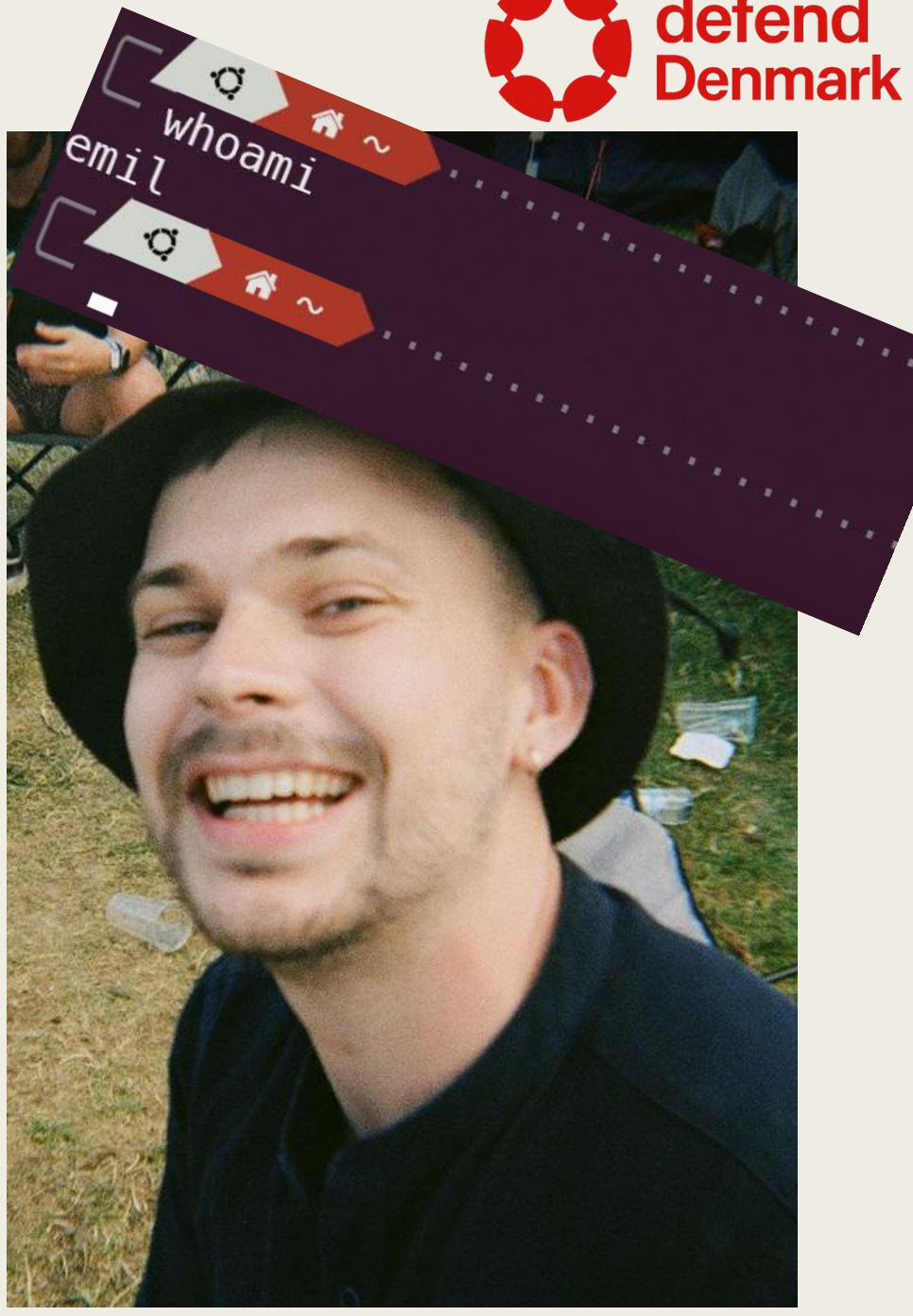
SUCCEEDING IN BUG BOUNTY HUNTING

Tips for getting your first bounty

whoami

- Studied the cybersecurity master 2020-2022
- Creating a Danish Bug Bounty platform: Defend Denmark
- Teacher of ‘Fundamentals of Cybersecurity’ @ AAU
- Various pentesting certs (OSCP, OSCE3)
- Freetime bug bounty hunter (why I give this talk)
- Web security researcher.

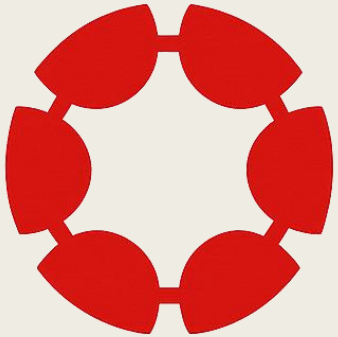


What is this talk?

- 2nd talk about bug bounty hunting
- A more technical approach to finding bugs
- How I approach a new target
  - *Recon*
  - *Deep dive*
- A bunch of random tools / tips
- Tips on writing reports

What is Defend Denmark

- Localized bug bounty platform
  - Danish hackers (residents ok)
  - Danish companies
- Sister company to Defend Iceland
  - Successful localized bug bounty platform
- We are in the process of launching
  - Onboarding hackers and looking for first customers (targets)
- Come talk to me after this talk if you want to get onboarded
  - Need clean criminal record
  - Signing of Defenders agreement (NDA, Scope rules etc)
  - MitID
  - Resident in Denmark with european citizenship



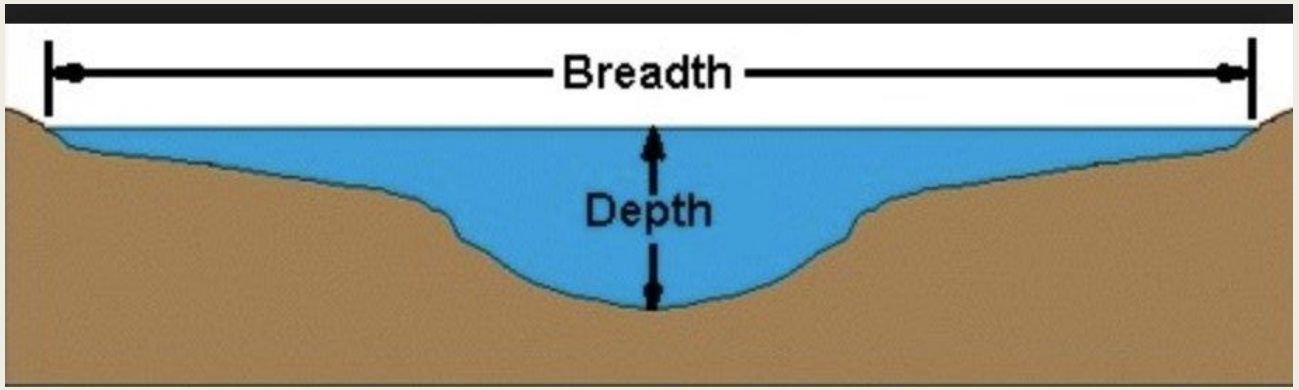
defend Denmark

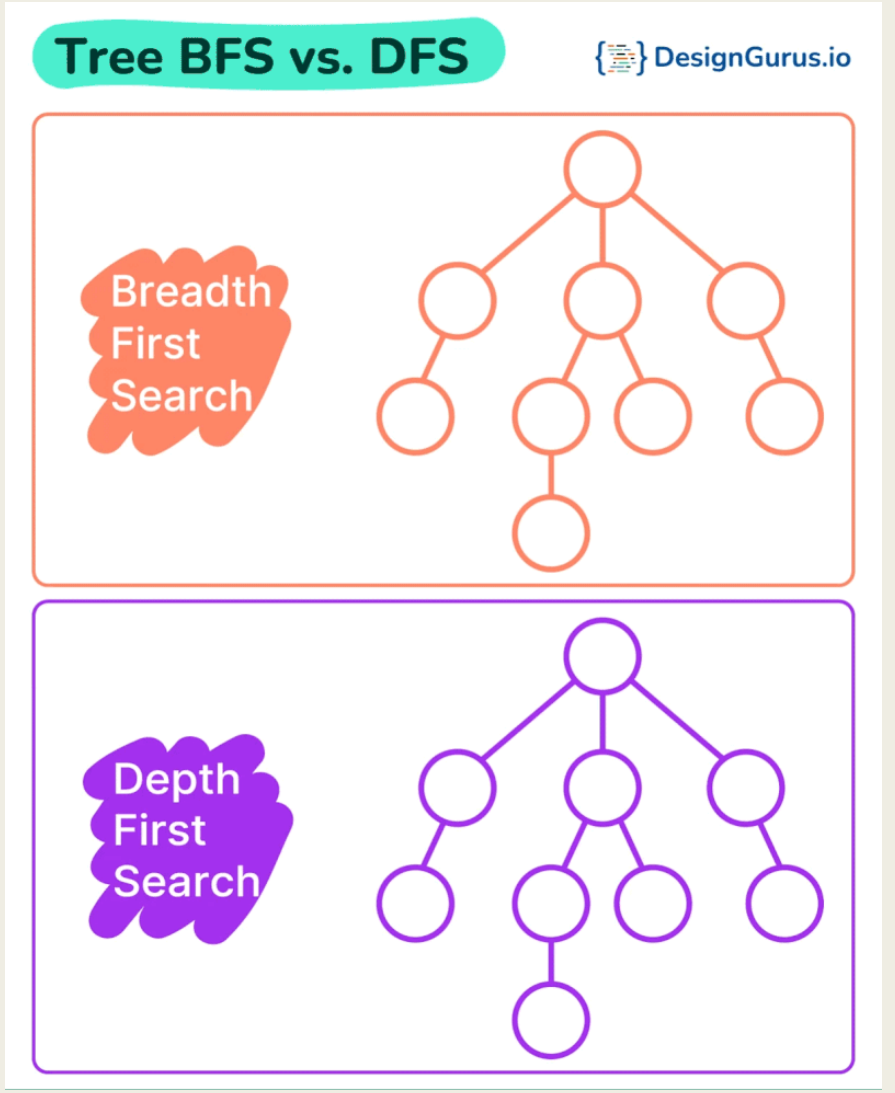
How to get the most out of this

- You know the ecosystem of bug bounty hunting
- You have signed up / will sign up to a bug bounty platform
- You understand the safe harbor and what is “out of scope”
- You have some setup that allows you to run burp/caido and cli tools

The 2 different approaches

- Either we go breadth first and map a lot of attack surface
- Or we go depth first, straight into the main application





Recon based approach - BFS

defend Denmark

- **Goal:** Use reconnaissance tools/approaches to find as much information as possible on the target
- **Why?** – Security through obscurity/hiding
  - *Developers may put some test/admin/sensitive feature on a site, but assume ”No one will find this”*
- What to look for?
  - *Subdomains (Staging and test environments, admin.example.com)*
  - *Non-public endpoints (/api/v1/test_admin_auth/auth/user)*
  - *Non-public functionality*
  - *Non-public parameters*
  - *Old functionality (What did the site use to expose, allow?)*
- Legacy functionality has a larger chance of being vulnerable
- This approach is easiest when **automated**

Deep dive into functionality - DFS

- **Goal:** Understand the target so well that conflicting functionality becomes apparant, the goal is to find logic bugs.
- **Why?** Logic bugs can be the most serious vulnerabilities, breaking confidentiality or integrity.
- How to navigate this approach?
  - *Use the application normally for some time*
  - *Observe requests being made to understand the structure and architecture of the site*
  - *What technologies can be inferred to be in use?*
  - *How does the application respond to bad input?*
  - *What does the auth model look like?*
- This approach is more **manual**

