Bug Bounty Recon The “Right” Way

Is it really right? - Bsides Budapest 2022

Khalil Abdellah Lemtaffah

Whoami?

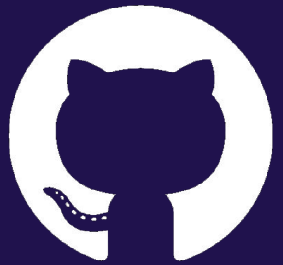
- Student, BSc Holder of Networks, Security and Computer Systems
- Following a Cybersecurity MSc - ELTE University
- Student Software Developer - ERICSSON
- Head of the Cybersecurity Club ECSC - ELTE University
- Hunter on Hackerone and Synack Red Team

Understand. The. Organization.

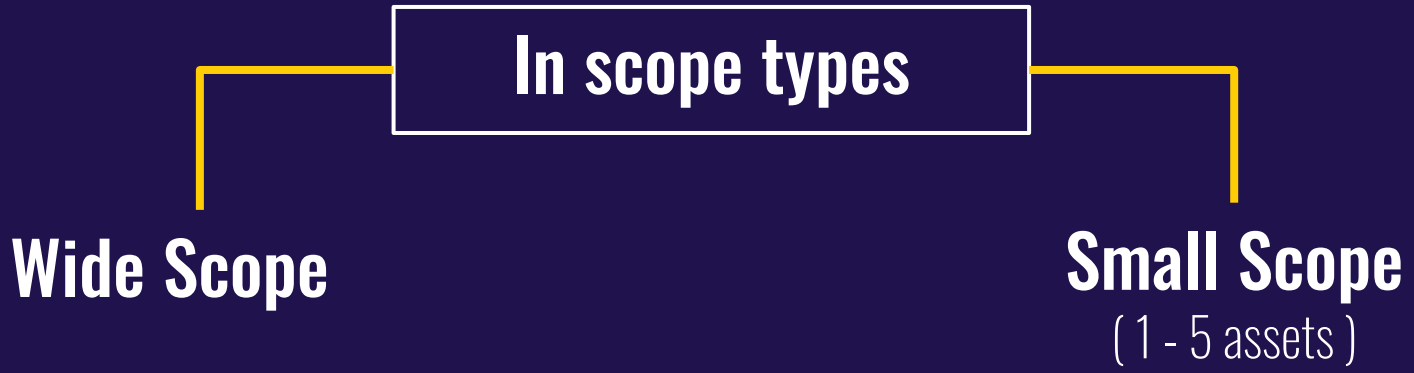
Ask yourself questions:

- Who is this company?
- Whom it's working with?
- Where is it located? (Important)
- Have I used its applications before?
- ...

Recon



More assets = bigger recon surface

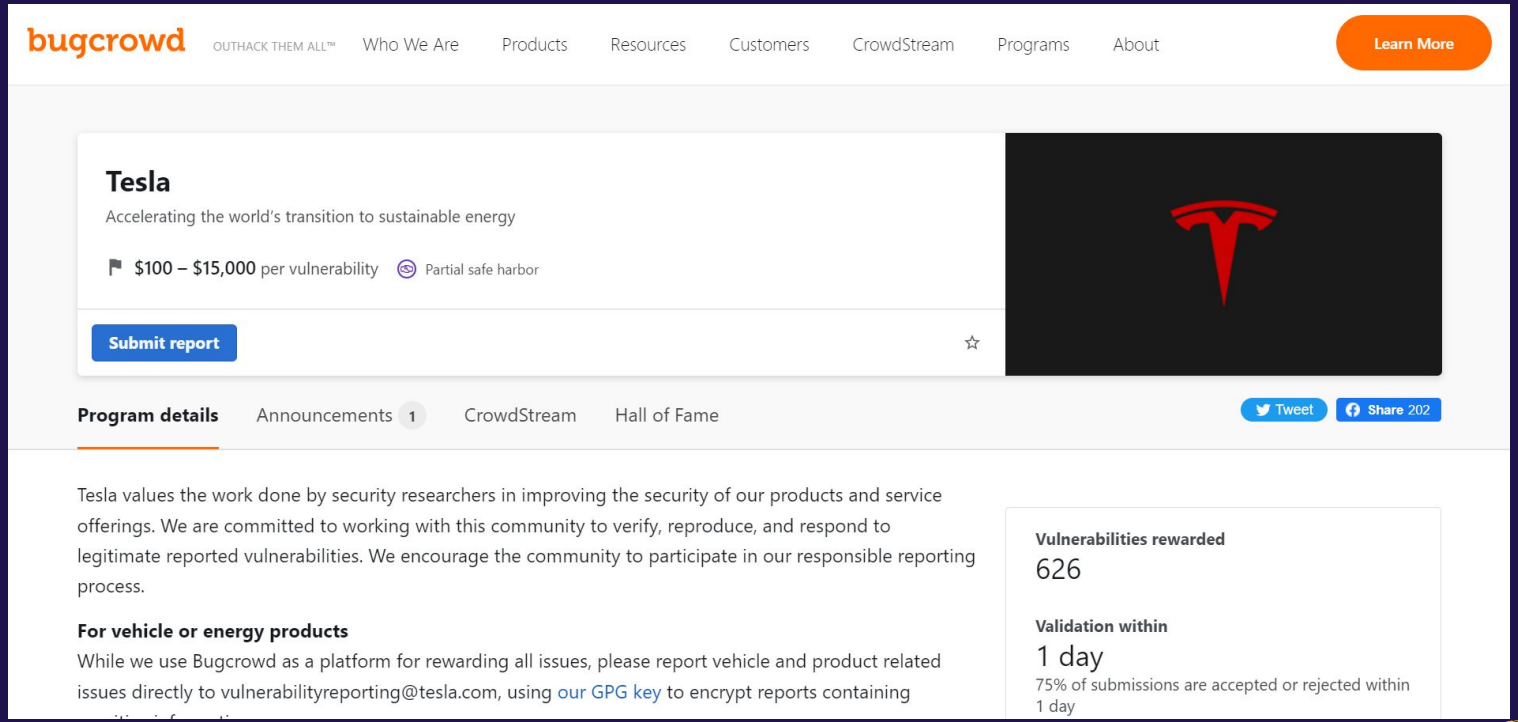

In scope types
Wide Scope
Small Scope
(1 - 5 assets)

