

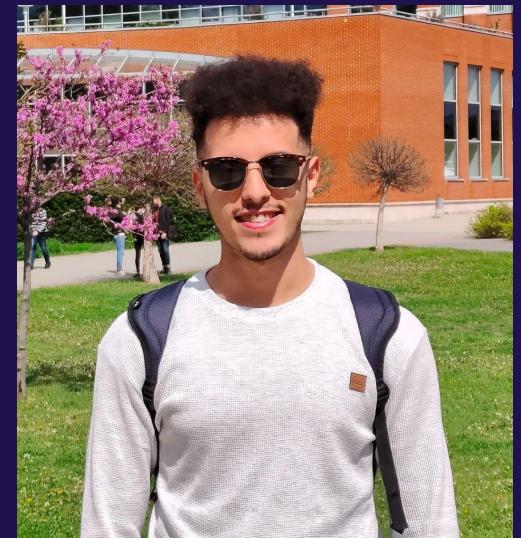
Bug Bounty Recon The “Right” Way

Is it really right? - Bsides Budapest 2022



Khalil Abdellah Lemtaffah

- 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.



@splint3rsec

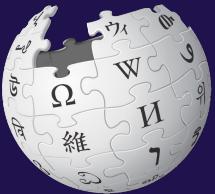


Ask yourself questions:

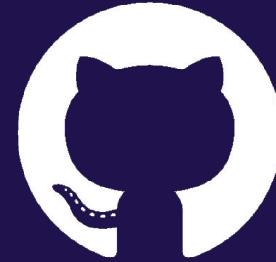
- Who is this company?
- Whom it's working with?
- Where is it located? (**Important**)
- Have I used its applications before?
- ...



@splint3rsec



WIKIPEDIA
The Free Encyclopedia



@splint3rsec

More assets = bigger recon surface



@splint3rsec

In scope types

Wide Scope

Small Scope
(1 - 5 assets)



@splint3rsec

Wide Scope



@splint3rsec

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



@splint3rsec

Example: Tesla

bugcrowd OUTHACK THEM ALL™ Who We Are Products Resources Customers CrowdStream Programs About Learn More

Tesla

Accelerating the world's transition to sustainable energy

\$100 – \$15,000 per vulnerability Partial safe harbor

Submit report



Program details Announcements 1 CrowdStream Hall of Fame

[Twitter Tweet](#) [Facebook Share 202](#)

Tesla values the work done by security researchers in improving the security of our products and service offerings. We are committed to working with this community to verify, reproduce, and respond to legitimate reported vulnerabilities. We encourage the community to participate in our responsible reporting process.

For vehicle or energy products

While we use Bugcrowd as a platform for rewarding all issues, please report vehicle and product related issues directly to vulnerabilityreporting@tesla.com, using [our GPG key](#) to encrypt reports containing sensitive information.