NEW TARGET LETS GO

LETS GET THAT BOUNTY

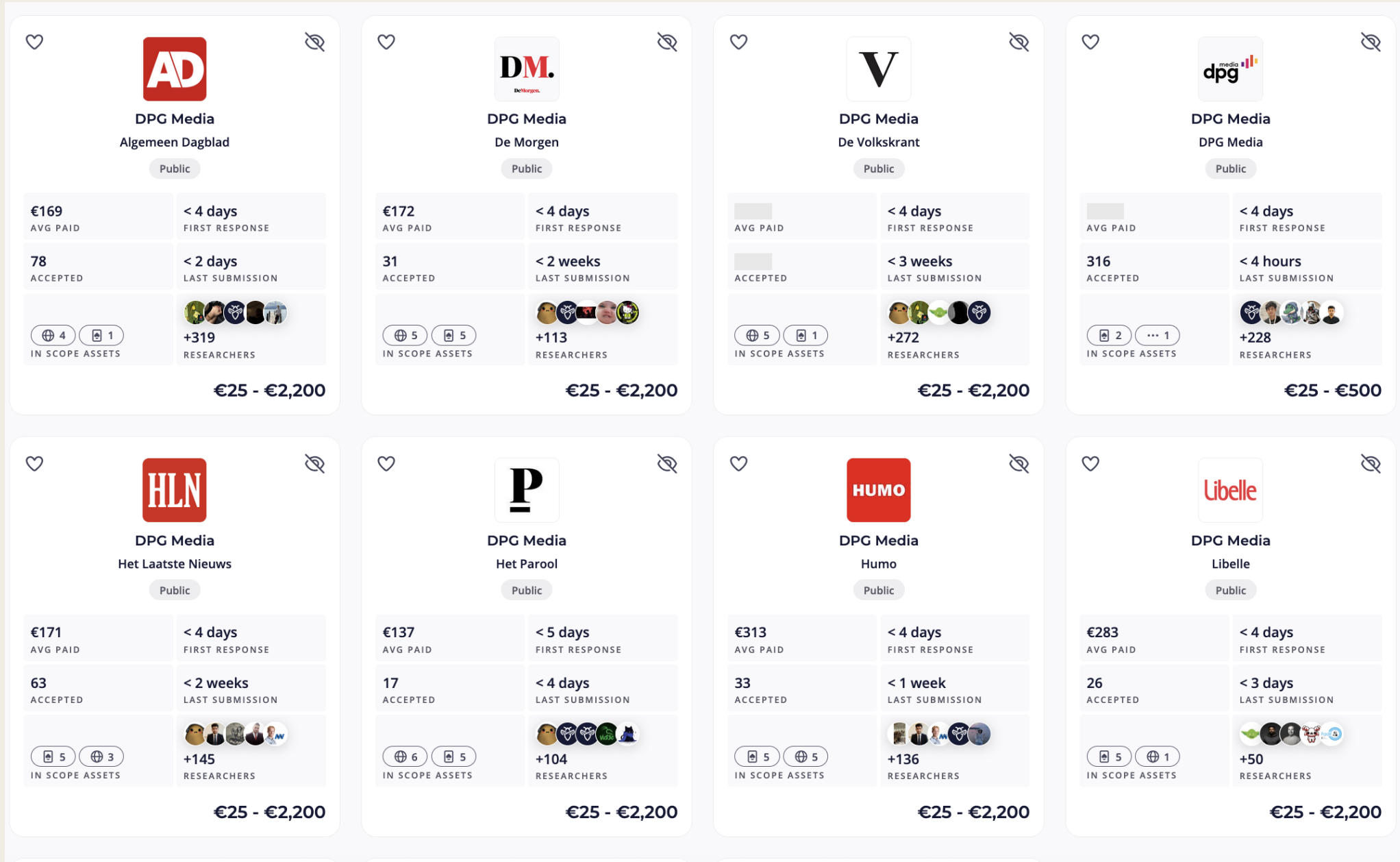
defend Denmark

media dpg

TARGET ACQUIRED

This is a good target because...

defend Denmark



Its public and very very broad

defend Denmark

Collapse all

*.dpgmedia.be — Wildcard — Tier 2

excluding

- login.dpgmedia.be

*.dpgmedia.nl — Wildcard — Tier 2

excluding

- login.dpgmedia.nl

Any related DPG media domain — Other — Tier 3

*Only applicable to domains that are **100% owned by DPG**.*
*For example, projects that are partly owned by DPG and partly owned by RTL (because of a joint venture between the two) are **not** in scope.*

Whois:

De Persgroep Publishing nv
Brusselstesteenweg 347
1730 Asse
België

DPG Media Services NV
Mediaplein 1
2018 Antwerpen
Belgium

Whats OOS

defend Denmark

Out of scope

Give feedback >

Redirects on unused domains

We have a substantial amount of parked domains due to acquisitions of other companies. Some of them redirect to other domains which can still be registered.
These types of link hijacking our out-of-scope for this program.

Highlighted

- Domains that are not 100% owned by DPG media
- Open redirects in privacy consent endpoints (eg `/privacygate-confirm`, `/privacy-wall` etc)
- Paywall can be bypassed
- User password leaks, not originating from a vulnerability on our side, can be reported but will not be rewarded with a bounty.

Application

- API key disclosure without proven business impact
- Wordpress usernames disclosure
- Pre-Auth Account takeover/OAuth squatting
- Self-XSS that cannot be used to exploit other users
- Verbose messages/files/directory listings without disclosing any sensitive information
- CORS misconfiguration on non-sensitive endpoints
- Missing cookie flags
- Missing security headers

defend Denmark

TARGET: DPGMEDIA.BE

and any other companies owned by DPG Media Group

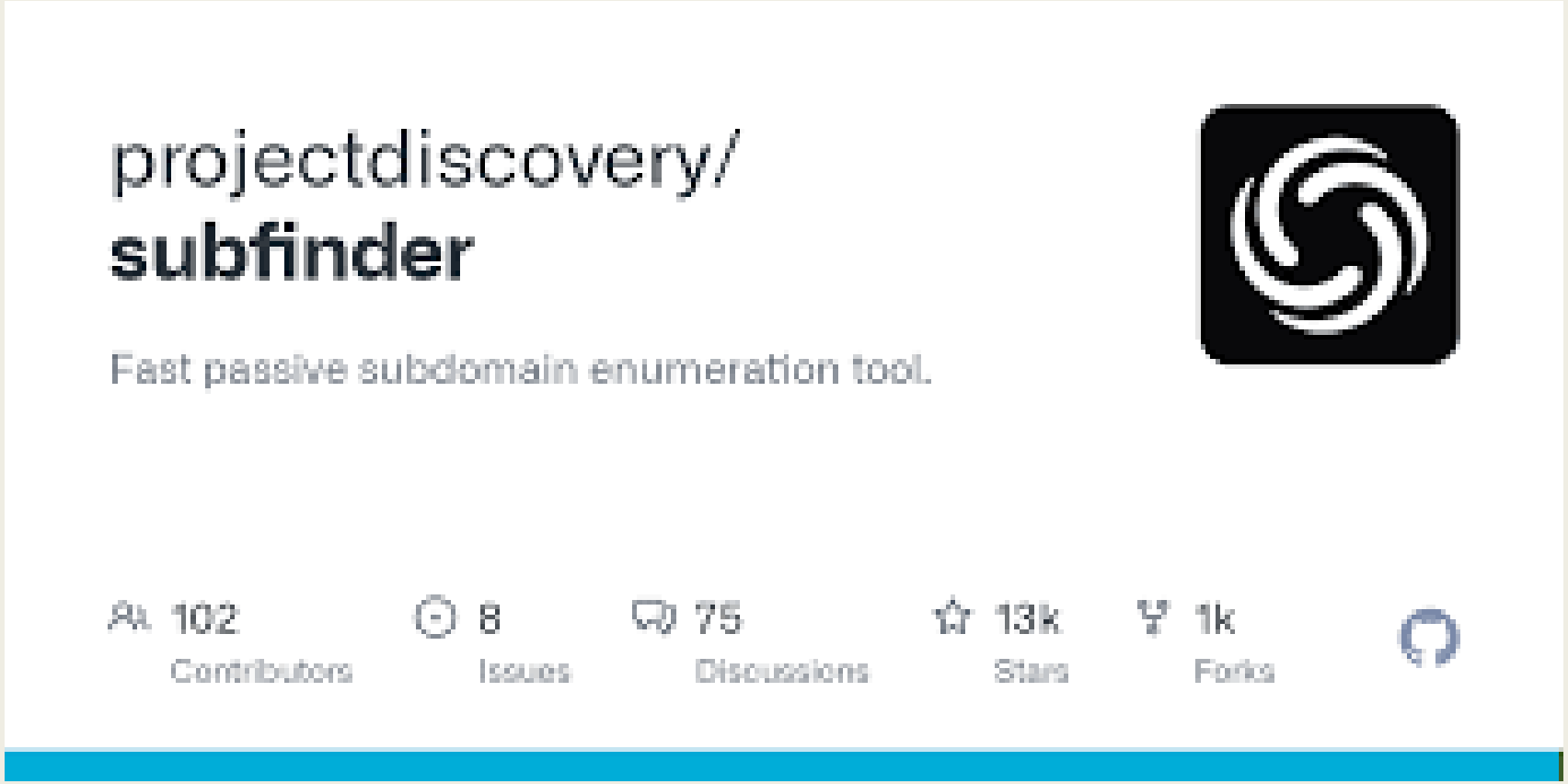
The goal – BFS FIRST

defend Denmark

- Figure out as many **subdomains** for our target as possible
- Figure out which **IP addresses** these run on
- Figure out which **services** run on these IP addresses
- Figure out which **HTTP apps** run on which ports, with a hostname in mind.

> " The goal of recon is to find more websites to hack"
>
> - Jhaddix

Tool: Subfinder



```
root@vmi2838169:/tmp# subfinder -d dpgmedia.be


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

                projectdiscovery.io

[INF] Current subfinder version v2.10.1 (latest)
[INF] Loading provider config from /root/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for dpgmedia.be

device1976001-37355395.dpgmedia.be
acc-pds.dpgmedia.be
unregister.dpgmedia.be
ucavo.dpgmedia.be
```

- ……

```
nexus-que.dpgmedia.be
octagonshop.dpgmedia.be
regqs.dpgmedia.be
minarsidur.dpgmedia.be
000073--v2sa2ca02b5887d8dfb5.dpgmedia.be
devopsims2.dpgmedia.be
prd-jitt.dpgmedia.be
ver4.dpgmedia.be
[INF] Found 9735 subdomains for dpgmedia.be in 4 minutes 4 seconds
```

Subfinder tips

- Subdomains may contain gold in the form of
  - *Old forgotten applications*
  - *Admin panels*
  - *Sites with less security*
- Use the **subfinder** API keys
  - *Can use more sources to find subdomains*
  - *Will give you more results than stock subfinder*
  - *Many of these keys are for free or very cheap*
- Filter off domains that don't point anywhere
  - *Check A and CNAME dns records for all domains*
  - *DNSX?*