Wide Scope

Recon - Wide Scope

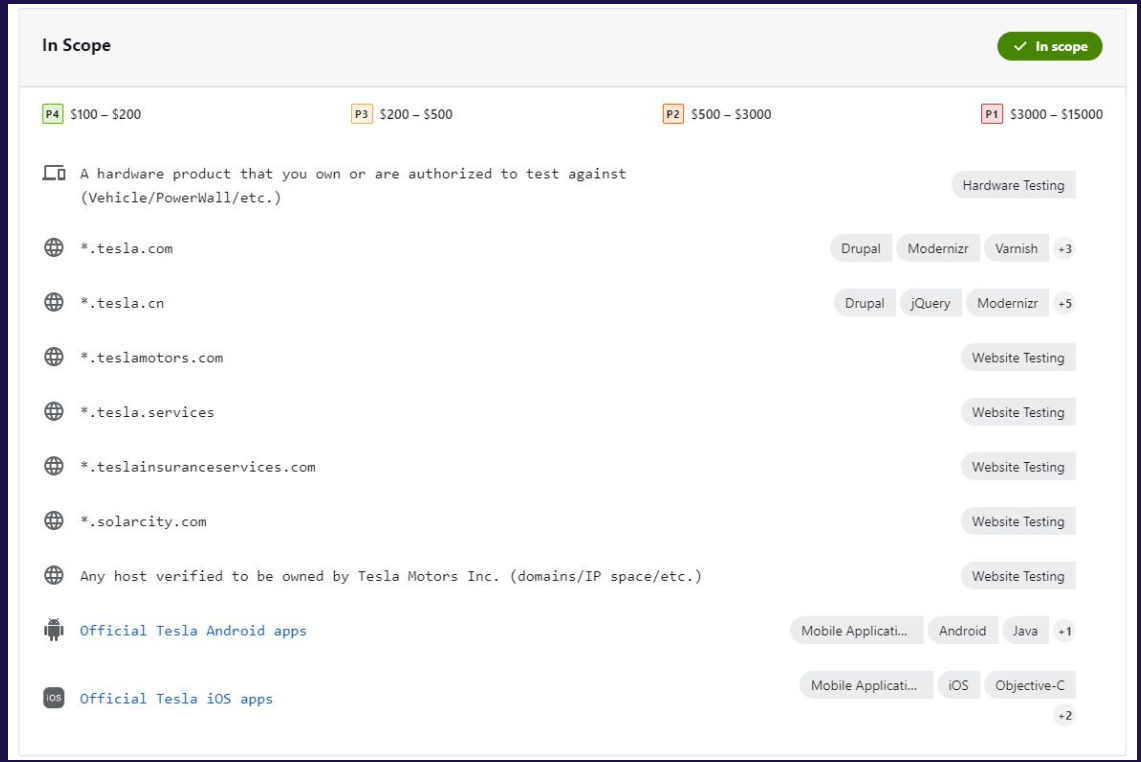
- *.target.TLD
- CIDR
- Mobile apps
- Cars
- Hardware

Example: Tesla



Recon - Wide Scope

Example: Tesla



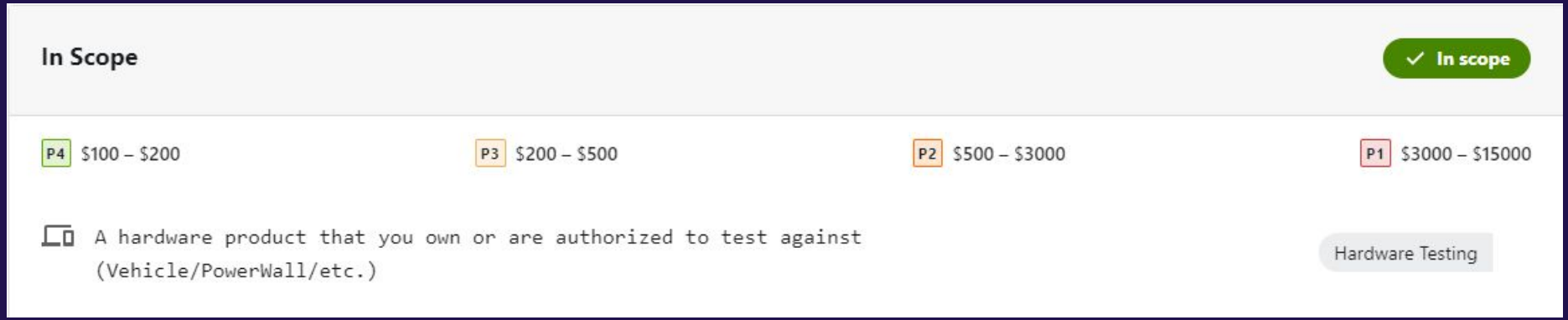
In Scope

In scope

P4 $100 – $200 | P3 $200 – $500 | P2 $500 – $3000 | P1 $3000 – $15000

A hardware product that you own or are authorized to test against (Vehicle/PowerWall/etc.)	Hardware Testing
*.tesla.com	Drupal, Modernizr, Varnish, +3
*.tesla.cn	Drupal, jQuery, Modernizr, +5
*.teslamotors.com	Website Testing
*.tesla.services	Website Testing
*.teslainsuranceservices.com	Website Testing
*.solarcity.com	Website Testing
Any host verified to be owned by Tesla Motors Inc. (domains/IP space/etc.)	Website Testing
Official Tesla Android apps	Mobile Applicati..., Android, Java, +1
Official Tesla iOS apps	Mobile Applicati..., iOS, Objective-C, +2

Example: Tesla



Recon - Wide Scope

Example: Tesla

*.tesla.com	Drupal, Modernizr, Varnish, +3
*.tesla.cn	Drupal, jQuery, Modernizr, +5
*.teslamotors.com	Website Testing
*.tesla.services	Website Testing
*.teslainsuranceservices.com	Website Testing
*.solarcity.com	Website Testing
Any host verified to be owned by Tesla Motors Inc. (domains/IP space/etc.)	Website Testing

Recon - Wide Scope

Example: Tesla

Small Scope

- **Same Story, limited attack surface**
- **Different approach** - Automation might not be useful here...

Tips and Mindset

➔ Checkout the origin of the company

Netherlands based?
Subdomain bruteforcing based on dutch wordlist

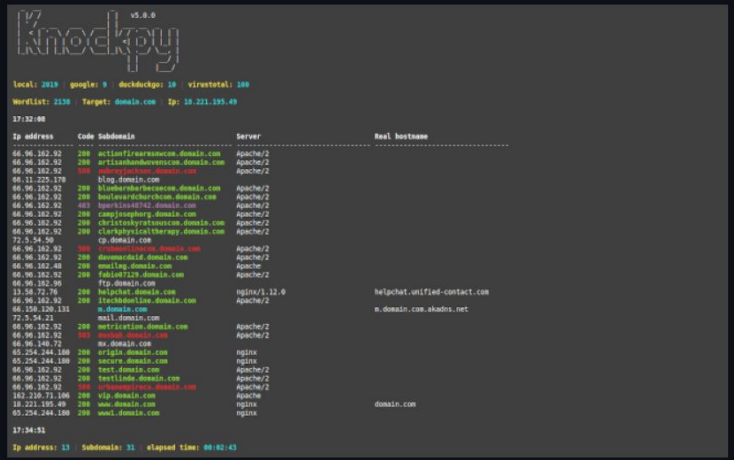
It is recommended to use this method after gathering subdomains with other tools and general wordlists!

Tips and Mindset - Country based subs

README.md

Knock Subdomain Scan v5.3.0

Knockpy is a python3 tool designed to quickly enumerate subdomains on a target domain through dictionary attack.