Vulnerabilities rewarded
626

Validation within
1 day
75% of submissions are accepted or rejected within 1 day

<https://bugcrowd.com/tesla>

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

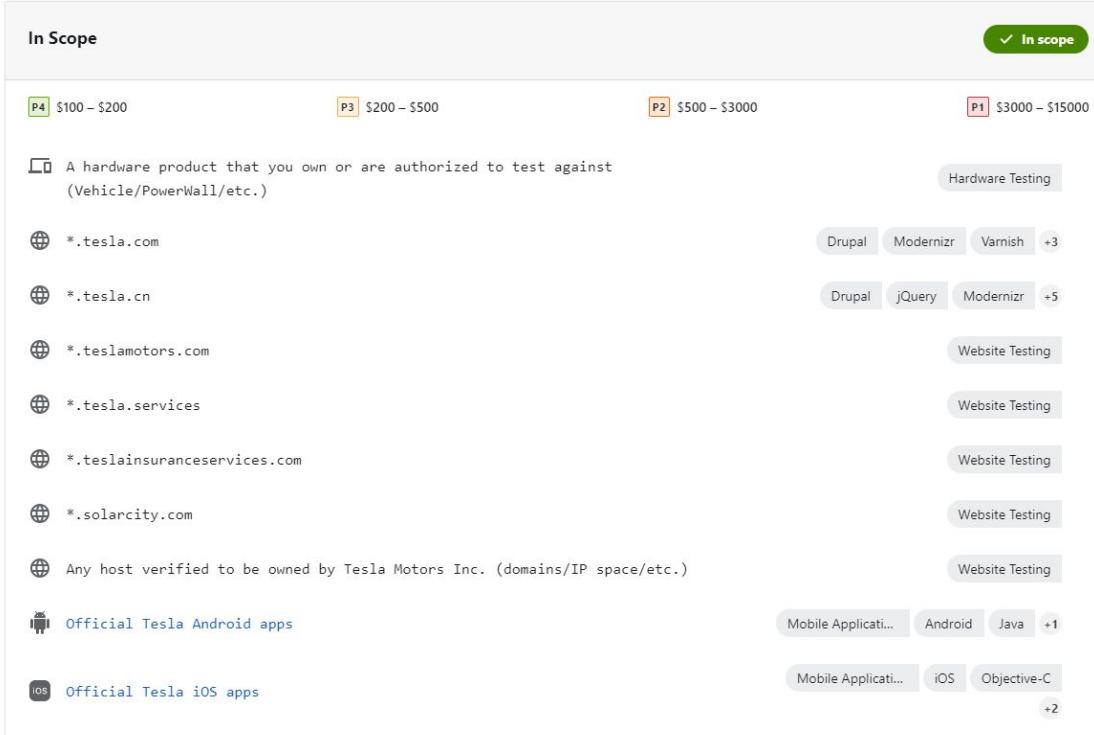
*.teslainsuranceservices.com Website Testing

*.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 Application Android Java +1

Official Tesla iOS apps Mobile Application iOS Objective-C +2



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

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			

Example: Tesla

Official Tesla Android apps

Mobile Application... Android Java +1

Official Tesla iOS apps

Mobile Application... iOS Objective-C +2

Small Scope

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



@splint3rsec

Tips and Mindset



@splint3rsec

→ Checkout the origin of the company

Where is it
located?
(Important)

Netherlands based?
**Subdomain bruteforcing based on
dutch wordlist**

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



@splint3rsec

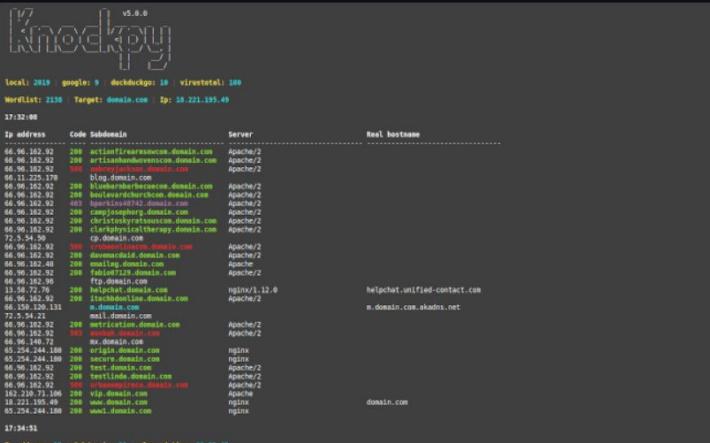
Tips and Mindset - Country based subs

17/70

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.