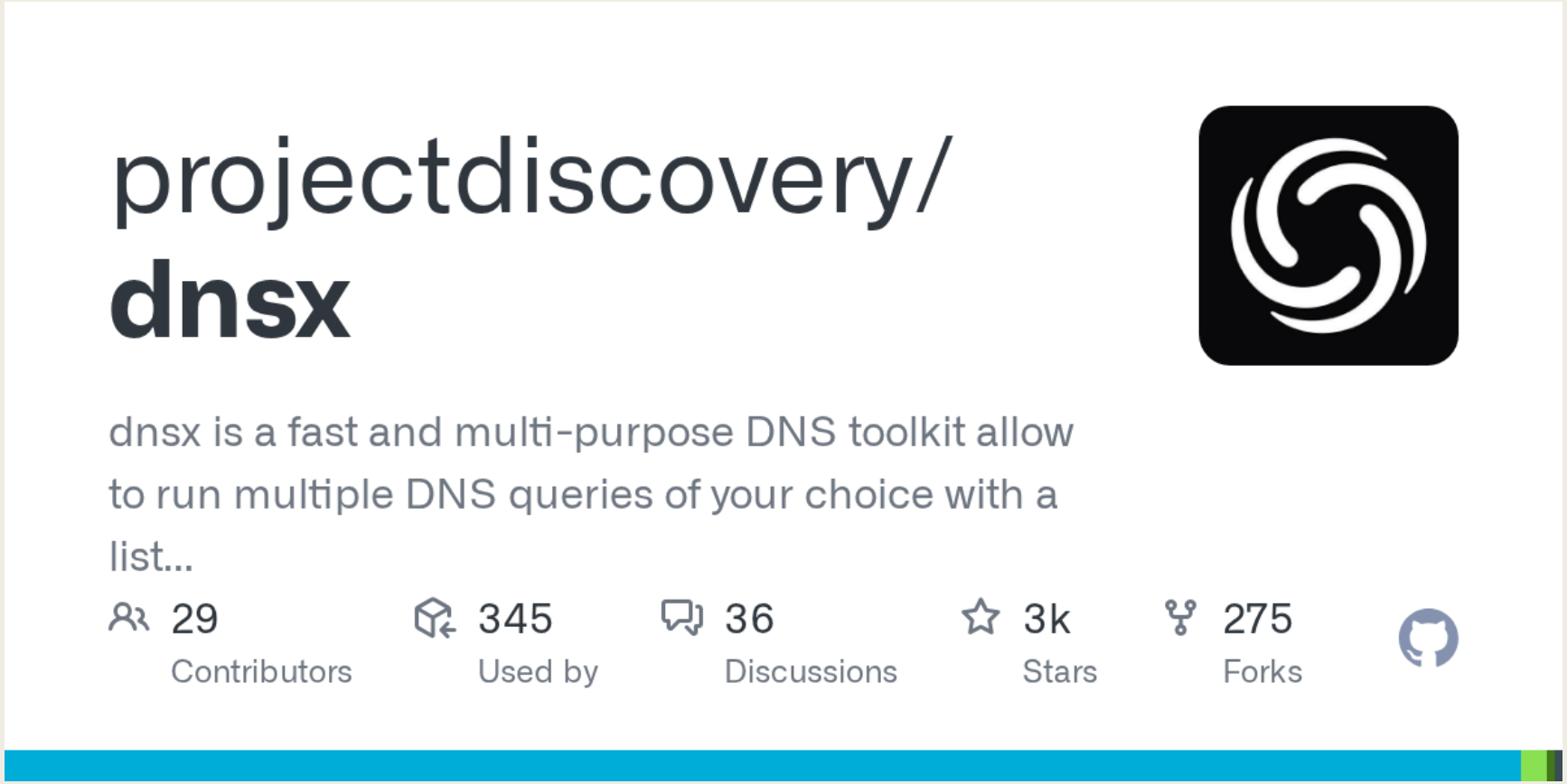
Subfinder API Sources

Subfinder supports the following data API sources:

NAME	URL
BeVigil	https://bevigil.com/osint-api
BinaryEdge	https://binaryedge.io
BufferOver	https://tls.bufferover.run
C99	https://api.c99.nl/
Censys	https://censys.io
CertSpotter	https://sslmate.com/certspotter/api/
Chaos	https://chaos.projectdiscovery.io
Chinaz	http://my.chinaz.com/ChinazAPI/DataCenter/MyDataApi
DNSDB	https://api.dnsdb.info
Fofa	https://fofa.info/static_pages/api_help
FullHunt	https://fullhunt.io
GitHub	https://github.com
Intelx	https://intelx.io

Tool: DNSX

defend Denmark



Tool: DNSX

defend Denmark

- We can cut down on some domains that are not live

```
root@vmi2838169:~/test# cat subfinder_results.txt | wc -l
9735
root@vmi2838169:~/test# cat subfinder_results.txt | dnsx | wc -l


      _                __  __
   __| | _ __   ___ \ \/ /
  / _` || '_ \ / __| \  /
 | (_| || | | |\__ \ /  \
  \__,_||_| |_||___//_/\_\

                projectdiscovery.io

[INF] Current dnsx version 1.2.2 (latest)
9100
root@vmi2838169:~/test#
```

Tool: DNSX

- But many domains resolve to the same IP
  - *There can be a wildcard situation*
  - **.site.dpgmedia.be --> 2.21.239.18*

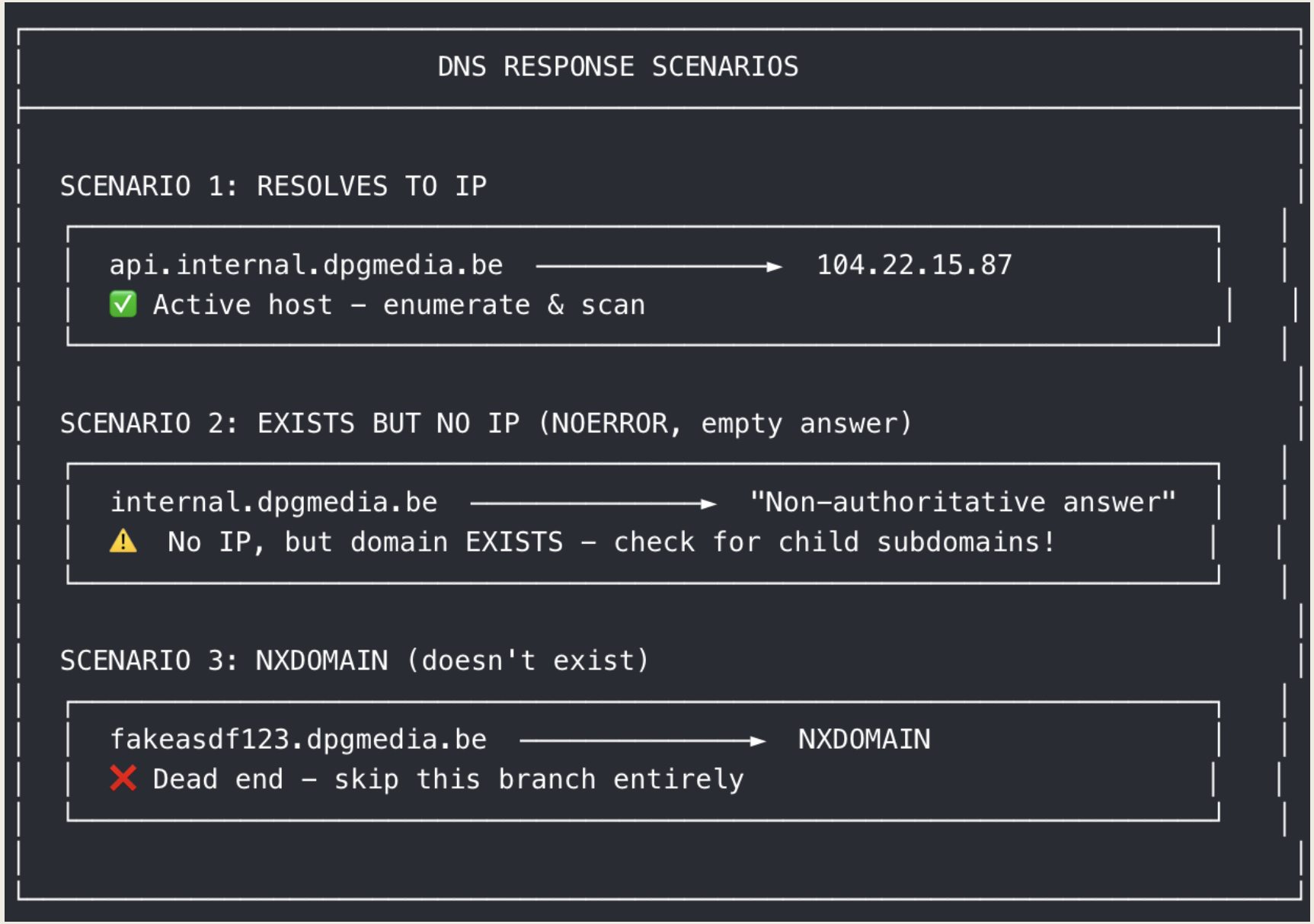
```
root@vmi2838169:~/test# head subfinder_results.txt | dnsx -ro

                     _                __  __
   __| | _ __    ___ \ \/ /
  / _` || '_ \ / __| \  /
 | (_| || | | |\__ \ /  \
  \__,_||_| |_||___//_/\_\

                projectdiscovery.io

[INF] Current dnsx version 1.2.2 (latest)
95.101.111.132
95.101.111.147
95.101.111.147
95.101.111.132
23.53.43.51
23.53.43.58
2.21.239.18
2.21.239.19
2.21.239.18
2.21.239.19
2.21.239.18
2.21.239.19
```

Tool: DNSX

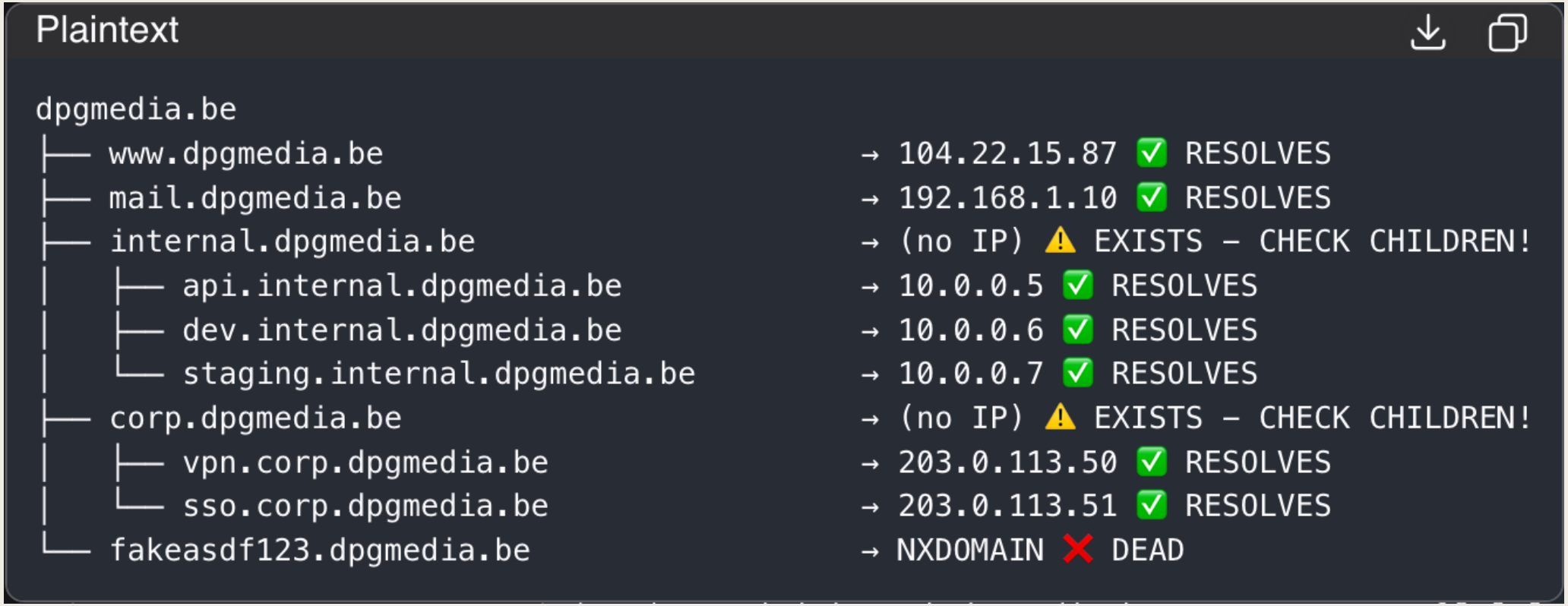
- But many domains resolve to the same IP
  - *There can be a wildcard situation*
  - **.site.dpgmedia.be --> 2.21.239.18*
  - *NXDOMAIN → Dead and ignore*
  - *No Answer → There may be something interesting here*

```
root@vmi2838169:~/test# cat subfinder_results.txt | dnsx -ro | sort | uniq > unique_ips.txt


                     _                __  __
   __| | _ __   ___ \ \/ /
  / _` || '_ \ / __| \  /
 | (_| || | | |\__ \ /  \
  \__,_||_| |_||___//_/\_\

                projectdiscovery.io

[INF] Current dnsx version 1.2.2 (latest)
root@vmi2838169:~/test# wc -l unique_ips.txt
103 unique_ips.txt
```