Very simply

```
python3 knockpy.py domain.com
```

Packages

No packages published

Contributors 7

Languages

Python 100.0%

Tips and Mindset - Country based subs

aem2.txt	Create aem2.txt	8 months ago
apache.txt	Add balancer for apache	13 months ago
axis.txt	standardisze line endings	2 years ago
big.txt	adding "dismiss" to big.txt	9 months ago
burp-parameter-names.txt	Sync with param-miner master repo	26 days ago
coldfusion.txt	standardisze line endings	2 years ago
combined_directories.txt	[Github Action] Updated combined_directories.txt	10 days ago
combined_words.txt	[Github Action] Updated combined_words.txt	10 days ago
common-and-dutch.txt	rename 's/_/-/g'	5 years ago
common-and-french.txt	rename 's/_/-/g'	5 years ago
common-and-italian.txt	rename 's/_/-/g'	5 years ago
common-and-portuguese.txt	renamed to correct name	2 years ago
common-and-spanish.txt	rename 's/_/-/g'	5 years ago
common-api-endpoints-mazen160.txt	Add "-" to split up words, moved files since PR accepted	4 years ago
common.txt	Add Hangfire console	16 days ago
confluence-administration.txt	Close #195 - Confluence administration	4 years ago
default-web-root-directory-linux.txt	Quick move about	4 years ago
default-web-root-directory-windows.txt	Quick move about	4 years ago
directory-list-1.0.txt	Discovery: Fix spelling and hyphenate some words	14 months ago

Tips and Mindset - Country based subs


```
splintersec@localhost:~$ knockpy volkskrant.nl

 _  __                  _
| |/ /                  | |   v5.3.0
| ' / _ __   ___   ___ | | ___ __  _   _
|  < | '_ \ / _ \ / __| |/ / '_ \| | | |
| . \| | | | (_) | (__|   <| |_) | |_| |
|_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                           | |     __/ |
                           |_|    |___/

local: 10757 | google: 0 | duckduckgo: 5 | virustotal: 0

Wordlist: 10762 | Target: volkskrant.nl | Ip: 23.213.161.225

23:02:36

Ip address      Code Subdomain                          Server                              Real hostname
--------------- ---- ---------------------------------- ----------------------------------- -----------------------------------
52.49.16.186    200  accounts.volkskrant.nl                                                 lb.eu1.gigya.com
23.213.161.215  406  account.volkskrant.nl              AkamaiGHost                         e123360.dscb.akamaiedge.net
23.213.161.225  200  beta.volkskrant.nl                                                     e15645.dscb.akamaiedge.net
23.213.161.225  200  brandedcontent.volkskrant.nl       Apache                              e15645.dscb.akamaiedge.net
146.185.53.23   200  blogs.volkskrant.nl                                                    dpp-public-cl21.persgroep-ops.net
146.185.53.23   200  blog.volkskrant.nl                                                     dpp-public-cl21.persgroep-ops.net
13.32.121.43    403  cmp.volkskrant.nl                  AmazonS3                            cdn-1294.privacy-mgmt.com
23.213.161.201  404  esales.volkskrant.nl               nginx/1.20.0                        e15410.dscb.akamaiedge.net
146.185.53.23   200  feeds.volkskrant.nl                                                    dpp-public-cl21.persgroep-ops.net
23.213.161.225  403  ims.volkskrant.nl                                                      e15462.dscb.akamaiedge.net
37.97.223.87    200  labs.volkskrant.nl
23.213.161.201  406  login.volkskrant.nl                AkamaiGHost                         e15410.dscb.akamaiedge.net
23.213.161.210  406  login2.volkskrant.nl               AkamaiGHost                         e15410.dscb.akamaiedge.net
146.185.53.23   200  m.volkskrant.nl                                                        dpp-public-cl21.persgroep-ops.net
23.213.161.210  503  mijn.volkskrant.nl                                                     e15410.dscb.akamaiedge.net
23.213.161.225  200  mobile.volkskrant.nl                                                   e15645.dscb.akamaiedge.net
23.213.161.199  200  myaccount.volkskrant.nl                                                e15454.dscb.akamaiedge.net
```

Normal subdomain bruteforce

Tips and Mindset - Country based subs


```
splintersec@localhost:~$ knockpy -w tmp/dutch.txt volkskrant.nl

 _  __                  _
| |/ /                  | |   v5.3.0
| ' / _ __   ___   ___| | ___ __  _   _
|  < | '_ \ / _ \ / __| |/ / '_ \| | | |
| . \| | | | (_) | (__|   <| |_) | |_| |
|_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                           | |     __/ |
                           |_|    |___/

local: 413777 | google: 0 | duckduckgo: 6 | virustotal: 0

Wordlist: 413783 | Target: volkskrant.nl | Ip: 23.213.161.225

23:19:12

Ip address      Code Subdomain                                                  Server                                                  Real hostname
--------------- ---- ---------------------------------------------------------- ------------------------------------------------------- --------------------
-----------------------------------------
52.17.82.217    200  accounts.volkskrant.nl                                                                                             lb.eu1.gigya.com
23.213.161.226  406  account.volkskrant.nl                                      AkamaiGHost                                             e123360.dscb.akamaie
dge.net
54.38.245.3     404  actie.volkskrant.nl                                        NCSA/1.4.2                                              varnish.qualifio.com
23.213.161.225       advertorial.volkskrant.nl                                                                                          e15645.dscb.akamaied
ge.net
146.185.53.23   200  archief.volkskrant.nl                                                                                              dpp-public-cl21.pers
groep-ops.net
146.185.53.23   200  blog.volkskrant.nl                                                                                                 dpp-public-cl21.pers
groep-ops.net
146.185.53.23   200  blogs.volkskrant.nl                                                                                                dpp-public-cl21.pers
groep-ops.net
23.213.161.212  200  brandedcontent.volkskrant.nl                               Apache                                                  e15645.dscb.akamaied
ge.net
23.67.141.39         caps.volkskrant.nl                                                                                                 e8821.dscb.akamaiedg
e.net
146.185.54.239       dagkrant.volkskrant.nl                                                                                             www5524.persgroep.be
46.30.126.135   200  digitalekrant.volkskrant.nl                                nginx                                                   www.e-pages.dk
23.213.161.201  200  inclusief.volkskrant.nl                                                                                            e15410.dscb.akamaied
ge.net
46.30.126.156   406  krant.volkskrant.nl                                        AkamaiGHost                                             e-pages.pub
37.97.223.87    200  labs.volkskrant.nl
```

Subdomain bruteforce using Dutch wordlist

```
knockpy -w custom_wordlist.txt target.tld
```

@splint3rsec

BSIDES BUDAPEST

Tips and Mindset - Country based subs


```
146.185.53.23    200  verkeer.volkskrant.nl
groep-ops.net
142.93.232.211        verhalen.volkskrant.nl
ng.com
146.185.53.23         verkiezingen.volkskrant.nl
groep-ops.net
2.16.181.34      404  video.volkskrant.nl
edge.net
146.185.53.23    200  vrij.volkskrant.nl
groep-ops.net
185.136.65.7     200  web.volkskrant.nl
185.136.64.7     200  WEB.volkskrant.nl
146.185.53.23    200  weblog.volkskrant.nl
groep-ops.net
146.185.53.23    200  webshop.volkskrant.nl
groep-ops.net
23.213.161.201   200  webwinkel.volkskrant.nl
ge.net
146.185.53.23    200  weer.volkskrant.nl
groep-ops.net
23.213.161.201   200  welkom.volkskrant.nl
ge.net
77.74.48.5            wijnen.volkskrant.nl
l
136.144.155.9    200  wiki.volkskrant.nl

51.124.81.192         Winkel.volkskrant.nl

51.124.81.192         winkel.volkskrant.nl

23.213.161.201   200  www.volkskrant.nl
```

Extra tip: it is recommended to run subdomain enumeration tools on the list of previously gathered subdomains