The terminal window shows the following output:

```
v5.3.0
Local: 2010 | google: 9  duckduckgo: 10  virustotal: 109
Wordlist: 2550  Target: domain.com  Port: 80,221,335,49
17:11:00

Ip address      Code Subdomain           Server          Real hostname
-----          -----
46.96.162.92    200 actionlivesoncom.domain.com   Apache/2
46.96.162.92    200 artisanhavencence.com       Apache/2
46.96.162.92    200 artisanhavencence.com       Apache/2
46.96.162.92    200 blog.domain.com             Apache/2
46.96.162.92    200 bluerabbitsecrect.com        Apache/2
46.96.162.92    200 bluerabbitsecrect.com        Apache/2
46.96.162.92    403 sponsered4742.domain.com    Apache/2
46.96.162.92    200 campionsgberg.domain.com     Apache/2
46.96.162.92    200 campionsgberg.domain.com     Apache/2
46.96.162.92    200 campionsgberg.domain.com     Apache/2
46.96.162.92    200 clearyphyscialtherapy.domain.com Apache/2
46.96.162.92    200 CQdomain.com                 Apache/2
46.96.162.92    200 devonmcauliford.domain.com  Apache/2
46.96.162.92    200 dominionhosting.com         Apache/2
46.96.162.92    200 Fabio129.domain.com        Apache/2
46.96.162.92    200 Tcp-0main.com                nginx/1.12.0
46.96.162.92    200 helpchat.unified-contact.com  Apache/2
46.96.162.92    200 itchchedonlive.domain.com   Apache/2
46.96.162.92    200 mail.domain.com              N.domain.com.akadns.net
72.5.54.21      200 metrictition.domain.com   Apache/2
46.96.162.92    200 mydomain.com                Apache/2
46.96.140.72    200 mx.domain.com               Apache/2
46.96.244.189   200 orfelia.domain.com        nginx
46.96.244.189   200 orfelia.domain.com        nginx
46.96.162.92    200 test.domain.com            Apache/2
46.96.162.92    200 testline.domain.com       Apache/2
46.96.162.92    200 testline.domain.com       Apache/2
162.230.71.106  200 vip.domain.com             Apache/2
162.230.71.106  200 www.domain.com             Apache/2
45.254.244.189  200 www1.domain.com        Apache/2

17:11:31
Ip address: 13  Subdomains: 33  elapsed time: 00:02:43
```

Very simply

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

Packages

No packages published

Contributors 7



Languages

Python 100.0%

Tips and Mindset - Country based subs

18/70

📄 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

```
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.dsrb.akamaiedge.net       |
| 23.213.161.225 | 200  | beta.volkskrant.nl           |              | e15645.dsrb.akamaiedge.net        |
| 23.213.161.225 | 200  | brandedcontent.volkskrant.nl | Apache       | e15645.dsrb.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.dsrb.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.dsrb.akamaiedge.net        |
| 37.97.223.87   | 200  | labs.volkskrant.nl           |              |                                   |
| 23.213.161.201 | 406  | login.volkskrant.nl          | AkamaiGHost  | e15410.dsrb.akamaiedge.net        |
| 23.213.161.210 | 406  | login2.volkskrant.nl         | AkamaiGHost  | e15410.dsrb.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.dsrb.akamaiedge.net        |
| 23.213.161.225 | 200  | mobile.volkskrant.nl         |              | e15645.dsrb.akamaiedge.net        |
| 23.213.161.199 | 200  | myaccount.volkskrant.nl      |              | e15454.dsrb.akamaiedge.net        |


```

Normal subdomain bruteforce

```
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.dsrb.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.dsrb.akamaied
ge.net				
146.185.53.23	200	archief.volkskrant.nl		dpp-public-cl21.pers
groep-ops.net				dpp-public-cl21.pers
146.185.53.23	200	blog.volkskrant.nl		dpp-public-cl21.pers
groep-ops.net				
146.185.53.23	200	blogs.volkskrant.nl		
groep-ops.net				
23.213.161.212	200	brandedcontent.volkskrant.nl	Apache	e15645.dsrb.akamaied
ge.net				
23.67.141.39		caps.volkskrant.nl		e8821.dsrb.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.dsrb.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
```

Tips and Mindset - Country based subs

21/70

```
146.185.53.23 200 verkeer.volkskrant.nl
groep-ops.net
142.93.232.211
ng.com
146.185.53.23
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      200  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
```



@splint3rsec

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.**



@splint3rsec

→ Trademark/Copyright based recon

For wide scope targets, including acquisitions..

The image shows a tweet from Jason Haddix (@jhaddix) with the following content:

== Trademark and Copyright Recon ==

How to find assets no other bug hunters have found.