Premium tip: DNS responses may leak hidden domains



Premium tip: DNS responses may leak hidden domains



Tool: HTTPX

- We want to get more websites to hack
- So we have to find websites from our target list
- Websites run http on port 80 and https on port 443, so we use httpx to scan for that

```
root@vmi2838169:~/test# cat dnsx_results.txt | httpx -status-code -title -content-length -web-server -location -no-color -fol
low-redirects -t 50 -no-fallback -random-agent | tee httpx_results.txt


    __    __  __       _  __
   / /_  / /_/ /_____ | |/ /
  / __ \/ __/ __/ __ \|   /
 / / / / /_/ /_/ /_/ /   |
/_/ /_/\__/\__/ .___/_/|_|
             /_/

                projectdiscovery.io

[INF] Current httpx version v1.7.1 (outdated)
[WRN] UI Dashboard is disabled, Use -dashboard option to enable
http://000645--v2-0-194.dpgmedia.be [403] [] [450] [Access Denied] []
http://000607-a280f3a275173c4dedv2.dpgmedia.be [403] [] [450] [Access Denied] []
http://0007509d--v2-02-k3.dpgmedia.be [403] [] [459] [Access Denied] []
https://000607-a280f3a275173c4dedv2.dpgmedia.be [403] [] [450] [Access Denied] []
https://000645--v2-0-194.dpgmedia.be [403] [] [450] [Access Denied] []
http://000480a2ca02b5887d8dfb5.dpgmedia.be [403] [] [459] [Access Denied] []
http://0-194-002-gw-self-okta-self-service-acp.dpgmedia.be [403] [] [459] [Access Denied] []
http://000365--v2a9ffcac07ec8ba3e5.dpgmedia.be [403] [] [459] [Access Denied] []
http://001194002-bucketokta-self-okta-self-service.dpgmedia.be [403] [] [459] [Access Denied] []
http://00000-okta-nlbeta-okta-idp.dpgmedia.be [403] [] [459] [Access Denied] []
http://000085--v2sa2ca02b5887d8dfb5.dpgmedia.be [403] [] [459] [Access Denied] []
http://000469d--v20-194.dpgmedia.be [403] [] [450] [Access Denied] []
http://0-9-13.dpgmedia.be [403] [] [450] [Access Denied] []
https://000085--v2sa2ca02b5887d8dfb5.dpgmedia.be [403] [] [459] [Access Denied] []
https://000325v2a2ca02b5887d8dfb5.dpgmedia.be [403] [] [459] [Access Denied] []
http://00-2-okta-mfa-ackint--acc08idsautodiscoverpermutations-ii.dpgmedia.be [403] [] [459] [Access Denied] []
https://0007509d--v2-02-k3.dpgmedia.be [403] [] [450] [Access Denied] []
https://000365--v2a9ffcac07ec8ba3e5.dpgmedia.be [403] [] [459] [Access Denied] []
http://0-194-002-gw-self-okta-self-service-dpgmedia-guest-1.dpgmedia.be [403] [] [459] [Access Denied] []
https://001172d.dpgmedia.be [403] [] [450] [Access Denied] []
http://001167v2-a2ff7068db85f8aa2.dpgmedia.be [403] [] [459] [Access Denied] []
```

Putting them all together

defend Denmark

```
subfinder -d [TARGET] -all | httpx -status-code -title -content-length
-web-server -asn –location -no-color -follow-redirects -t 50 -ports
80,8080,443,8443,4443,8888 -no-fallback -probe-all-ips -random-agent
```

Leads us new places

```
http://freewheel-jitt.dpgmedia.be [301,200] [] [372035] [AmazonS3] [https://freewheel-jitt.dpgmedia.be/]
http://help.dpgmedia.be [301,303,200] [] [70747] [Log into Atlassian - DPG Media Jira] [] [https://atlassian.dpgmedia.net/jira/servicedesk/
https://help.dpgmedia.be [301,303,200] [] [70753] [Log into Atlassian - DPG Media Jira] [] [https://atlassian.dpgmedia.net/jira/servicedesk/
http://host-141-116-200-89.dpgmedia.be [403] [] [399] [Access Denied] []
https://host-141-116-200-89.dpgmedia.be [403] [] [399] [Access Denied] []
```

EXTRA TARGET: dpgmedia.net

NEW TARGET:

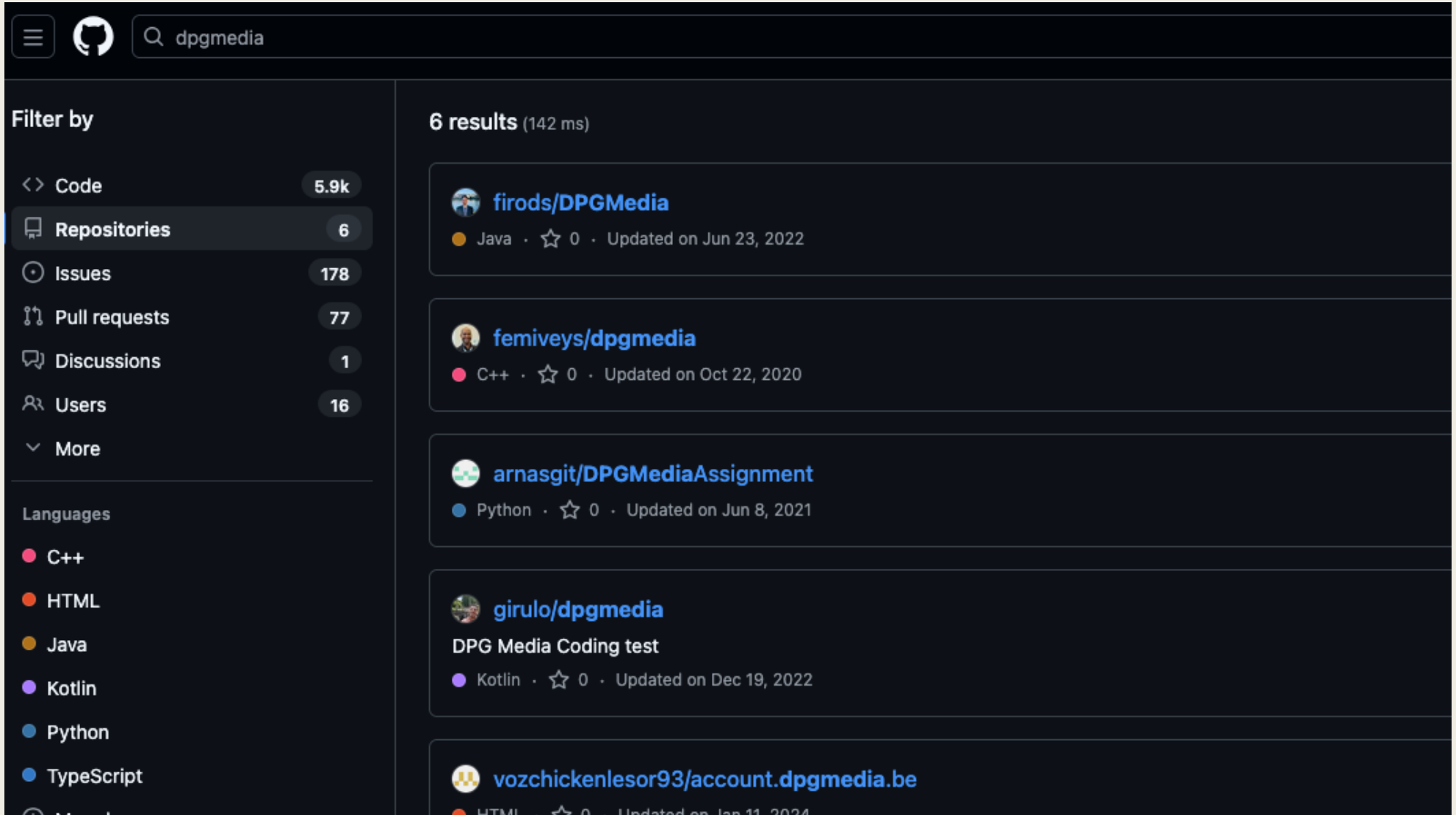
DPGMEDIA.NET

and now we run the tools again over and over and over and over

Tool: GITHUB OSINT?

defend Denmark

- Search for your targets sites on github to discover potential code relating to the target.
  - *Whitebox is always preferrable to blackbox*



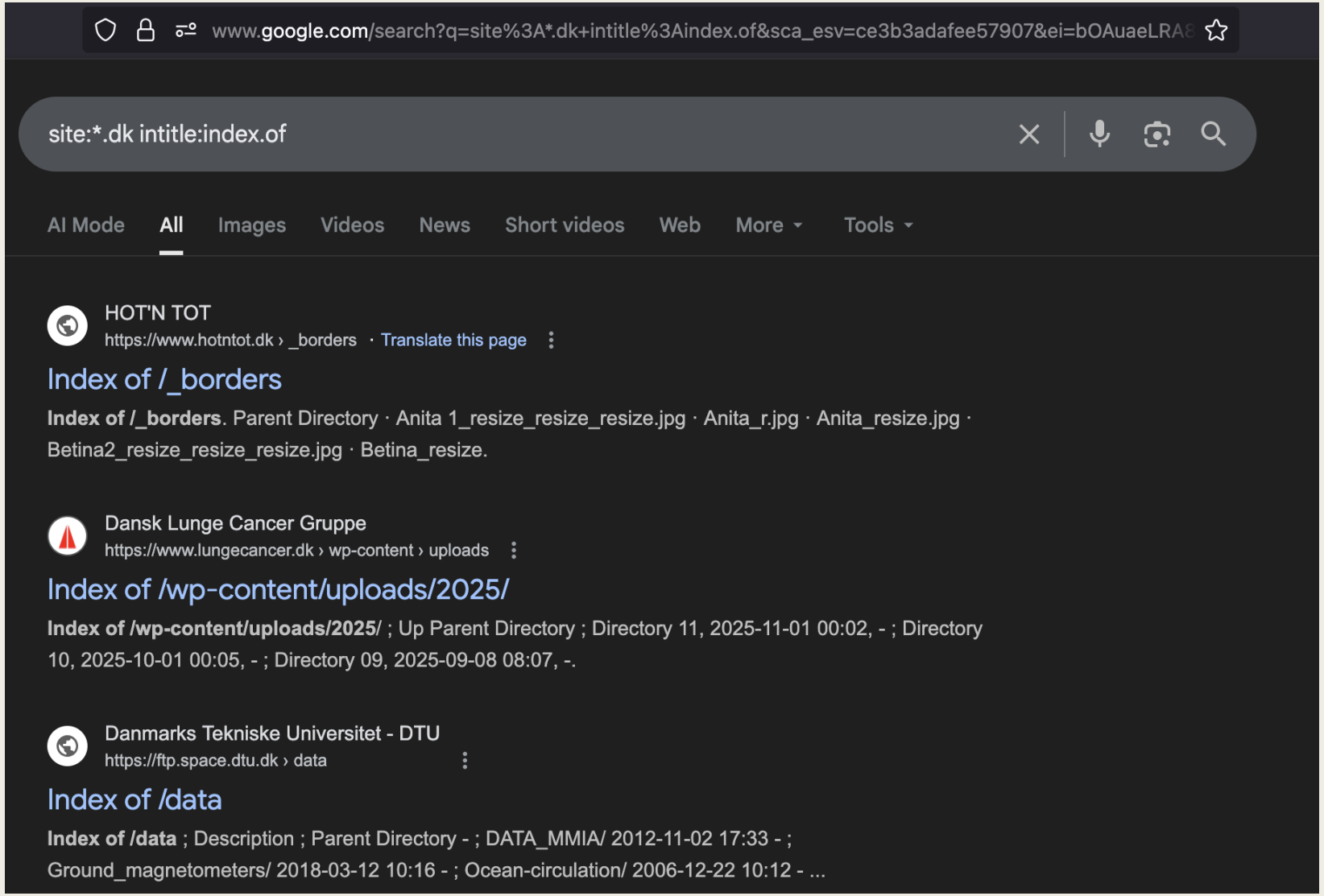
Premium tip: Dorking

defend Denmark

What is Google Hacking/Dorking?

