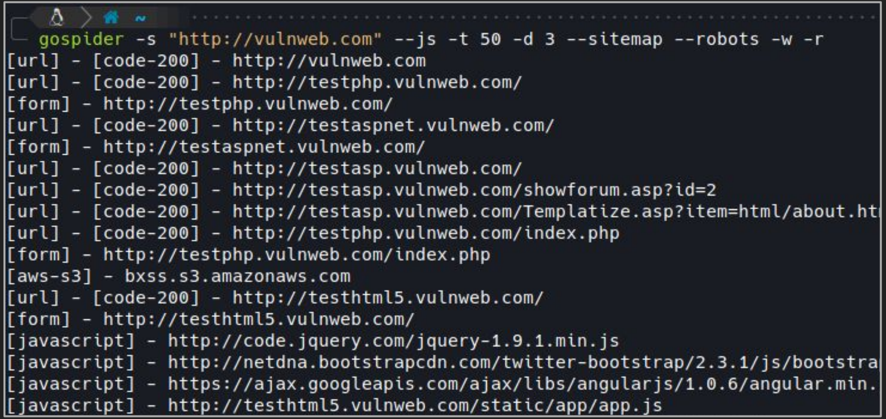
Common DNS Record Types

Record	Description
A	Address record (IPv4)
AAAA	Address record (IPv6)
CNAME	Canonical Name record
MX	Mail Exchanger record
NS	Nameserver record
PTR	Pointer record
SOA	Start of Authority record
SRV	Service Location record
TXT	Text record

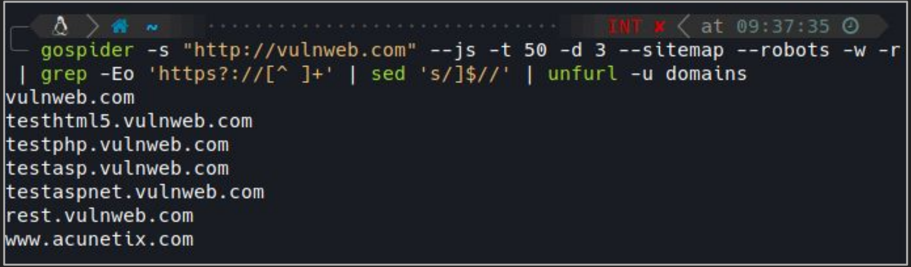
CRAWLING

Goal: collect from the source code of the subdomains that resolve to web services.

- Web solver: httpx (https://github.com/projectdiscovery/httpx)
- Crawler: gospider (https://github.com/jaeles-project/gospider)
- Filtering: unfurl (https://github.com/tomnomnom/unfurl)