One of my simple "secrets" for years.

Little automation exists for it.

\$\$\$
a thread🧵

🌟 follow, retweet, & like for more hacker tips! 🌟

1/x

5:53 AM · May 4, 2022 · Twitter Web App

Tips and Mindset - Copyright recon

24/70



Jason Haddix @Jhaddix · May 4

In several of these programs, a simple trick that I use to great success is finding copyright and trademark text. For example:

"© Copyright, XYZ1212 Company, 2020" on Google.

Then use the minus operator like:

"© Copyright, XYZ1212 Company, 2020" -xyz1212.com

4/x

Stuff he found using this dork



...



He removes the unwanted websites with the minus sign



Jason Haddix @Jhaddix · May 4

I have found whole new domains and tlds, that NO tester had tread before, using this simple technique.

I have found:

- Old marketing sites
- Outdated installs of software
- Build tools
- and more

Search for old years too... 1995+ and also check trademark strings.

5/x



@splint3rsec

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

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



The screenshot shows the official AT&T website. At the top, there's a navigation bar with links for Deals, Wireless, Internet, TV, Prepaid, and Business. Below the navigation is a search bar with placeholder text "I'm looking for..." and a magnifying glass icon. To the right of the search bar are icons for a heart, a shopping cart, Support, and Account. A yellow arrow points downwards from the URL "https://www.att.com/" to the main content area of the website.

In the center of the page, there's a banner message: "Don't forget! Mother's Day is May 8. Get your gift delivered with free shipping. [Shop gift guide](#)".

The main content features two promotional sections:

- TRADE-IN A GALAXY PHONE**
Any year. Any condition.
Learn how to get Samsung Galaxy S22 Ultra for up to \$800 off. Spoil her with something special.
With trade-in of Galaxy Note, S, or Z series smartphone. Other terms apply. [See offer details](#)
- LEARN HOW EVERYONE GETS iPhone 13 Pro Max for up to \$700 off**
With eligible trade-in. Only the best for Mom.
[See offer details](#)

At the bottom of the page, there are links for MOTHER'S DAY, WIRELESS, and AT&T UNLIMITED ELITE®.

<https://hackerone.com/att>

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](#)

[Newsroom](#)



[Make a store appointment](#)

[Careers](#)

[Contact us](#)

[Feedback](#)

[TechBuzz blog](#)

[Help & info](#)

[Ver en español](#)

[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](#)

©2022 AT&T Intellectual Property. All rights reserved.



@splint3rsec

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

[Site map](#)

[Coverage maps](#)

[Terms of use](#)

[Access](#)

©2022 AT&T Intellectual Property. All rights reserved.



@splint3rsec

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

The screenshot shows a Google search results page with the query "intext:"©2022 AT&T Intellectual Property." -att.co". The results are as follows:

- https://www.attdreaminblack.com** > the... ▾ Oldal lefordítása
Latest News - AT&T Dream in Black
Copyright © 2022 AT&T Intellectual Property All rights reserved. AT&T, Globe logo, Dream in Black, Dream in Black logo are registered trademarks of AT&T ...
- https://learn.att.jobs** app › categories ▾ Oldal lefordítása
AT&T Learn
2022 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual ...
- https://turnupthelove.com** > commitments ▾ Oldal lefordítása
Commitments - AT&T Turn Up The Love Logo
2022 AT&T Intellectual Property. All rights reserved. AT&T and the Globe logo are registered trademarks of AT&T Intellectual Property and/or AT&T affiliated ...
- https://www.attpublicpolicy.com** > ope... ▾ Oldal lefordítása
Open Internet - AT&T Public Policy
2022 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T ...



@splint3rsec

You can also search using
older copyright words...

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



@splint3rsec

Older copyrights = Older websites = More vulnerabilities



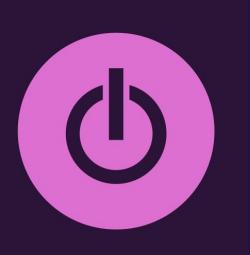
@splint3rsec

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!