Google Dorking, also known as Google Hacking, is a technique that utilizes advanced search operators to uncover information on the internet that may not be readily available through standard search queries.

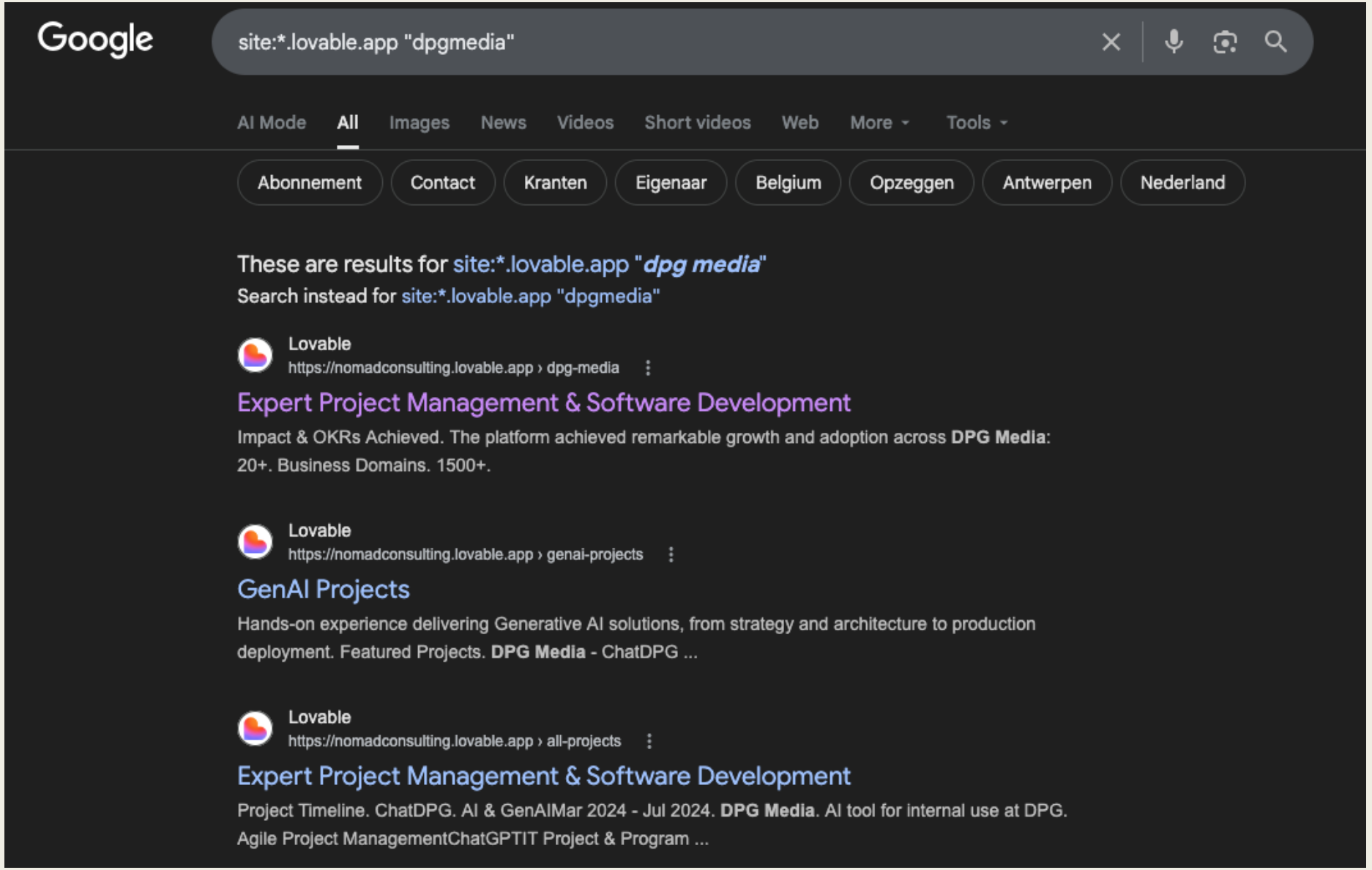
This strategy takes advantage of the features of Google's search algorithms to locate specific text strings within search results. Notably, while the term "hacking" suggests an illicit activity, Google Dorking is entirely legal and often used by security professionals to identify vulnerabilities in their systems.


www.google.com/search?q=site%3A*.dk+intitle%3Aindex.of&sca_esv=ce3b3adafee57907&ei=bOAuaeLRA8
site:*.dk intitle:index.of
AI Mode
All
Images
Videos
News
Short videos
Web
More
Tools
HOT'N TOT
https://www.hotntot.dk › _borders · Translate this page
Index of /_borders
Index of /_borders. Parent Directory · Anita 1_resize_resize_resize.jpg · Anita_r.jpg · Anita_resize.jpg · Betina2_resize_resize_resize.jpg · Betina_resize.
Dansk Lunge Cancer Gruppe
https://www.lungecancer.dk › wp-content › uploads
Index of /wp-content/uploads/2025/
Index of /wp-content/uploads/2025/ ; Up Parent Directory ; Directory 11, 2025-11-01 00:02, - ; Directory 10, 2025-10-01 00:05, - ; Directory 09, 2025-09-08 08:07, -.
Danmarks Tekniske Universitet - DTU
https://ftp.space.dtu.dk › data
Index of /data
Index of /data ; Description ; Parent Directory - ; DATA_MMIA/ 2012-11-02 17:33 - ; Ground_magnetometers/ 2018-03-12 10:16 - ; Ocean-circulation/ 2006-12-22 10:12 - ...

Premium tip: Google Dorking

Premium tip: Google dorking - 2026

defend Denmark

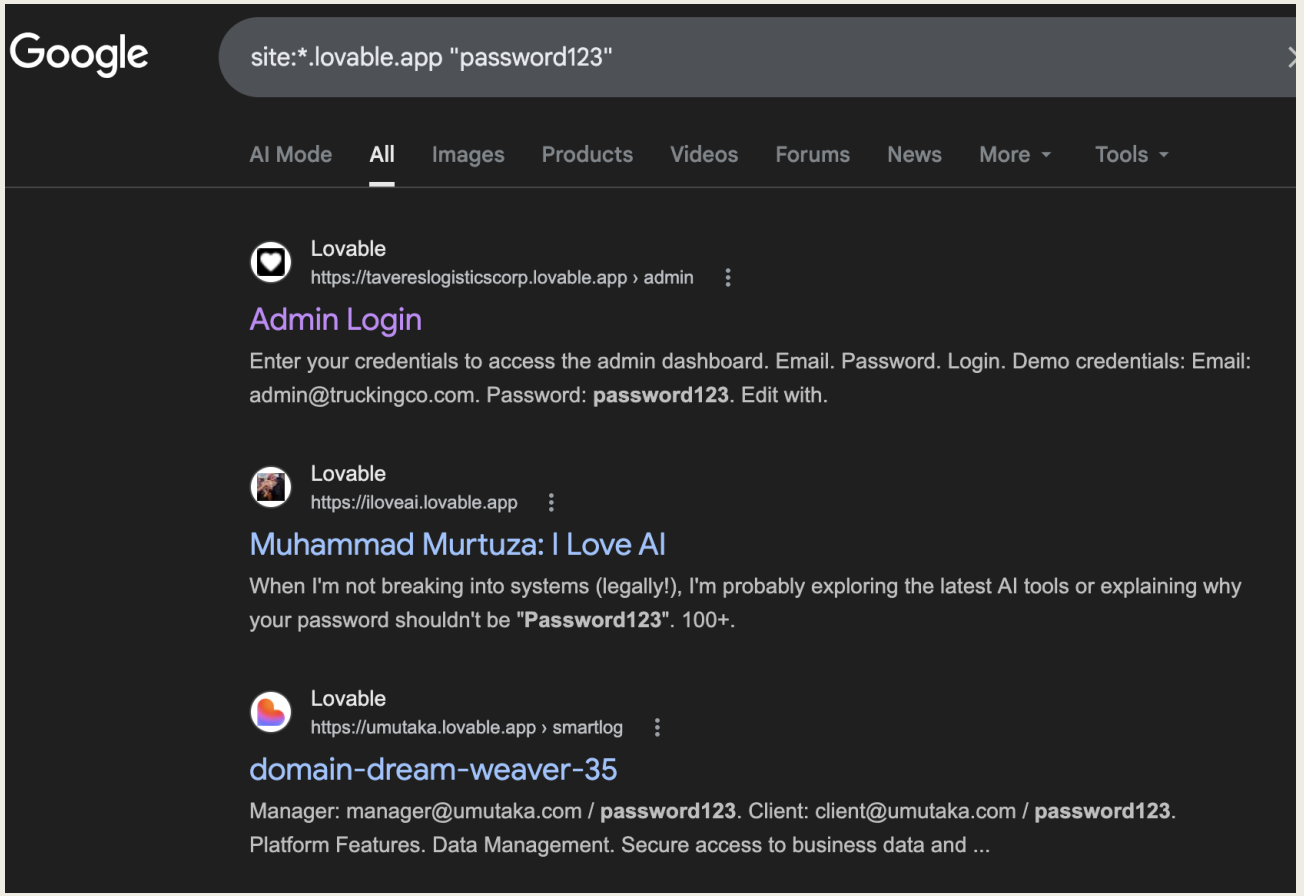


Premium tip: Google dorking - 2026

defend Denmark

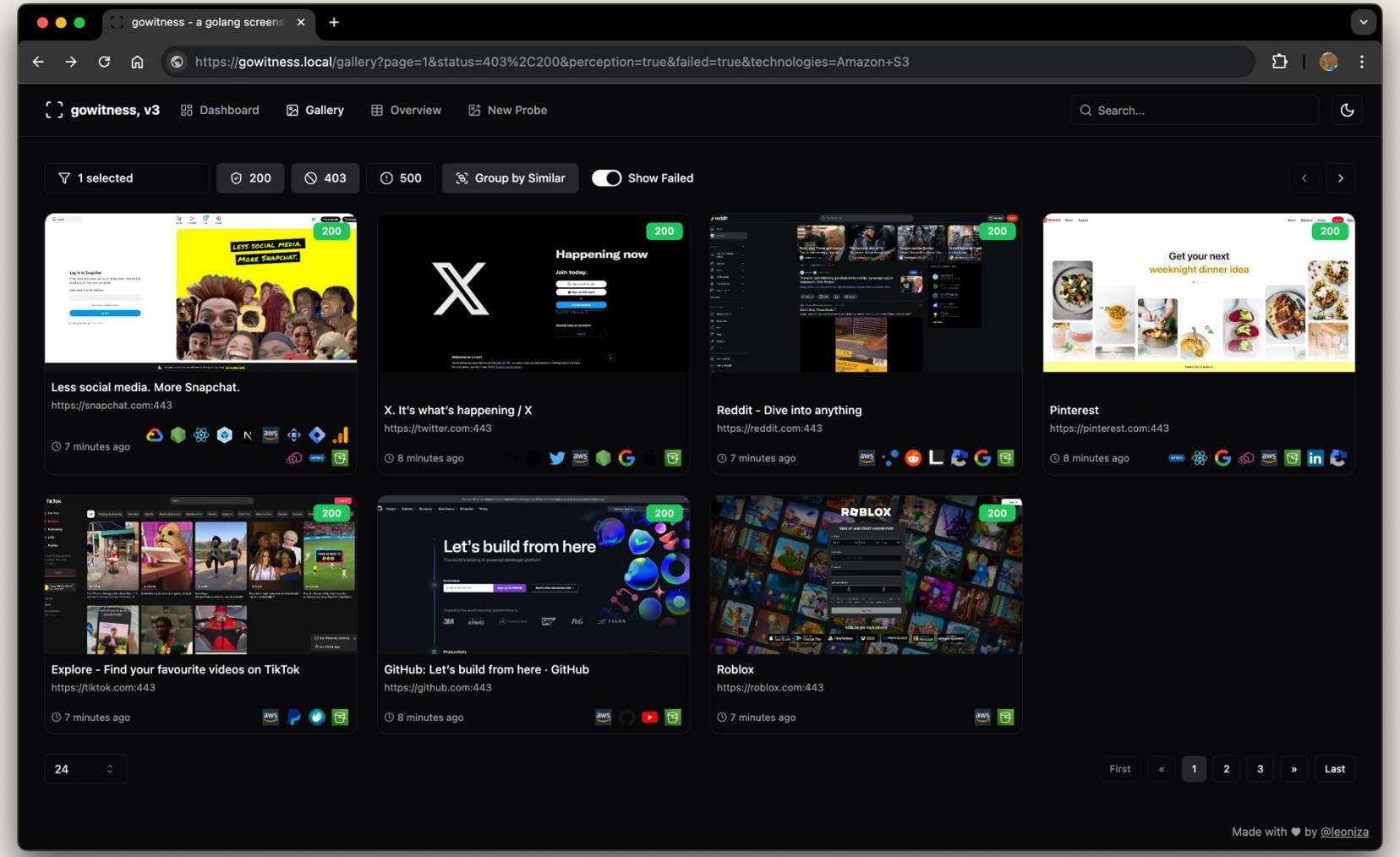
- Mange skubber vibe-coded produkter hurtigt ud I production
- Hvis de har opkobling til backend, så er der en mulighed for at udnytte dem
- Tjek de store vibe code platforme ud med google dorking:

```
site:*.vercel.app
site:*.netlify.app
site:*.pages.dev
site:*.fly.dev
site:*.railway.app
site:*.render.com
site:*.streamlit.app
site:*.hf.space
site:*.modal.run
site:*.workers.dev -
site:*.deno.dev
```