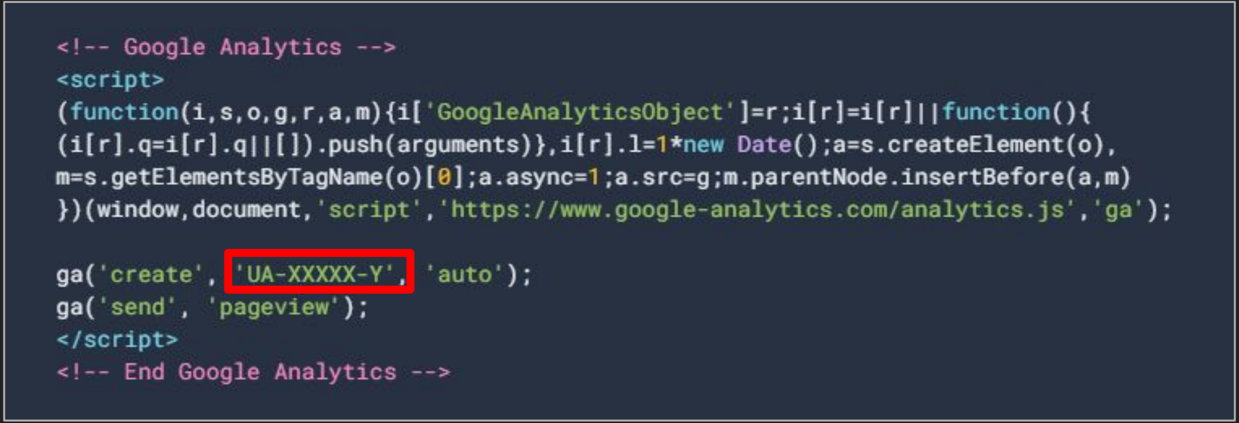
```
gospider -s "http://vulnweb.com" --js -t 50 -d 3 --sitemap --robots -w -r
[url] - [code-200] - http://vulnweb.com
[url] - [code-200] - http://testphp.vulnweb.com/
[form] - http://testphp.vulnweb.com/
[url] - [code-200] - http://testaspnet.vulnweb.com/
[form] - http://testaspnet.vulnweb.com/
[url] - [code-200] - http://testasp.vulnweb.com/
[url] - [code-200] - http://testasp.vulnweb.com/showforum.asp?id=2
[url] - [code-200] - http://testasp.vulnweb.com/Templatize.asp?item=html/about.ht
[url] - [code-200] - http://testphp.vulnweb.com/index.php
[form] - http://testphp.vulnweb.com/index.php
[aws-s3] - bxss.s3.amazonaws.com
[url] - [code-200] - http://testhtml5.vulnweb.com/
[form] - http://testhtml5.vulnweb.com/
[javascript] - http://code.jquery.com/jquery-1.9.1.min.js
[javascript] - http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/js/bootstra
[javascript] - https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.
[javascript] - http://testhtml5.vulnweb.com/static/app/app.js
```



```
gospider -s "http://vulnweb.com" --js -t 50 -d 3 --sitemap --robots -w -r
 | grep -Eo 'https?://[^ ]+' | sed 's/]$//' | unfurl -u domains
vulnweb.com
testhtml5.vulnweb.com
testphp.vulnweb.com
testasp.vulnweb.com
testaspnet.vulnweb.com
rest.vulnweb.com
www.acunetix.com
```

ANALYTICS ID

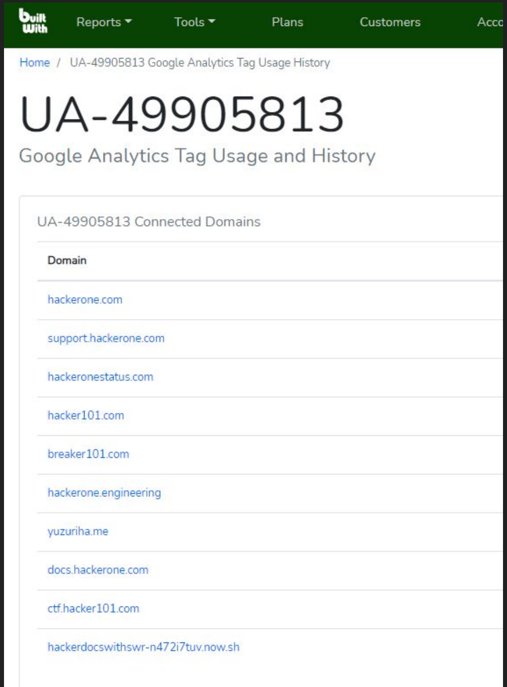
- Google service to get site usage statistics
- Common identifier for sites of the same owner
- Present in the JS of the page
- Available services: BuiltWith and hackertarget.com
- Tool: analyticsRelationships (https://github.com/Josue87/AnalyticsRelationships)



```
<!-- Google Analytics -->
<script>
(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){
(i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o),
m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m)
})(window,document,'script','https://www.google-analytics.com/analytics.js','ga');

ga('create', 'UA-XXXXX-Y', 'auto');
ga('send', 'pageview');
</script>
<!-- End Google Analytics -->
```