For time tracking



For notes



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



- [!\[\]\(d257b6c8528eb7f0e396ffe01c4f6799_img.jpg\) Day 1 - Choose a program](#)
- [!\[\]\(f9108160801447942436f622c25765d1_img.jpg\) Day 2 - Setup a VPS + tools](#)
- [!\[\]\(698e11e06210785a617f890dd18f669d_img.jpg\) Day 3 → 8 - Recon and use the app as a normal user](#)
- [!\[\]\(f53b43a0ac2882a6e8a3472568f3af89_img.jpg\) Day 8 → Day 30 - Hack and Pray](#)
- [!\[\]\(8541c57930a1790e6c40fe6055195da3_img.jpg\) Notes / takeaways](#)

Rules

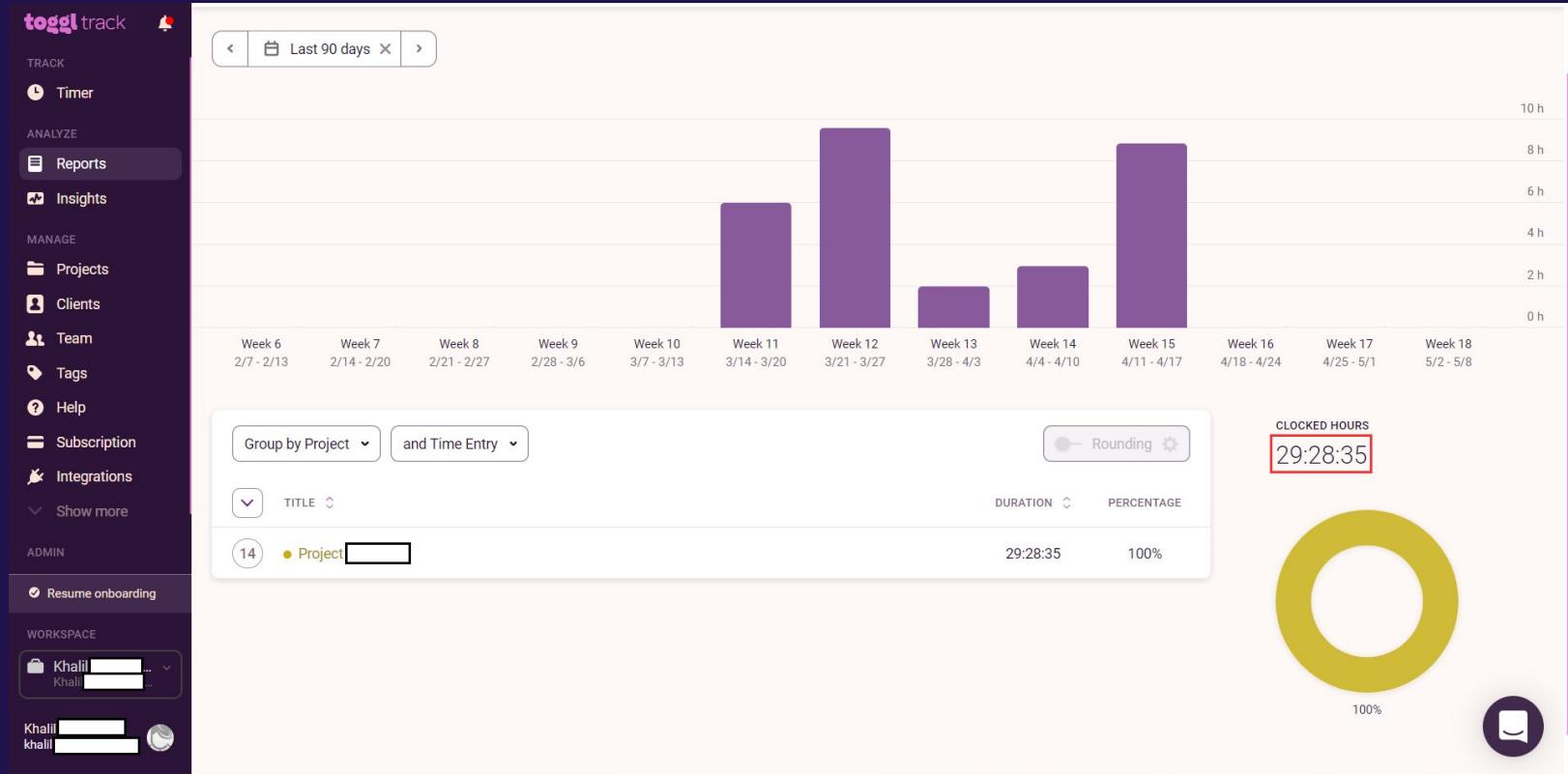
- 1 hour hunt on weekdays, 2 hours hunt on weekends
- Continuous hunting, no breaks allowed.
- Stick to only one program, no changing allowed
- If you fail the streak, You have to do something you don't like ⇒ Run 4 hours non stop
- Track your time with Toggl Track
- The challenge starts today (15th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