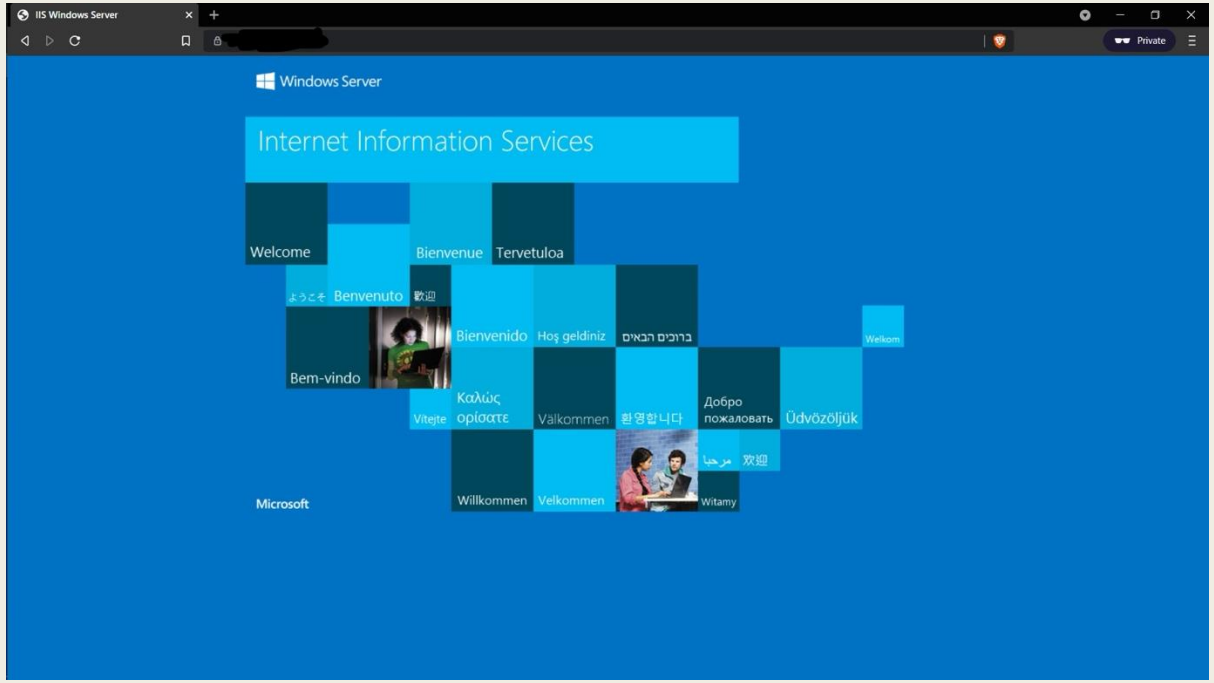
Tool: Gowitness?

- Given a list of targets, navigate to them and take a screenshot
  - *Allows us to much faster rule out stuff that is not relevant / that is relevant*
- https://github.com/sensepost/gowitness

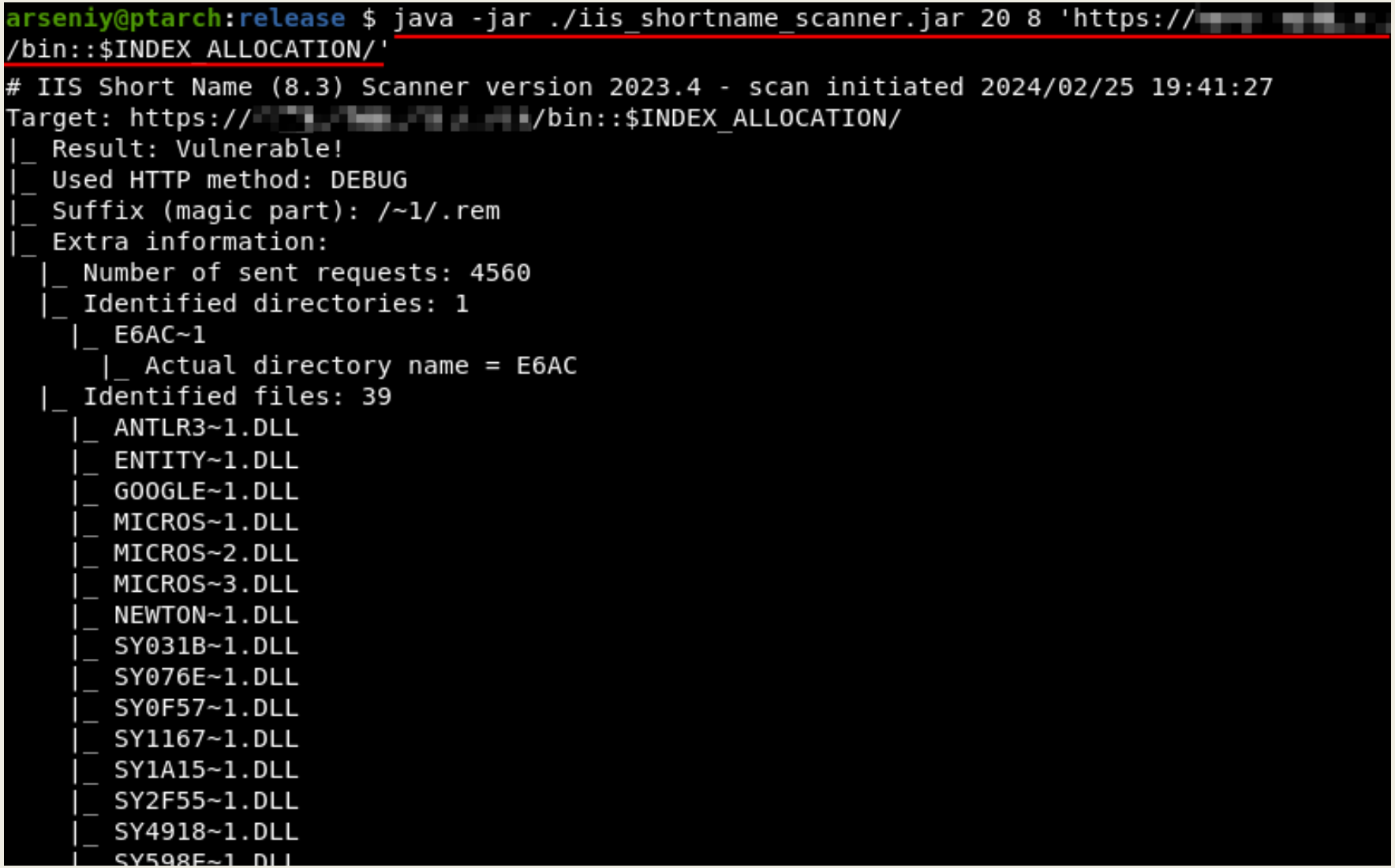


What are we looking for?

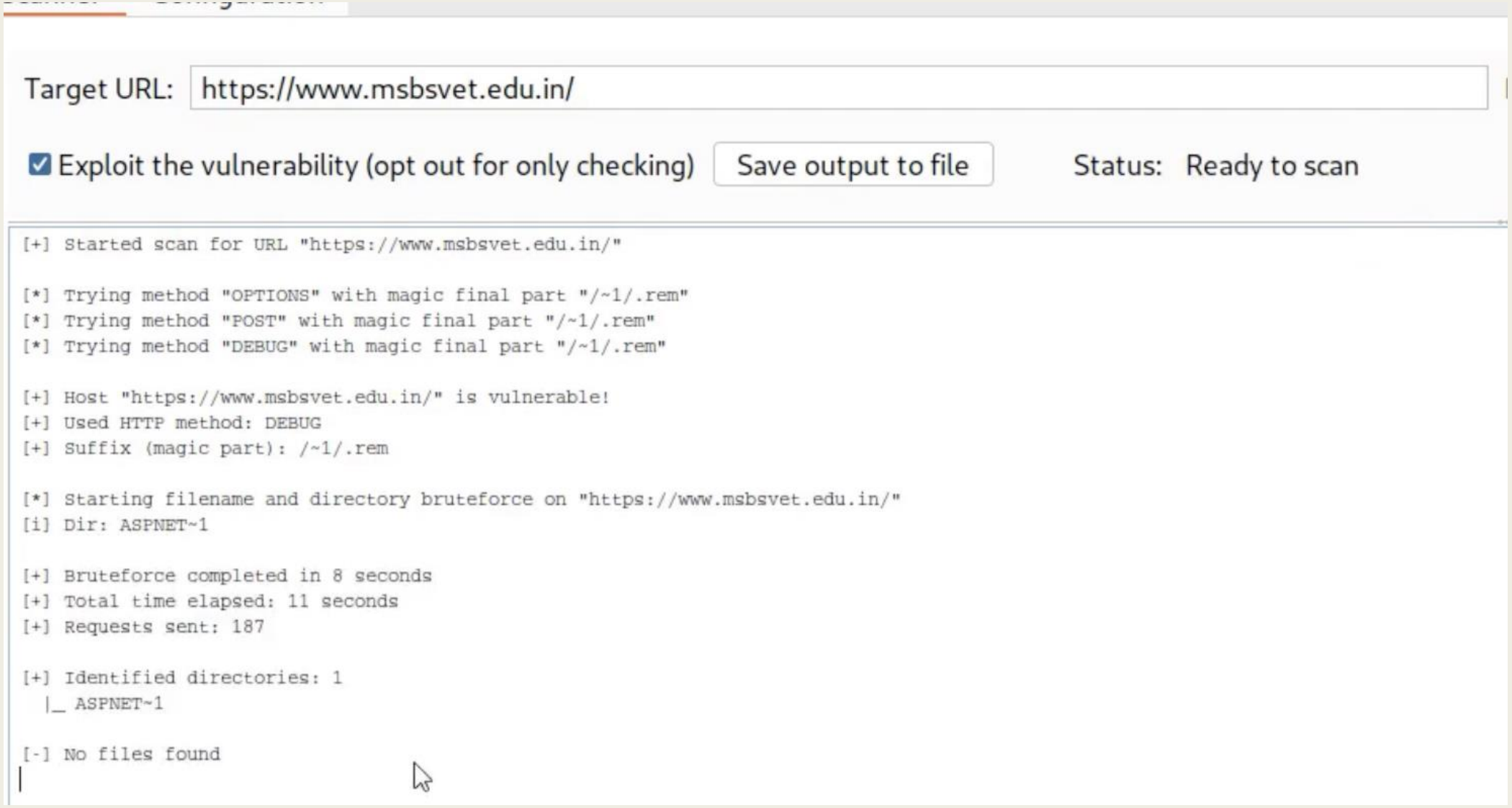
- Stuff that looks **OLD**
- Anything related to admin-panels
- Anything that looks like we can log in
- Default content (IIS, Tomcat ?)
- VPN stuff?
  - *Citrix, Ivanti, Fortinet, Palo Alto*
  - *Tons of vulnerabilities here*