ANALYTICS ID: Sources and Tools

BuiltWith



Home / UA-49905813 Google Analytics Tag Usage History

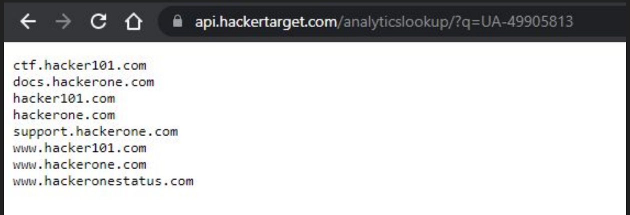
UA-49905813

Google Analytics Tag Usage and History

UA-49905813 Connected Domains

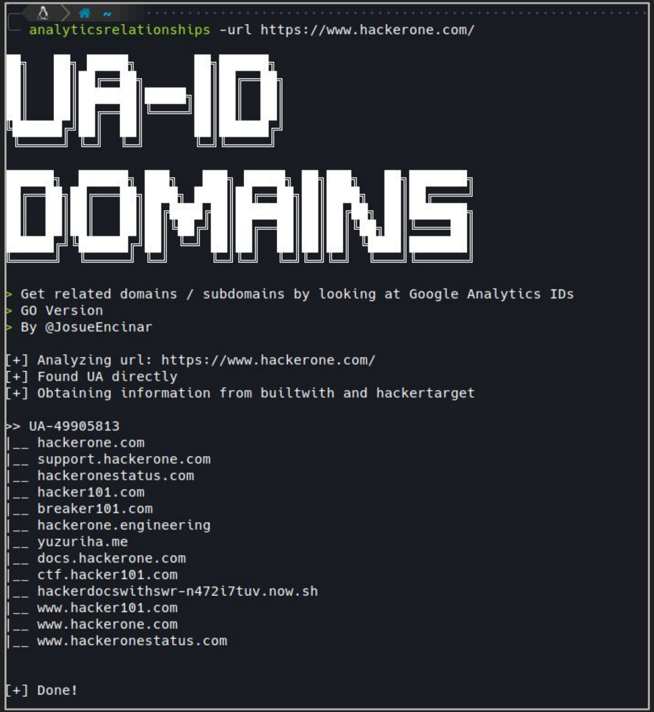
Domain
hackerone.com
support.hackerone.com
hackeronestatus.com
hacker101.com
breaker101.com
hackerone.engineering
yuzuriha.me
docs.hackerone.com
ctf.hacker101.com
hackerdocswithswr-n472i7tuv.now.sh

hackertarget



```
ctf.hacker101.com
docs.hackerone.com
hacker101.com
hackerone.com
support.hackerone.com
www.hacker101.com
www.hackerone.com
www.hackeronestatus.com
```

analyticsRelationships

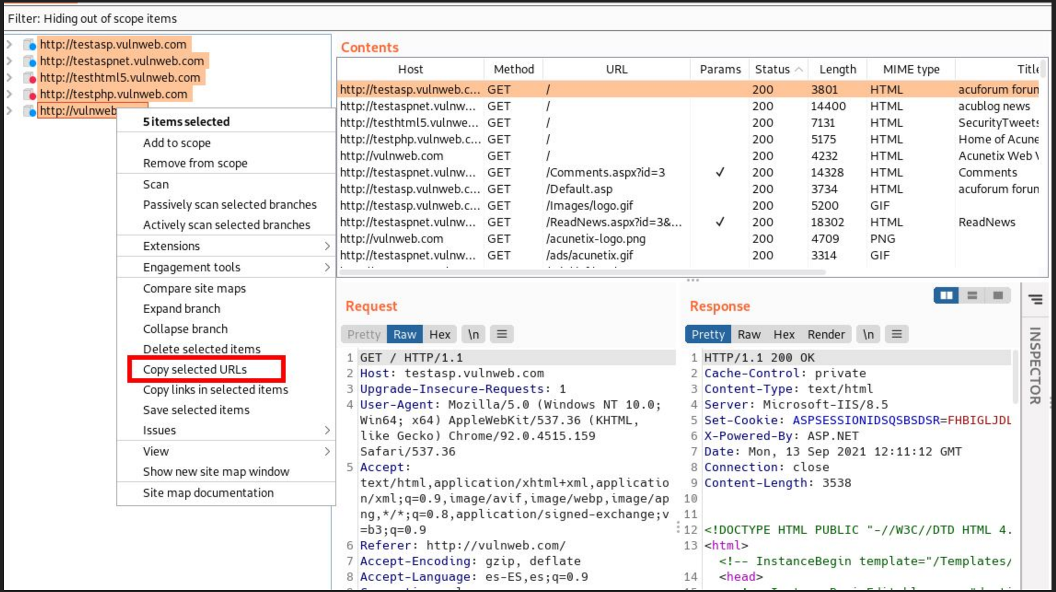


```
analyticsrelationships -url https://www.hackerone.com/

UA-ID
DOMAINS

> Get related domains / subdomains by looking at Google Analytics IDs
> GO Version
> By @JosueEncinar

[+] Analyzing url: https://www.hackerone.com/
[+] Found UA directly
[+] Obtaining information from builtwith and hackertarget

>> UA-49905813
|__ hackerone.com
|__ support.hackerone.com
|__ hackeronestatus.com
|__ hacker101.com
|__ breaker101.com
|__ hackerone.engineering
|__ yuzuriha.me
|__ docs.hackerone.com
|__ ctf.hacker101.com
|__ hackerdocswithswr-n472i7tuv.now.sh
|__ www.hacker101.com
|__ www.hackerone.com
|__ www.hackeronestatus.com


[+] Done!
```