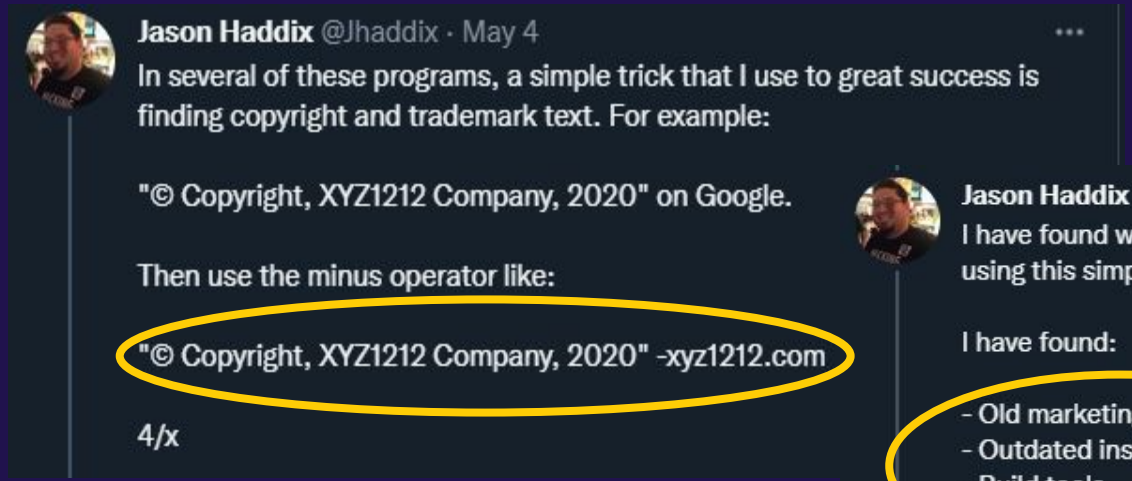
```
subfinder -dL subdomains.txt | httpx
```

It's all about being creative and looking for the right things in the right place.

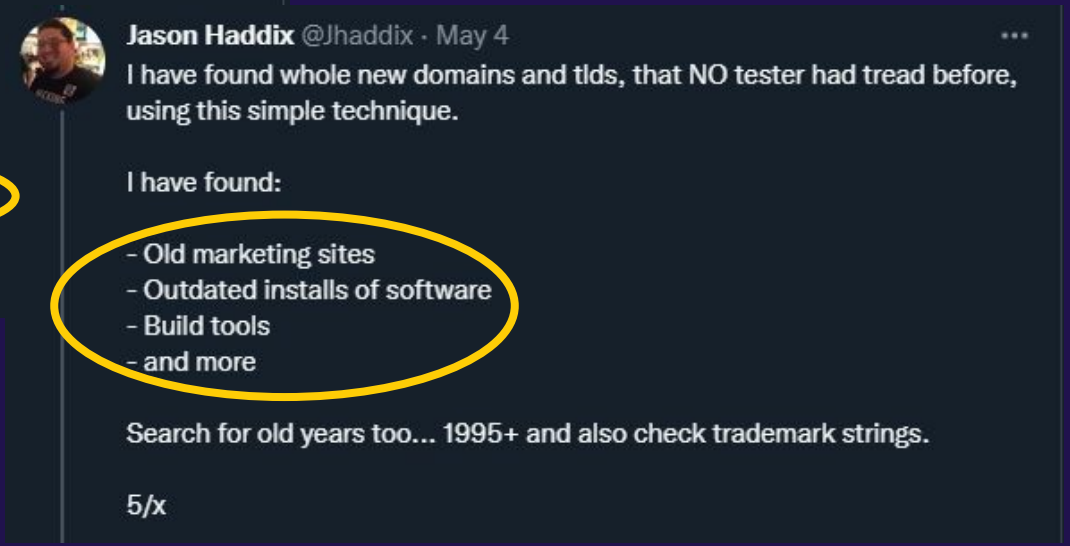
- Trademark/Copyright based recon

  For wide scope targets, including acquisitions..

Tips and Mindset - Copyright recon



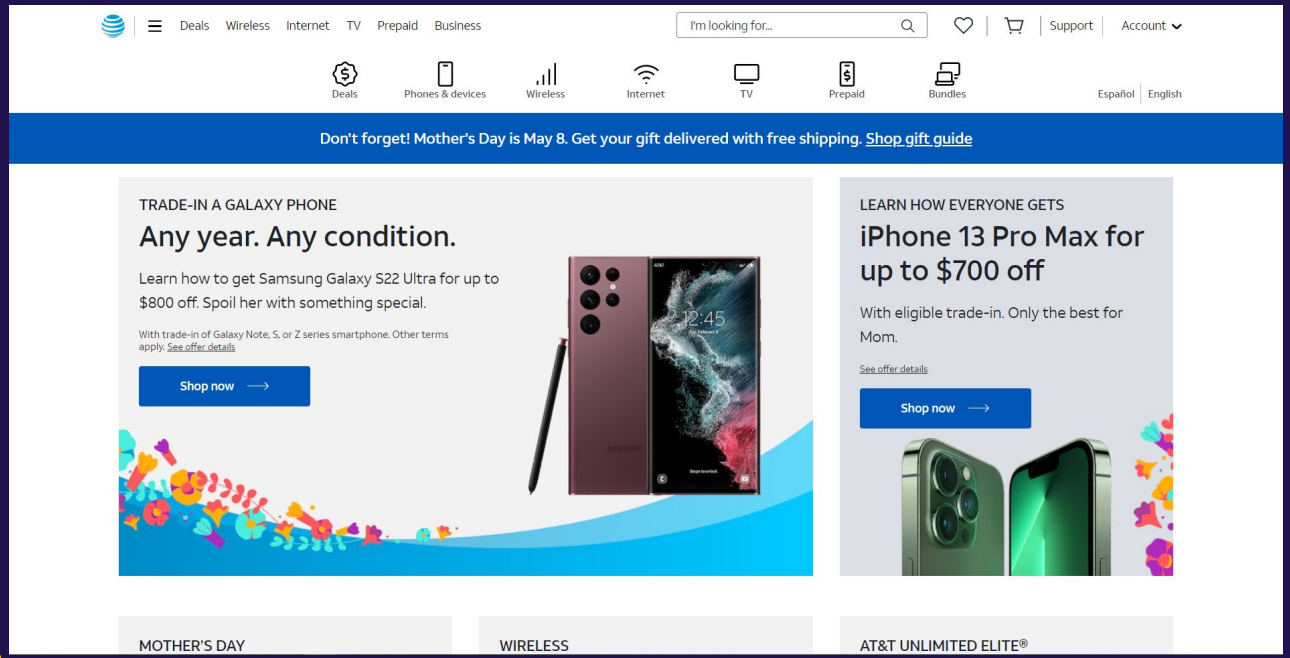
He removes the unwanted websites with the minus sign