@splint3rsec

Tips and Mindset - Note taking

35/70



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 😊



@splint3rsec

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



Certificate

*.google.com		GTS CA 1C3	GTS Root R1	GlobalSign Root CA
Subject Name				
Common Name	*.google.com			
Issuer Name				
Country	US			
Organization	Google Trust Services LLC			
Common Name	GTS CA 1C3			
Validity				
Not Before	Mon, 18 Apr 2022 08:32:19 GMT			
Not After	Mon, 11 Jul 2022 08:32:18 GMT			
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			



@splint3rsec

Subject Alt Names

DNS Name	*.google.com
DNS Name	*.appengine.google.com
DNS Name	*.cdn.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	*.googleapis.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	*.ytmp3.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	*.youtubeeeducation.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



@splint3rsec

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



@splint3rsec

Bruteforce using wordlists the server will understand



Bruteforcing
directories with
php wordlist



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



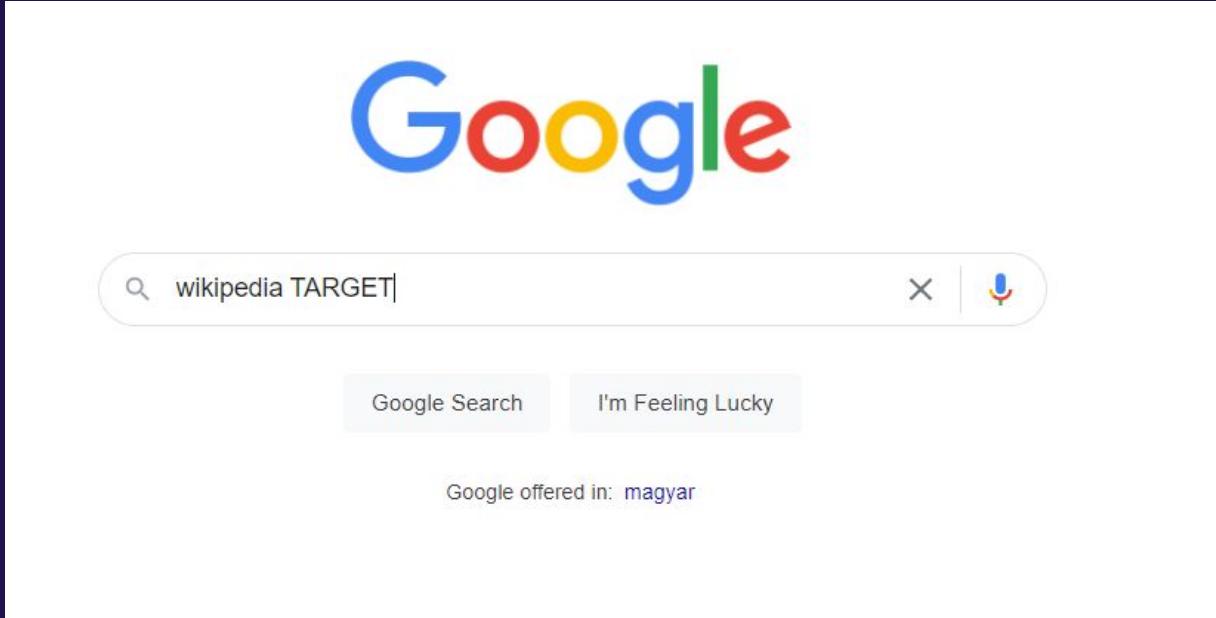
@splint3rsec

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



@splint3rsec

Started by looking for the less-crowded areas and domains



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

The screenshot shows a Wikipedia search results page for the query "List of acquisitions by TARGET". The page has a dark blue header with the title "List of acquisitions by TARGET". Below the header, there is a navigation bar with links for "Article" (selected), "Talk", "Read", "Edit", "View history", and a search bar. The main content area features a large red-bordered box containing the text "List of acquisitions by TARGET". Below this box, a note says "From Wikipedia, the free encyclopedia". To the left of the main content, there is a sidebar with the Wikipedia logo and links to "Main page", "Contents", "Current events", "Random article", "About Wikipedia", "Contact us", and "Donate". On the right side, there are two promotional banners: one for "INTERNATIONAL MUSEUM DAY" encouraging contributions to cultural topics, and another for a "WIKIDATA CONTEST FROM 4 TO 18 MAY 2022" offering prizes.

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

Let's do some subdomain enumeration!



@splint3rsec

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