BURP SUITE

Navigation → Collection

Tool: unfurl (https://github.com/tomnomnom/unfurl)



Filter: Hiding out of scope items

Contents

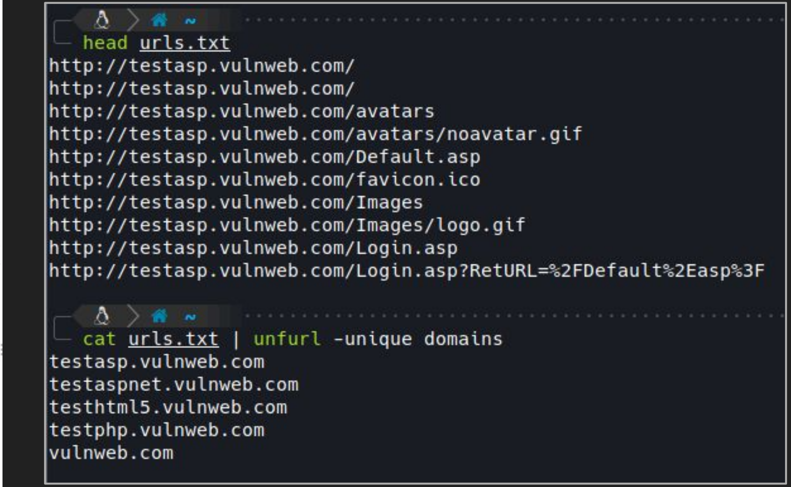
Host	Method	URL	Params	Status	Length	MIME type	Title
http://testasp.vulnweb.c...	GET	/		200	3801	HTML	acuforum forun
http://testaspnet.vulnw...	GET	/		200	14400	HTML	acublog news
http://testhtml5.vulnwe...	GET	/		200	7131	HTML	SecurityTweet:
http://testphp.vulnweb.c...	GET	/		200	5175	HTML	Home of Acune
http://vulnweb.com	GET	/		200	4232	HTML	Acunetix Web \
http://testaspnet.vulnw...	GET	/Comments.aspx?id=3	✓	200	14328	HTML	Comments
http://testasp.vulnweb.c...	GET	/Default.asp		200	3734	HTML	acuforum forun
http://testasp.vulnweb.c...	GET	/Images/logo.gif		200	5200	GIF	
http://testaspnet.vulnw...	GET	/ReadNews.aspx?id=3&...	✓	200	18302	HTML	ReadNews
http://vulnweb.com	GET	/acunetix-logo.png		200	4709	PNG	
http://testaspnet.vulnw...	GET	/ads/acunetix.gif		200	3314	GIF	

Request

```
GET / HTTP/1.1
Host: testasp.vulnweb.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/92.0.4515.159
Safari/537.36
Accept:
text/html,application/xhtml+xml,applicatio
n/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v
=b3;q=0.9
Referer: http://vulnweb.com/
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9
```