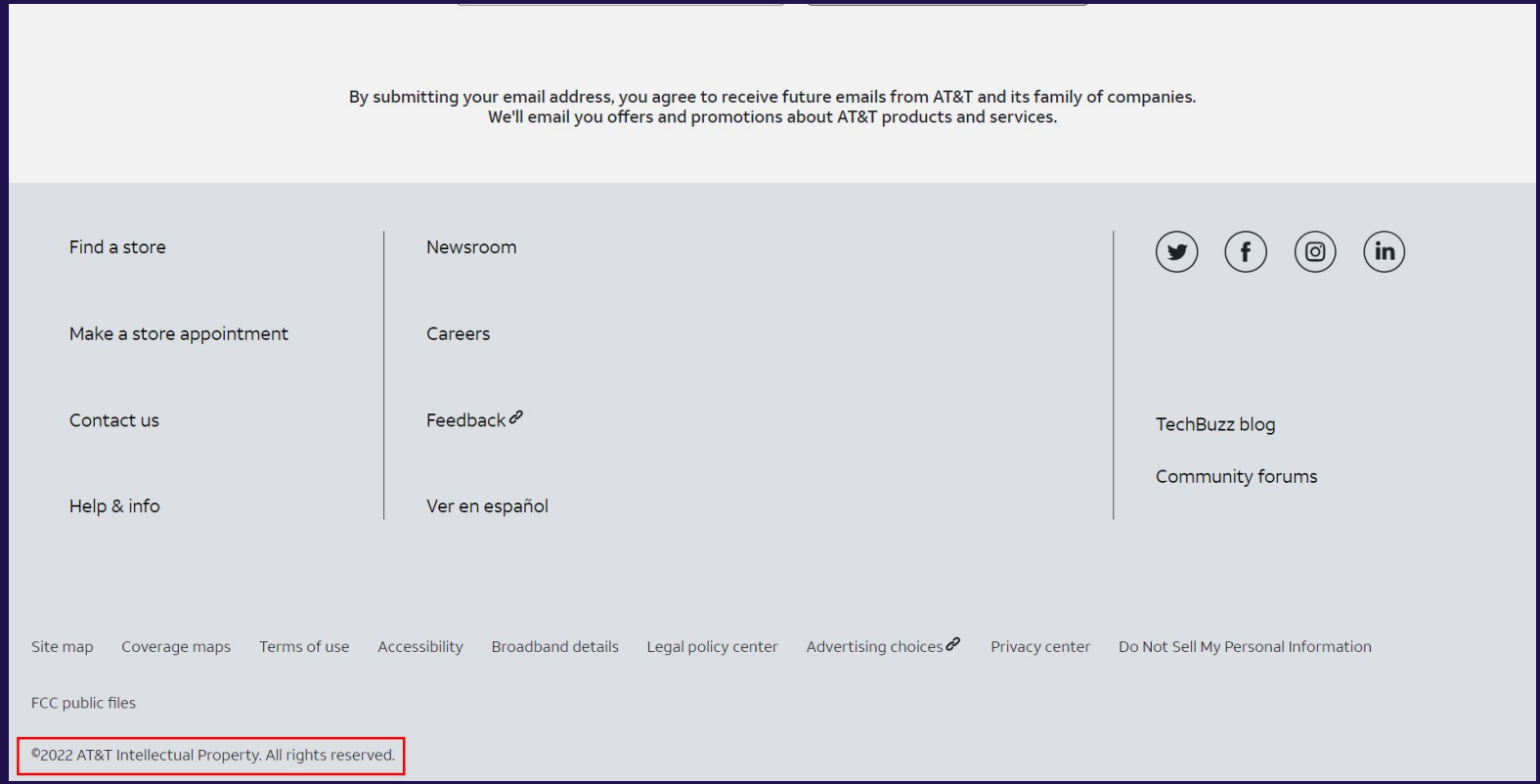
Stuff he found using this dork

Let's look for other domains owned by AT&T using this method

https://www.att.com/



Tips and Mindset - Copyright recon



By submitting your email address, you agree to receive future emails from AT&T and its family of companies.
We'll email you offers and promotions about AT&T products and services.

Find a store
Make a store appointment
Contact us
Help & info

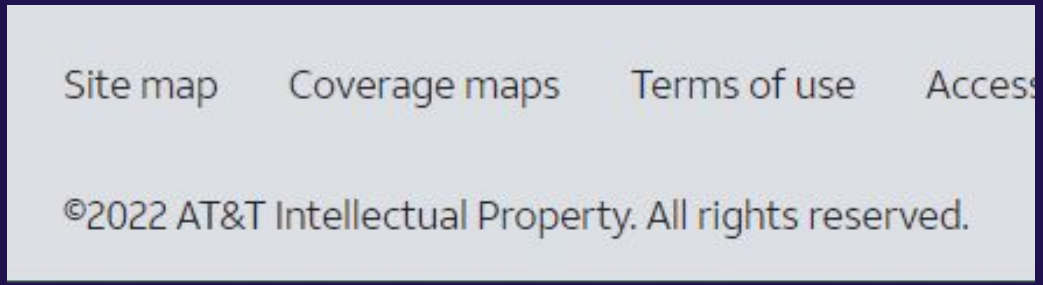
Newsroom
Careers
Feedback
Ver en español

TechBuzz blog
Community forums

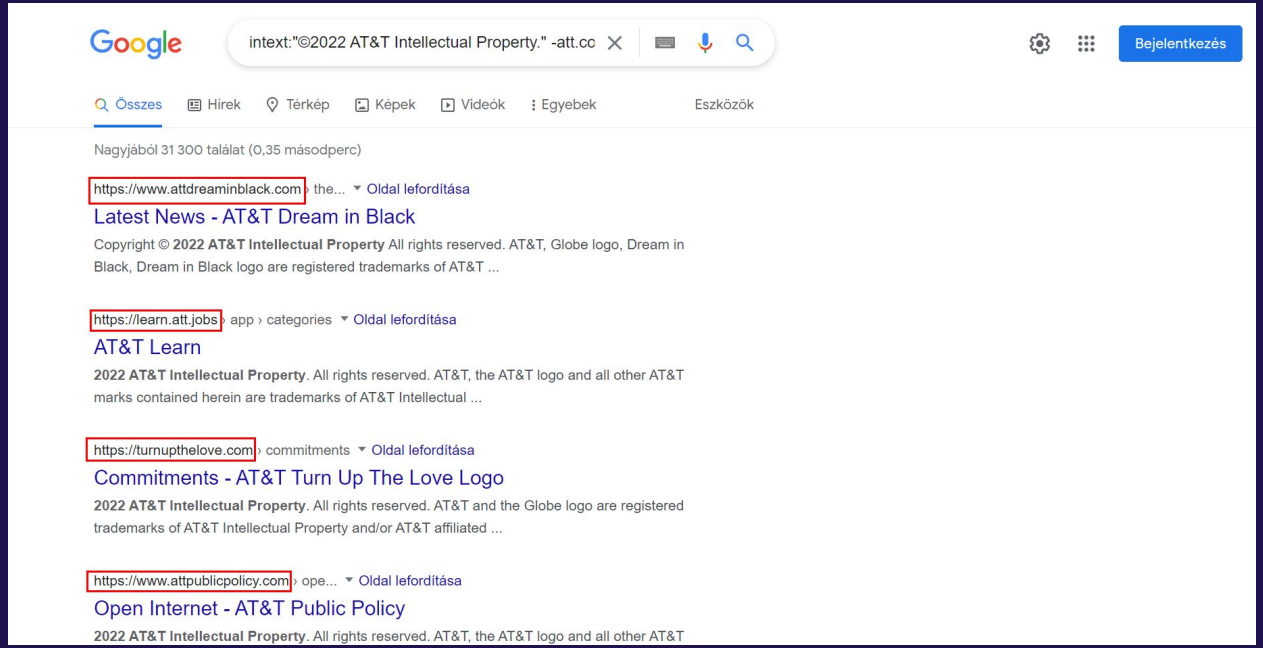
Site map Coverage maps Terms of use Accessibility Broadband details Legal policy center Advertising choices Privacy center Do Not Sell My Personal Information

FCC public files

Now we should find other domains/subdomains that contain the same words



Using google dorks we can find other interesting domains owned by the same company