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



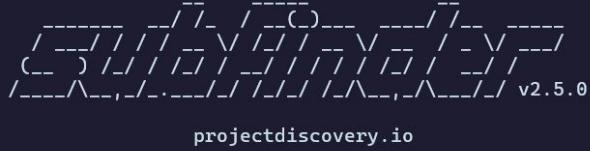
@splint3rsec

<https://github.com/projectdiscovery/httpx>



How good recon gifted me an SQLi?

51/70



Output of subfinder + httpx

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] in 2 seconds 109 milliseconds
[INF] Found 250 subdomains for [REDACTED]
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] []
```

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

<https://a2a.TARGET.com/a2a/index.jsp>

Two inputs: username and password



@splint3rsec

Tested everything usual on the login fields:

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



@splint3rsec

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



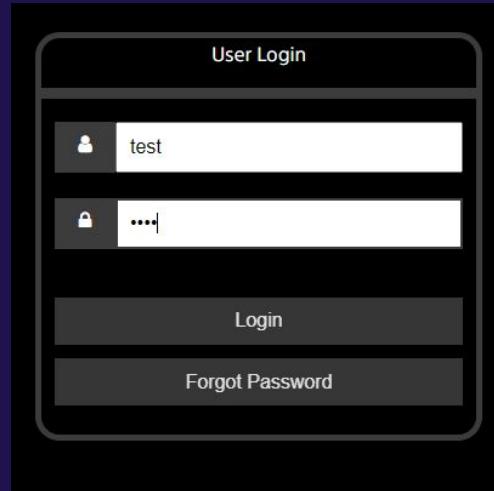
@splint3rsec

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
```



@splint3rsec

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



@splint3rsec

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



@splint3rsec

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



@splint3rsec

SQLmap gave nothing on
the first try btw...

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



@splint3rsec

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...



@splint3rsec

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



@splint3rsec

How good recon gifted me an SQLi?

62/70

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



@splint3rsec



How good recon gifted me an SQLi?

63/70

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



@splint3rsec

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



@splint3rsec

Same fields, this time I inserted single quotes

POST /a2ahs HTTP/1.1

Cookies: <cookies>

...

user_id=test'&password=test'&org=sthg



@splint3rsec

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

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



@splint3rsec

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



@splint3rsec

10 minutes later:

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

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

Type: AND/OR time-based blind
Title: Oracle AND time-based blind
Payload: [REDACTED]
-- 
[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 [REDACTED] entries
available databases [REDACTED]:
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
```



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