Response

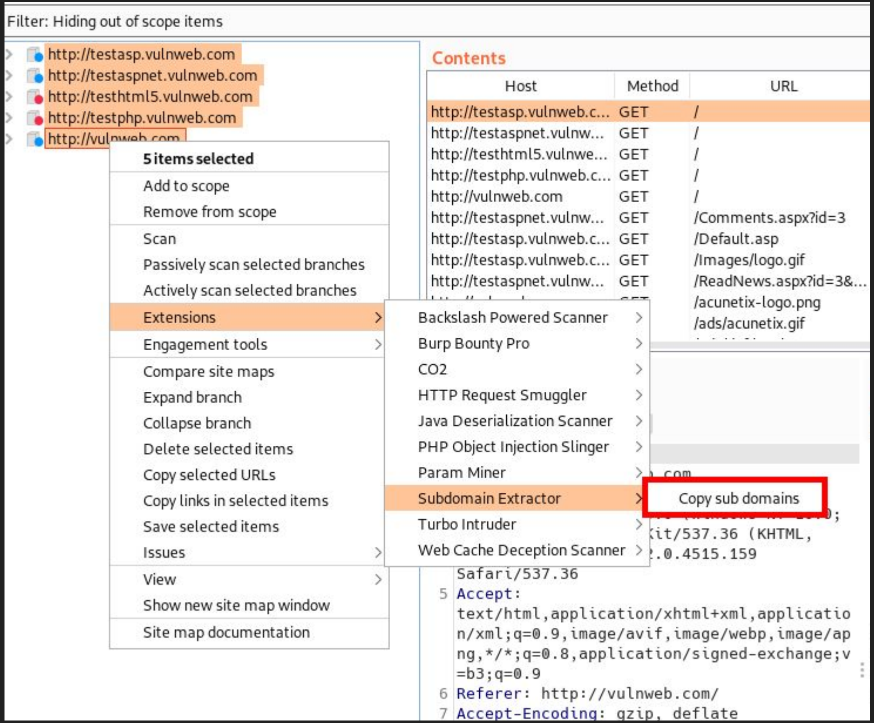
```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html
Server: Microsoft-IIS/8.5
Set-Cookie: ASPSESSIONIDSQSBSDSR=FHBIGLJDL
X-Powered-By: ASP.NET
Date: Mon, 13 Sep 2021 12:11:12 GMT
Connection: close
Content-Length: 3538


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.
<html>
  <!-- InstanceBegin template="/Templates/
  <head>
```



```
head urls.txt
http://testasp.vulnweb.com/
http://testasp.vulnweb.com/
http://testasp.vulnweb.com/avatars
http://testasp.vulnweb.com/avatars/noavatar.gif
http://testasp.vulnweb.com/Default.asp
http://testasp.vulnweb.com/favicon.ico
http://testasp.vulnweb.com/Images
http://testasp.vulnweb.com/Images/logo.gif
http://testasp.vulnweb.com/Login.asp
http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F

cat urls.txt | unfurl -unique domains
testasp.vulnweb.com
testaspnet.vulnweb.com
testhtml5.vulnweb.com
testphp.vulnweb.com
vulnweb.com
```