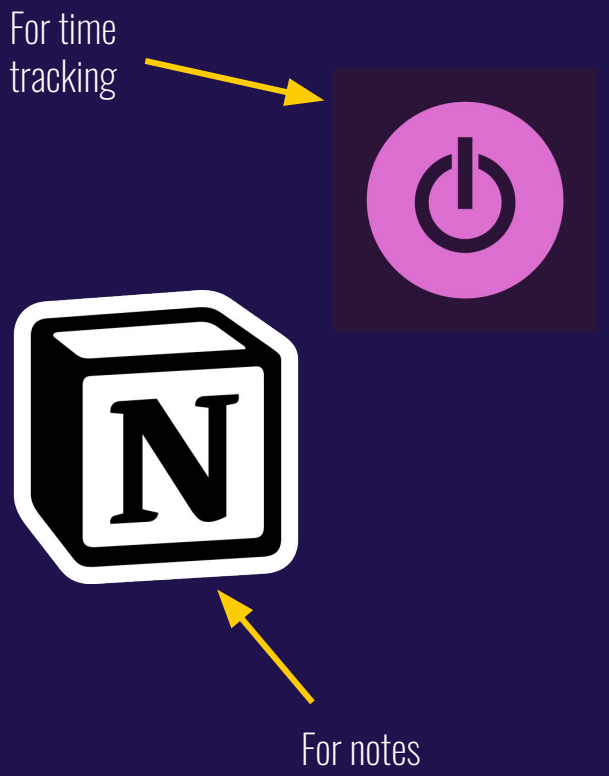
You can also search using older copyright words...

```
Intext:"©2016 at&t intellectual property." -att.com
```

Older copyrights = Older websites = More vulnerabilities

Golden tip:
Always track your progress, note down every small detail and use a time tracker.

You're actually tricking your mind to see the progress and do more!



Set goals:
For example - This month I will hunt for 20 hours and score $2,000 in bounties

20 hours will be 5 hours per week, which is considered relatively low compared to what you can give as an average...

I did the same before this talk, goals:

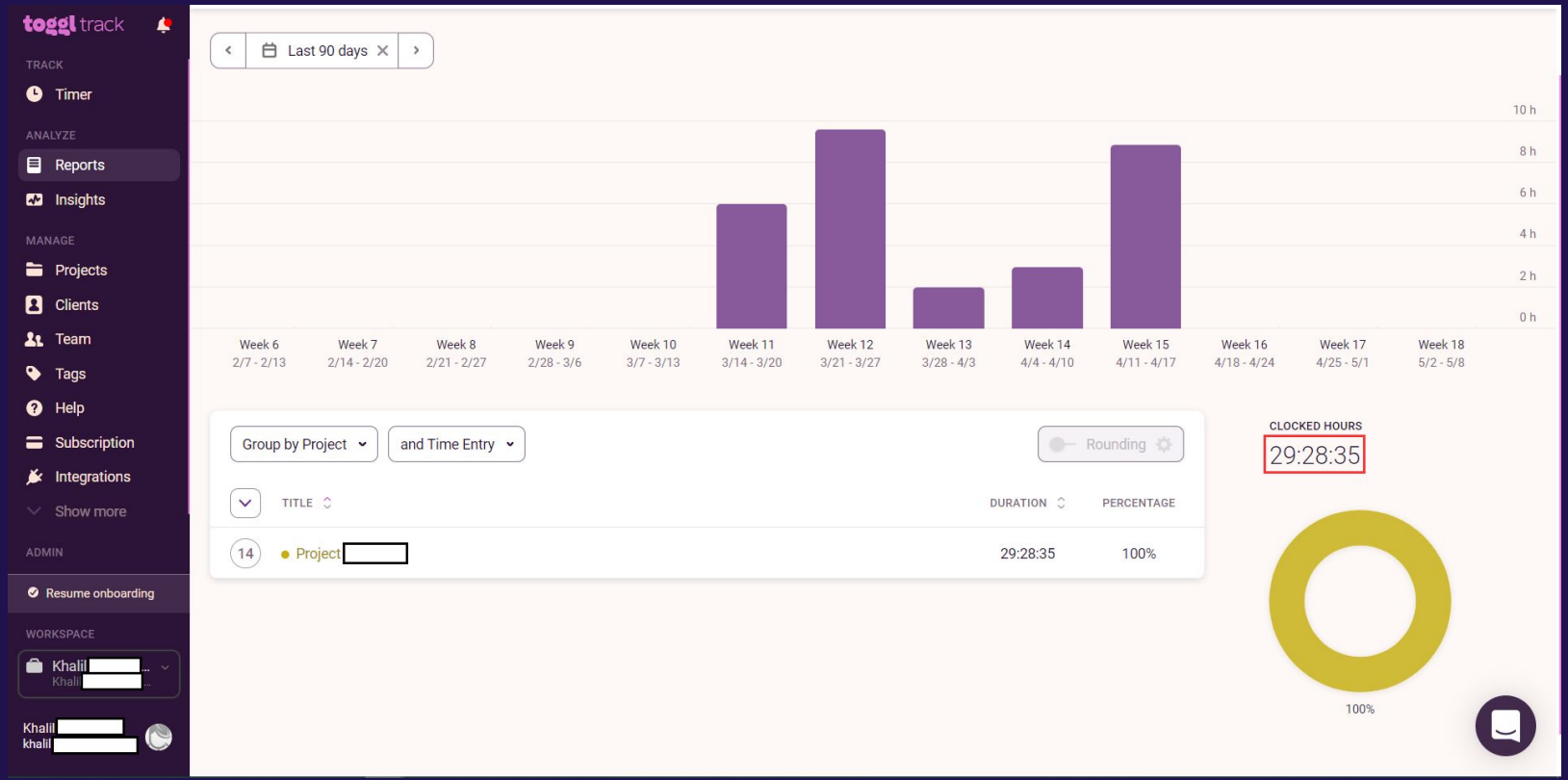
- Pick a program, stick with it
- Minimum 20 hours of hunting
- Minimum $1,000 bounties

- Day 1 - Choose a program
- Day 2 - Setup a VPS + tools
- Day 3 → 8 - Recon and use the app as a normal user
- Day 8 → Day 30 - Hack and Pray
- Notes / takeaways

Rules

- 1 hour hunt on weekdays, 2 hours hunt on weekends
- Continuous hunting, no breaks allowed.
- Stick to only one program, no changing allowed
- If you fail the streak, You have to do something you don't like ⇒ Run 4 hours non stop
- Track your time with Toggl Track
- The challenge starts today (15th of March) and will end on the 15th of April
- Bounties are not allowed to get spent before the final day.

Tips and Mindset - Note taking



Didn't make it to 4 figures

Results:
29:28:35 Time spent + $XXX bounties

Probably I lost the battle, but I know I will win the war 😋

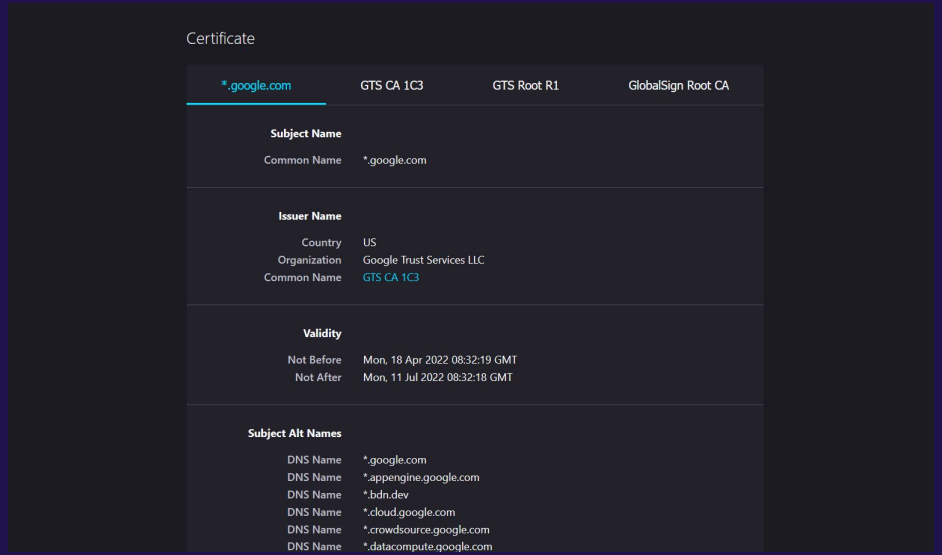
What I actually won from this sprint:

- Cash
- Recon data
- Knowledge
- Made connections with the triagers
- Successfully managed my time in exams period
- ...