Premium tip: IIS Tilde Enumeration scan



Premium tip: IIS Tilde Enumeration scan



Hack IIS servers when you find them

defend Denmark

shubs
@infosec_au

Why I love hacking IIS servers:
- Case insensitive, amazing for content discovery
- IIS Shortname
- VIEWSTATE deserialization RCE gadget
- Web.config upload tricks
- Debug mode w/ detailed stack traces and full path
- Debugging scripts often deployed (ELMAH, Trace)
- Telerik RCE

9:23 AM · Dec 21, 2020 · Twitter Web App

View Tweet activity

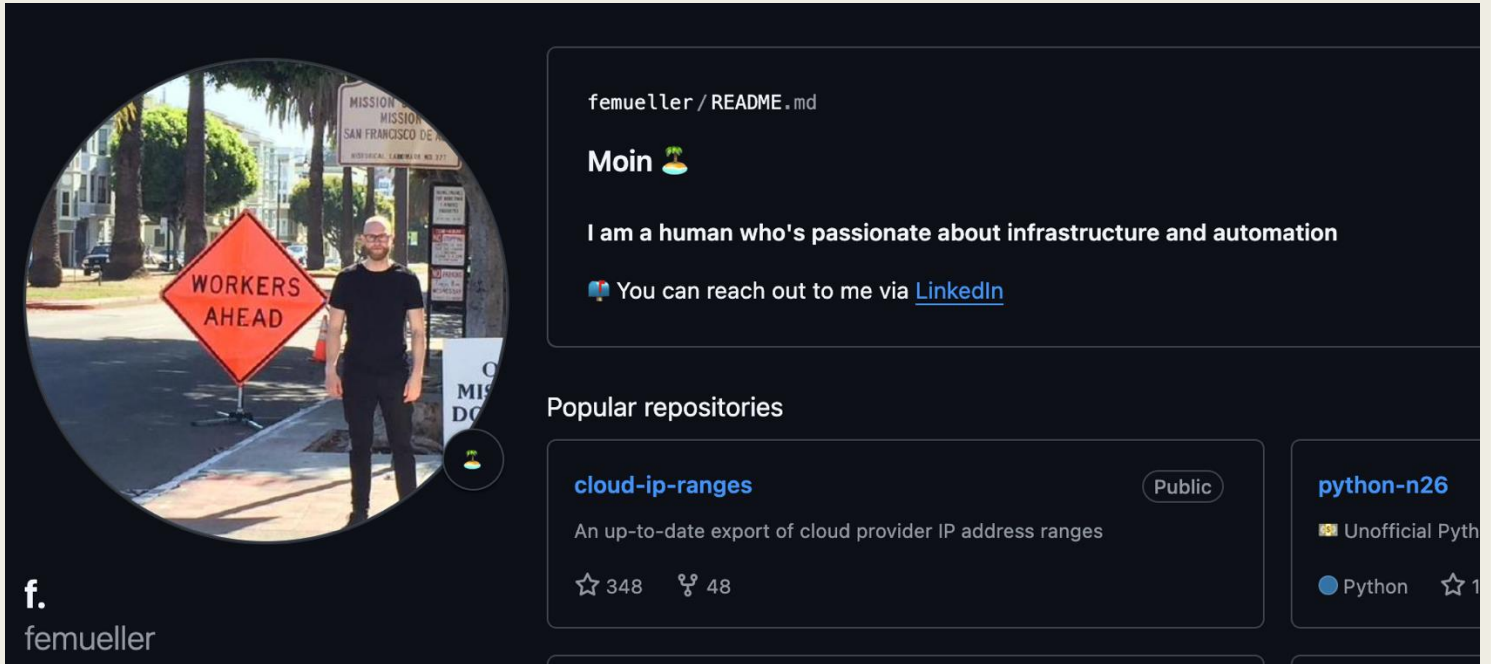
186 Retweets **2** Quote Tweets **938** Likes

Extra cloud recon

- The goal is ***still*** to find as many websites to hack
  - Many companies use cloud providers
  - Amazon AWS, Google Cloud, Azure
  - These cloud companies own certain IP ranges
  - You spin up a machine -> Get an IP
- We can query the IP's on 443 to get **certificate** information
- This may yield **NEW** main domains and subdomains

Extra cloud recon

- AWS- https://ip-ranges.amazonaws.com/ip-ranges.json
- Cloudflare
  - IPv4 - https://www.cloudflare.com/ips-v4
  - IPv6 - https://www.cloudflare.com/ips-v6
- DigitalOcean - https://digitalocean.com/geo/google.csv
- Google Cloud - https://www.gstatic.com/ipranges/cloud.json
- Oracle Cloud - https://docs.oracle.com/iaas/tools/public_ip_ranges.json
- Linode - https://geoip.linode.com/
- Azure??? - https://docs.microsoft.com/en-us/azure/virtual-network/public-ip-addresses



Extra cloud recon

- I have done this for you (In June)
- I will give you the data
- (it's a lot)
- BUT…
- Its without IP data, so if there is no domain resolution the other way, or cloudflare, you have to find it yourself.

```
~/Research/Caduceus_cloud_scans  (2.318s)
cat * | grep dpgmedia

atlassian-2-api.dpgmedia.net
atlassian-test-api.dpgmedia.net
dpgmedia.moreoptimal.com
dpgmedia.net
kubernetes-ingress-dpgmedia.dpgmedia
landingpage.dpgmedia.net
mijn-omgeving-attachments-acc.nonprod.mo.dpgmedia.cloud
moving-house-service-prod-api.179998496726.dpgmedia.cloud
payment-service-prod-api.179998496726.dpgmedia.cloud
pmpportal.dpgmedia.nl
sales.dpgmedia.be
videoproductie.dpgmedianl
*.249926456136.dpgmedia.cloud
*.724847031422.dpgmedia.cloud
*.datastudio.dpgmedia.cloud
*.dc.dpgmedia.cloud
*.dpgdsp-adv-nonprod.dpgmedia.cloud
*.dpgmedia.net
*.hr.dpgmedia.cloud
*.identity.dpgmedia.cloud
*.jawbreaker.dpgmedia.cloud
*.push-o-matic.471112909760.dpgmedia.cloud
atlassian-2-api.dpgmedia.net
atlassian-test-api.dpgmedia.net
dpgmedia.net
kubernetes-ingress-dpgmedia.dpgmedia
landingpage.dpgmedia.net
photohub-web.non-prod.picture.dpgmedia.cloud
photohub-web.standalone.non-prod.picture.dpgmedia.cloud
pmpportal.dpgmedia.nl
push-o-matic.471112909760.dpgmedia.cloud
sales.dpgmedia.be
seo-discover-non-prod.730335273431.dpgmedia.cloud
videobs.dpgmedia.cloud
videoproductie.dpgmedianl
```

NEW TARGET:

DPGMEDIA.CLOUD

and now we run the tools again over and over and over and over

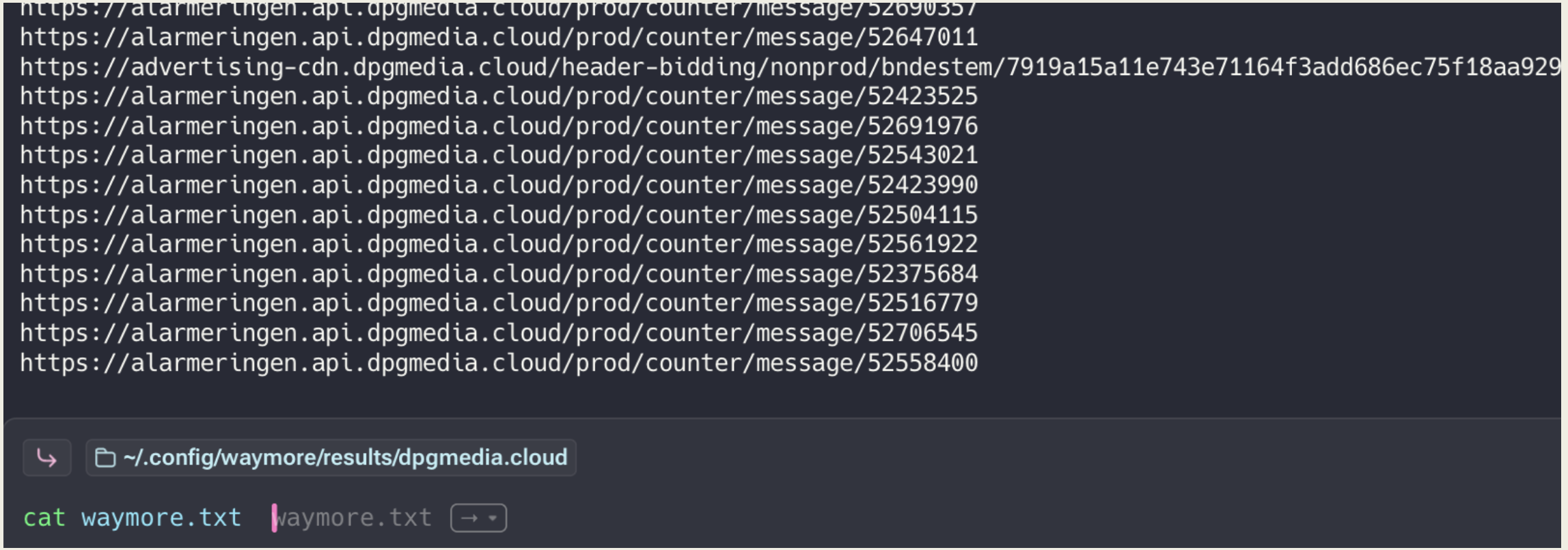
Tool: Waymore

- We want to take an apex domain
- And then figure out all full urls that this domain has ever been in
- We can use waybackarchives, but its good to also include other sources.
- **Waymore:**

```
waymore -i dpgmedia.cloud -mode U
```

Tool: Waymore

Tool: Waymore - Filtering



Tool: Waymore - Filtering

```
https://advertising-cdn.dpgmedia.cloud/header-bidding/prod/startpagina/5ccb4bd29b282904e96c04e09de8a92c1805bb8e.js
https://advertising-cdn.dpgmedia.cloud/header-bidding/prod/24kitchen/da7c0f81042d3e4aa4486395bbe8785c51985400.js
https://advertising-cdn.dpgmedia.cloud/native-templates/prod/hln/templates.js?version=471
https://advertising-cdn.dpgmedia.cloud/header-bidding/prod/mamaplaats/e597f302dc4e045b019660dad50b7e87982dda08.js
https://advertising-cdn.dpgmedia.cloud/native-templates/prod/24kitchen/templates.js?version=194
https://advertising-cdn.dpgmedia.cloud/native-templates/prod/7sur7/templates.js?version=405
https://advertising-cdn.dpgmedia.cloud/native-templates/prod/tubantia/templates.js?version=275
https://cdn-01.krantnl.dpgmedia.cloud/krant.nl-onderstroom/production/releases/1.2.89/60c6633fd48fd3591f35.js
https://cdn-01.krantnl.dpgmedia.cloud/krant.nl-onderstroom/production/releases/1.2.85/6d5604dc59d0632ffeb7.js
https://advertising-cdn.dpgmedia.cloud/native-templates/prod/hln/templates.js?version=636
https://advertising-cdn.dpgmedia.cloud/native-templates/prod/24kitchen/templates.js?version=161
https://advertising-cdn.dpgmedia.cloud/native-templates/prod/kekmama/templates.js?version=150
https://cdn-01.krantnl.dpgmedia.cloud/krant.nl-onderstroom/production/releases/1.2.77/54ecb6f8ea018a3917d8.js
https://advertising-cdn.dpgmedia.cloud/creative-enrichments/538847770.json
https://advertising-cdn.dpgmedia.cloud/native-templates/prod/brabantsdagblad/templates.js?version=359
https://advertising-cdn.dpgmedia.cloud/header-bidding/prod/autoweek/6ea15d06c7863565dc9fc2dafd65448bfc943496.js
https://advertising-cdn.dpgmedia.cloud/native-templates/prod/top40/templates.js?version=153
https://advertising-cdn.dpgmedia.cloud/native-templates/prod/gelderlander/templates.js?version=235
https://advertising-cdn.dpgmedia.cloud/header-bidding/nonprod/bndestem/7919a15a11e743e71164f3add686ec75f18aa929.js

~/.config/waymore/results/dpgmedia.cloud

cat waymore.txt | grep -v message  waymore.txt
```