BURP SUITE

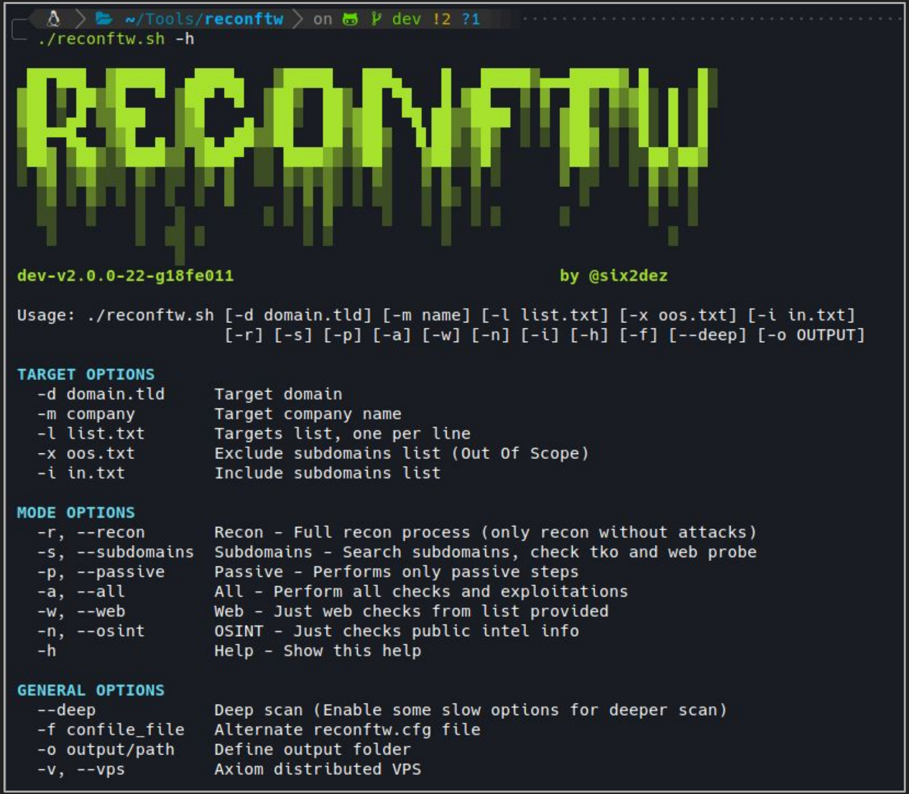
Extension: Subdomain Extractor (https://github.com/portswigger/burp-subdomain)



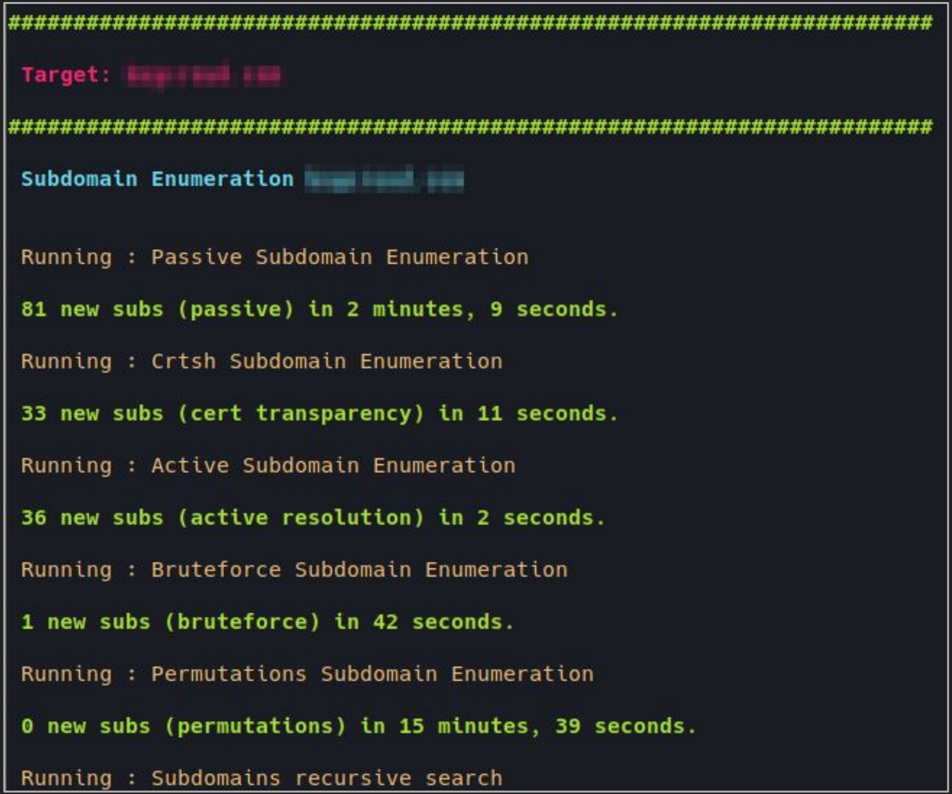
Host	Method	URL
http://testasp.vulnweb.c...	GET	/
http://testaspnet.vulnw...	GET	/
http://testhtml5.vulnwe...	GET	/
http://testphp.vulnweb.c...	GET	/
http://vulnweb.com	GET	/
http://testaspnet.vulnw...	GET	/Comments.aspx?id=3
http://testasp.vulnweb.c...	GET	/Default.asp
http://testasp.vulnweb.c...	GET	/Images/logo.gif
http://testaspnet.vulnw...	GET	/ReadNews.aspx?id=3&...
		/acunetix-logo.png
		/ads/acunetix.gif

```
.com
0;
it/537.36 (KHTML,
.0.4515.159
Safari/537.36
Accept:
text/html,application/xhtml+xml,applicatio
n/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v
=b3;q=0.9
Referer: http://vulnweb.com/
Accept-Encoding: gzip, deflate
```