"Secret" Subdomain gathering tricks:

Websites use HTTPS → SSL certificates → Subject Alt Names

youtube.com's certificate →



Tips and Mindset - Subject Alt. Names

Subject Alt Names

DNS Name	*.google.com
DNS Name	*.appengine.google.com
DNS Name	*.bdn.dev
DNS Name	*.cloud.google.com
DNS Name	*.crowdsource.google.com
DNS Name	*.datacompute.google.com
DNS Name	*.google.ca
DNS Name	*.google.cl
DNS Name	*.google.co.in
DNS Name	*.google.co.jp
DNS Name	*.google.co.uk
DNS Name	*.google.com.ar
DNS Name	*.google.com.au
DNS Name	*.google.com.br
DNS Name	*.google.com.co
DNS Name	*.google.com.mx
DNS Name	*.google.com.tr
DNS Name	*.google.com.vn
DNS Name	*.google.de
DNS Name	*.google.es
DNS Name	*.google.fr
DNS Name	*.google.hu
DNS Name	*.google.it
DNS Name	*.google.nl
DNS Name	*.google.pl
DNS Name	*.google.pt
DNS Name	*.googleadapis.com
DNS Name	*.googleapis.cn
DNS Name	*.googlevideo.com
DNS Name	*.gstatic.cn

These additional DNS names can help google define multiple hostnames for the same SSL certificate.

DNS Name	*.ytimg.com
DNS Name	android.com
DNS Name	*.android.com
DNS Name	*.flash.android.com
DNS Name	g.cn
DNS Name	*.g.cn
DNS Name	g.co
DNS Name	*.g.co
DNS Name	goo.gl
DNS Name	www.goo.gl
DNS Name	google-analytics.com
DNS Name	*.google-analytics.com
DNS Name	google.com
DNS Name	googlecommerce.com
DNS Name	*.googlecommerce.com
DNS Name	ggpht.cn
DNS Name	*.ggpht.cn
DNS Name	urchin.com
DNS Name	*.urchin.com
DNS Name	youtu.be
DNS Name	youtube.com
DNS Name	*.youtube.com
DNS Name	youtubeeducation.com
DNS Name	*.youtubeeducation.com
DNS Name	youtubekids.com

IP address approach:

Look for the IP addresses of the company using ASN number, and fetch the Alternative Names from alive addresses

bgp.he.net
ASN search

asnlookup.com
ASN to IP blocks

Automate the last part using your fav scripting language

You got for yourself a fresh subdomains list that is most probably missed by the majority of hunters...

Pick a weird looking subdomain and start the hunt!

Note: If you found something, make sure that it belongs to the company!

您必须使用与服务器技术匹配的单词列表!

相同的语言？ → 你会发现一些东西

Bruteforce using wordlists the server will understand

Bruteforcing directories with php wordlist

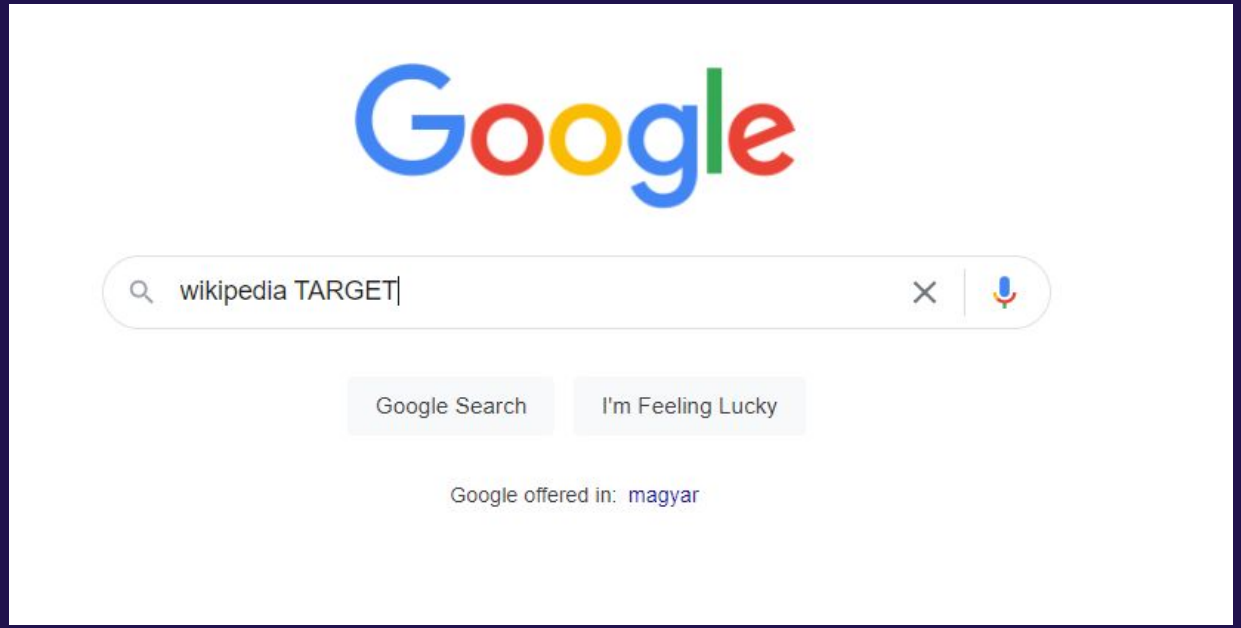
What the hell are you asking for?

Asp files on the server

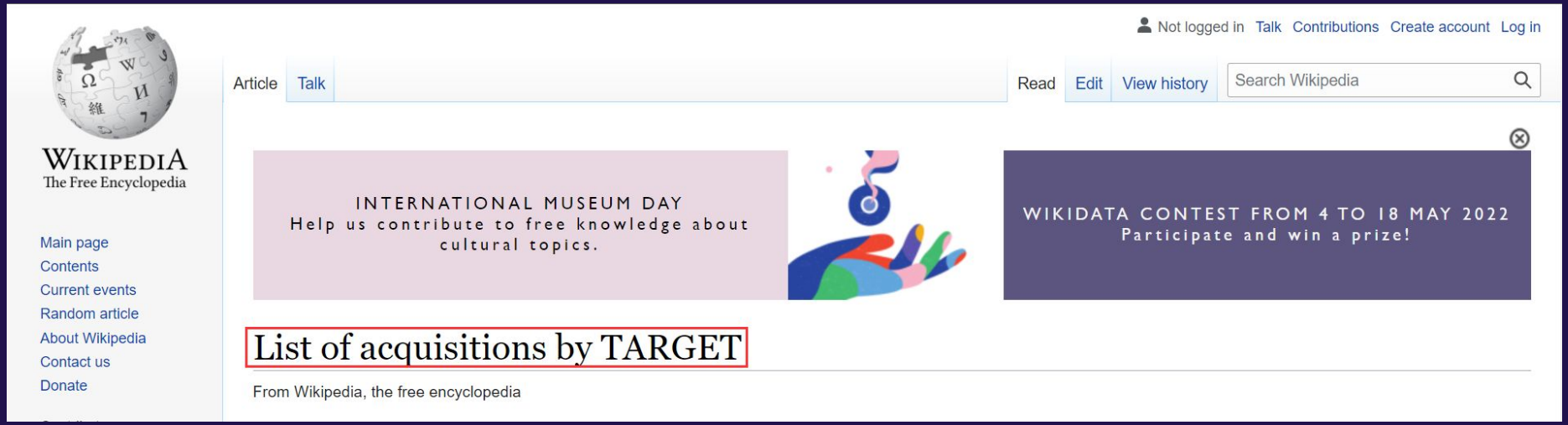
- Build your own wordlists, this helps a lot in the future
- Save endpoints from other disclosed reports
- Fetch paths from JS files (Linkfinder on Github)
- Spider the web application and save the output