reconFTW



```
~/Tools/reconftw on dev !2 ?1
./reconftw.sh -h

dev-v2.0.0-22-g18fe011                                    by @six2dez

Usage: ./reconftw.sh [-d domain.tld] [-m name] [-l list.txt] [-x oos.txt] [-i in.txt]
                     [-r] [-s] [-p] [-a] [-w] [-n] [-i] [-h] [-f] [--deep] [-o OUTPUT]

TARGET OPTIONS
  -d domain.tld     Target domain
  -m company        Target company name
  -l list.txt       Targets list, one per line
  -x oos.txt        Exclude subdomains list (Out Of Scope)
  -i in.txt         Include subdomains list

MODE OPTIONS
  -r, --recon       Recon - Full recon process (only recon without attacks)
  -s, --subdomains  Subdomains - Search subdomains, check tko and web probe
  -p, --passive     Passive - Performs only passive steps
  -a, --all         All - Perform all checks and exploitations
  -w, --web         Web - Just web checks from list provided
  -n, --osint       OSINT - Just checks public intel info
  -h                Help - Show this help

GENERAL OPTIONS
  --deep            Deep scan (Enable some slow options for deeper scan)
  -f confile_file   Alternate reconftw.cfg file
  -o output/path    Define output folder
  -v, --vps         Axiom distributed VPS
```



```
###############################################################

Target: [redacted]

###############################################################

Subdomain Enumeration [redacted]


Running : Passive Subdomain Enumeration

81 new subs (passive) in 2 minutes, 9 seconds.

Running : Crtsh Subdomain Enumeration

33 new subs (cert transparency) in 11 seconds.

Running : Active Subdomain Enumeration

36 new subs (active resolution) in 2 seconds.

Running : Bruteforce Subdomain Enumeration

1 new subs (bruteforce) in 42 seconds.

Running : Permutations Subdomain Enumeration

0 new subs (permutations) in 15 minutes, 39 seconds.

Running : Subdomains recursive search
```

References

https://github.com/OWASP/Amass

https://github.com/projectdiscovery/subfinder

https://github.com/tomnomnom/assetfinder

https://github.com/Findomain/Findomain

https://github.com/cgboal/sonarsearch

https://github.com/bp0lr/gauplus

https://github.com/tomnomnom/waybackurls

https://github.com/eslam3kl/crtfinder

https://github.com/projectdiscovery/dnsx

https://github.com/UnaPibaGeek/ctfr

https://github.com/A3h1nt/Subcert

https://github.com/AnikHasibul/crtscan

https://github.com/d3mondev/puredns

https://github.com/projectdiscovery/shuffledns

https://github.com/vortexau/dnsvalidator

https://github.com/Josue87/gotator

https://github.com/projectdiscovery/httpx

https://github.com/jaeles-project/gospider

https://github.com/tomnomnom/unfurl

https://github.com/Josue87/AnalyticsRelationships

https://github.com/lc/gau

https://github.com/portswigger/burp-subdomain

https://github.com/six2dez/reconftw

Thanks :)