Summing up what we discussed, let's see how I found an SQL injection!

Started by looking for the less-crowded areas and domains



Searched for the list of acquisitions (you can use many other services for this)



Found a seed controlled by the same company
example: TARGETebcd.com

Let's do some subdomain enumeration!

Tip for alive subdomains:
I personally use httpx with the following flags

```
cat subs.txt | httpx -title -status-code
    -content-length -follow-redirects
```

https://github.com/projectdiscovery/httpx

How good recon gifted me an SQLi?

Output of subfinder + httpx

```
               __    _____           __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/ v2.5.0

                projectdiscovery.io

Use with caution. You are responsible for your actions
Developers assume no liability and are not responsible for any misuse or damage.
By using subfinder, you also agree to the terms of the APIs used.

[INF] Loading provider config file /home/splintersec/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for [redacted]
[INF] Found 250 subdomains for [redacted] in 2 seconds 109 milliseconds
https://[redacted]m [302,302,200] [5731] [[redacted]] [https://[redacted]/index.jsp]
https://[redacted]com [302,302,200] [7419] [[redacted]] [https://[redacted]/index.jsp]
https://[redacted]com [302,302,200] [7419] [[redacted]] [https://[redacted]/index.jsp]
https://[redacted].com [302,302,200] [7370] [[redacted]] [https://[redacted]]
https://[redacted]com [302,302,200] [5731] [[redacted]] [https://[redacted]]
https://[redacted] [200] [161] [Index of /]
https://[redacted].com [200] [161] [Index of /]
https://[redacted]com [200] [125] []
https://[redacted] [404] [315] [[redacted]]
https://[redacted][302,200] [50852] [[redacted]] [https://[redacted]]
https://[redacted]m [302,200] [9514] [[redacted]] [https://[redacted]
[redacted]/welcome.cgi]
https://[redacted].com [302,302,302,302,200] [9089] [Login] [https://[redacted].xhtml]
https://[redacted] [302,301,302,302,200] [15475] [[redacted]] [https://[redacted]
[redacted]/Default.aspx]
http://[redacted] [200] [936] []
```

https://github.com/projectdiscovery/httpx

The first link gave a login panel, example of the url:

`https://a2a.TARGET.com/a2a/index.jsp`

Two inputs: `username` and `password`

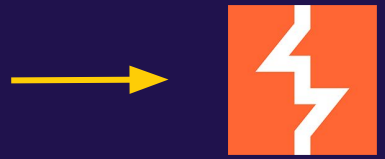
Tested everything usual on the login fields:

- SQL Injection
- Code Injection
- XSS
- Credentials like (admin/admin...)

Wasn't successful, I also checked the source code of the page, read javascript code... Nothing.

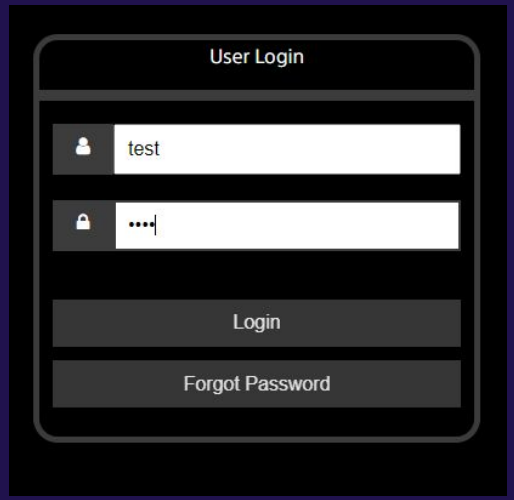
Let's see what happens in the backend

username: **test**
password: **test**



```
POST /a2a/REDACTED/a2a_token HTTP/1.1
Cookies: <cookies>
…

user_id=test&password=test&org=sthg
```



Sent the http request to sqlmap, and continued my testing...

```
POST /a2a/REDACTED/a2a_token
```

Analyzing the request and the response, I noticed that the POST url path contains “token”, which means there’s a token exchange somewhere in the backend

The POST request gives the following response

```
HTTP/1.1 302 Found

Location: https://a2ahs.TARGET.com
Connection: close
Cache-Control: no-cache
Pragma: no-cache
```

SQLmap gave nothing on the first try btw…

And after some redirects, it gets back to the first subdomain with the login error message

Big hm!

- The token is fetched from another subdomain, which was a blank page.
- There's no trace for the subdomain on the javascript files...

Logic of the login panel

POST request to here

https://a2a.TARGET.com/a2a/REDACTED/a2a_token

https://a2ahs.TARGET.com/

https://a2a.TARGET.com/

Fetch auth token from here

If auth token is valid, login successful

How good recon gifted me an SQLi?


```
https://a2a.TARGET.com/a2a/REDACTED/a2a_token
```

How good recon gifted me an SQLi?

https://a2a.TARGET.com/a2ahs/

New login panel, looks older, felt it was vulnerable to SQL injection

Same fields, this time I inserted single quotes

```
POST /a2ahs HTTP/1.1
Cookies: <cookies>
…

user_id=test’&password=test’&org=sthg
```

```
http failure response for
https://a2a.TARGET.com/a2ahs/: 500 Internal Server
Error
```

Jackpot! There's a high chance for an SQL injection

Tested normal injections, didn't work,
sent the request to SQLmap...

10 minutes later:

```
Parameter: user_id (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
    Payload:

    Type: error-based
    Title: Oracle AND error-based - WHERE or HAVING clause (UTL_INADDR.GET_HOST_ADDRESS)
    Payload:

    Type: AND/OR time-based blind
    Title: Oracle AND time-based blind
    Payload:
---
[22:52:51] [INFO] the back-end DBMS is Oracle
back-end DBMS: Oracle
[22:52:51] [WARNING] schema names are going to be used on Oracle for enumeration as the counterpart to database names on other DBMSes
[22:52:51] [INFO] fetching database (schema) names
[22:52:51] [INFO] used SQL query returns  entries
available databases [ ]:
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
```

The form was vulnerable to an error based SQL injection, where the DB stored a lot of sensitive information

Tried to escalate it to an RCE using the –os-shell argument, wasn't successful

That was the story of how I found an SQL injection in 1 hour of good recon, takeaways:

- Think of ways others could have missed
- BurpSuite on the background always helps
- Put more time on something only if you feel it's worth it
- Automate anything that the machine can do for you

Thank you!

@splint3rsec

BSIDES BUDAPEST