Tool: Waymore - Filtering

```
https://cdn-01.krantnl.dpgmedia.cloud/krant.nl-onderstroom/production/releases/1.2.97/6ca69ba.js
http://nou-images-test.magazines.dpgmedia.cloud/
https://sto-web-prod.magazines.dpgmedia.cloud/
http://freewheel-prod.dpgdsp-adv-prod.dpgmedia.cloud/
https://cdn-01.krantnl.dpgmedia.cloud/krant.nl-onderstroom/production/releases/1.2.82/f9c7d372d4ee108376e8.js
https://cdn-01.krantnl.dpgmedia.cloud/krant.nl-onderstroom/production/releases/1.2.83/c877b6935816dbf84617.js
https://cdn-03.tapp.dpgmedia.cloud/tapp-verticals-lossebladen/production/releases/2.0.85/Checkout.js
https://frontend.kijk-live.radio.dpgmedia.cloud/_nuxt/CMdla_7R.js
http://creative.dpgdsp-adv-prod.dpgmedia.cloud
https://podcast.api.dpgmedia.cloud/shows/politieke-podcast/de-toptransfer-van-coenradie-kan-iets-losmaken-op-rechts/cl
https://cdn-01.krantnl.dpgmedia.cloud/krant.nl-onderstroom/production/releases/1.2.91/7afcb97.js
https://cdn-01.krantnl.dpgmedia.cloud/krant.nl-onderstroom/production/releases/1.2.80/455dbfbde0913f47fd1a.js
https://familieberichten-test.advalue.dpgmedia.cloud/
https://embrace.api.distributie.dpgmedia.cloud/
https://cdn-01.krantnl.dpgmedia.cloud/tapp-onderstroom/production/releases/1.2.98/b86b554.js
https://vsg-videoservice-test.magazines.dpgmedia.cloud/
https://cdn-01.krantnl.dpgmedia.cloud/krant.nl-onderstroom/production/releases/1.2.89/60c6633fd48fd3591f35.js
https://cdn-01.krantnl.dpgmedia.cloud/krant.nl-onderstroom/production/releases/1.2.85/6d5604dc59d0632ffeb7.js
https://cdn-01.krantnl.dpgmedia.cloud/krant.nl-onderstroom/production/releases/1.2.77/54ecb6f8ea018a3917d8.js
```

```
~/.config/waymore/results/dpgmedia.cloud

cat waymore.txt | grep -v message | grep -v advertising
```

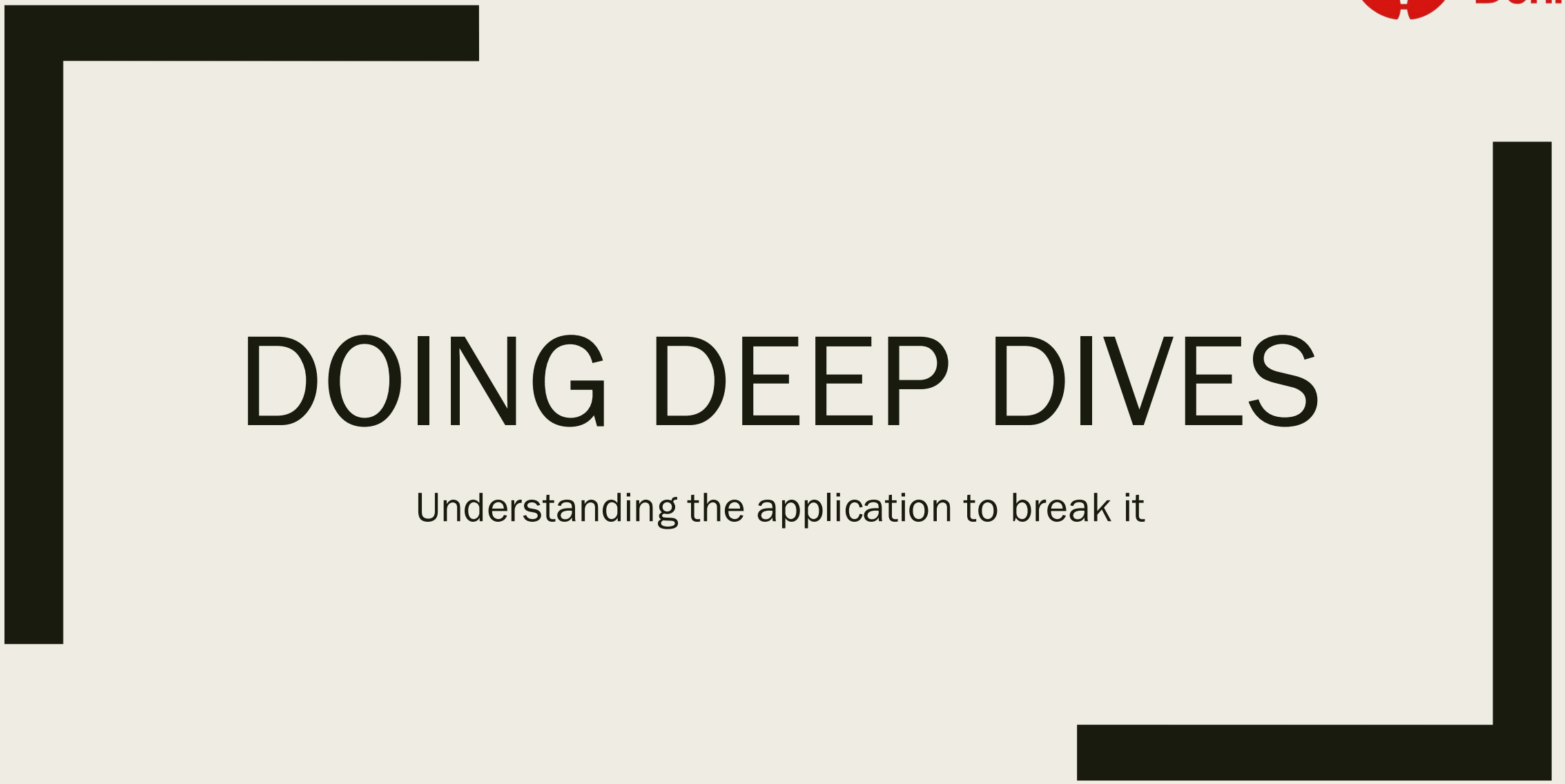
Tool: Waymore – or just going for gold

defend Denmark

```
~/.config/waymore/results/dpgmedia.cloud  (10.603s)
cat waymore.txt | grep login | httpx -status-code -title -content-length -web-server  -follow-redirects -t 50 -no-fallback
http://acc.bo.tapp.dpgmedia.cloud/login [403] [453] [Access Denied] []
http://cognito.auth.471112767068.dpgmedia.cloud/login?approval_prompt=force&client_id=1qeffg9q3k8fqaocg5v6ng0adl&redirect_uri=https%3A%2F%2Fstag.joe.be%2Foauth2%2Fcallback&response_type=code&scope=openid+email&state=jGuqTRmV96ToBMr8kmdXyU5c8-0q42DOMZmywiuEumU%3A%2F [403] [915] [ERROR: The request could not be satisfied] [CloudFront]
https://acc.bo.tapp.dpgmedia.cloud/login [403] [453] [Access Denied] []
http://profileservice.familieberichten.test-olr.dpgmedia.cloud/core/login?signin=b97a640b009793d15ad2f2b17f00ab7b [403] [453] [Access Denied] []
http://backoffice.familieberichten.test-olr.dpgmedia.cloud/login?ReturnUrl=%2F [403] [453] [Access Denied] []
https://prod.bo.tapp.dpgmedia.cloud/login [403] [453] [Access Denied] []
https://profileservice.familieberichten.test-olr.dpgmedia.cloud/core/login?signin=1537e69c06eb54f75c0d64b47b21401d [403] [453] [Access Denied] []
https://profileservice.familieberichten.test-olr.dpgmedia.cloud/core/login?signin=b97a640b009793d15ad2f2b17f00ab7b [403] [453] [Access Denied] []
https://backoffice.familieberichten.test-olr.dpgmedia.cloud/login?ReturnUrl=%2F [403] [453] [Access Denied] []
https://player-creator.radio.dpgmedia.cloud/login [200] [5555] [Qmusic - Players Management] [nginx]
http://prod.bo.tapp.dpgmedia.cloud/login [301,403] [453] [Access Denied] []
http://profileservice.familieberichten.test-olr.dpgmedia.cloud/core/login?signin=1537e69c06eb54f75c0d64b47b21401d [301,403] [453] [Access Denied] []
https://vr-events.radio.dpgmedia.cloud/login [200] [5122] [DPG Radio - Visual Radio for Events] [nginx]
https://popular-web-next.team010.dpgmedia.cloud/login?dpg_campaign=stdc_ed&dpg_medium=comments&dpg_source=ed&callback_url=https%3A%2F%2Fpopular-web-next.team010.dpgmedia.cloud%2Feindhoven%2Fde-verdwijntruc-van-niet-kunstenaar-leo-van-vegchel-ik-wil-mijn-nabestaanden-niet-opschepen-met-mijn-werk~a996af45%2F [] [17] [awselb/2.0]
https://popular-web-next.team010.dpgmedia.cloud/login?dpg_source=ed&callback_url=https%3A%2F%2Fpopular-web-next.team010.dpgmedia.cloud%2Fbinnenland%2Fterrorisme-via-tiktok-14-jarigen-verspreidden-propaganda-van-is~a8c07eb9%2F&dpg_campaign=stdc_ed&dpg_medium=menu [] [17] [awselb/2.0]
https://popular-web-next.team010.dpgmedia.cloud/login?dpg_campaign=stdc_dg&dpg_medium=comments&dpg_source=dg&callback_url=https%3A%2F%2Fpopular-web-next.team010.dpgmedia.cloud%2Fsport%2Fd [] [17] [awselb/2.0]
https://popular-web-next.team010.dpgmedia.cloud/login?dpg_campaign=stdc_dg&dpg_medium=comments&dpg_source=dg&callback_url=https%3A%2F%2Fpopular-web-next.team010.dpgmedia.cloud%2Fbi [] [17] [awselb/2.0]
https://popular-web-next.team010.dpgmedia.cloud/login?dpg_campaign=stdc_pzc&dpg_medium=menu&dpg_source=pzc&callback_url=https%3A%2F%2Fpopular-web-next.team010.dpgmedia.cloud%2Frotterdam%2Fwillem-van-hanegem-zwaar-geraakt-door-overlijden-feyenoord-legende-kindvall-dacht-dat-hij-onsterfelijk-was~a55aa01c%2F [] [17] [awselb/2.0]
https://popular-web-next.team010.dpgmedia.cloud/login?dpg_campaign=stdc_ed&dpg_medium=comments&dpg_source=ed&callback_url=https%3A%2F%2Fpopular-web-next.team010.dpgmedia.cloud%2F [] [17] [awselb/2.0]
http://player-creator.radio.dpgmedia.cloud/login [301,200] [5555] [Qmusic - Players Management] [nginx]
https://popular-web-next.team010.dpgmedia.cloud/login?dpg_medium=menu&dpg_source=ed&callback_url=https%3A%2F%2Fpopular-web-next.team010.dpgmedia.cloud%2Feindhoven%2Fgraffiti-battle-in-berenkuil-nog-niet-ten-einde-fuck-hamas-free-hostages-is-overgeschilderd~a3d3fc21%2F&dpg_campaign=stdc_ed [] [17] [awselb/2.0]
```

THAT'S IT FOR RECON

I mean there are millions of more tips, but we cannot cover them all



DOING DEEP DIVES

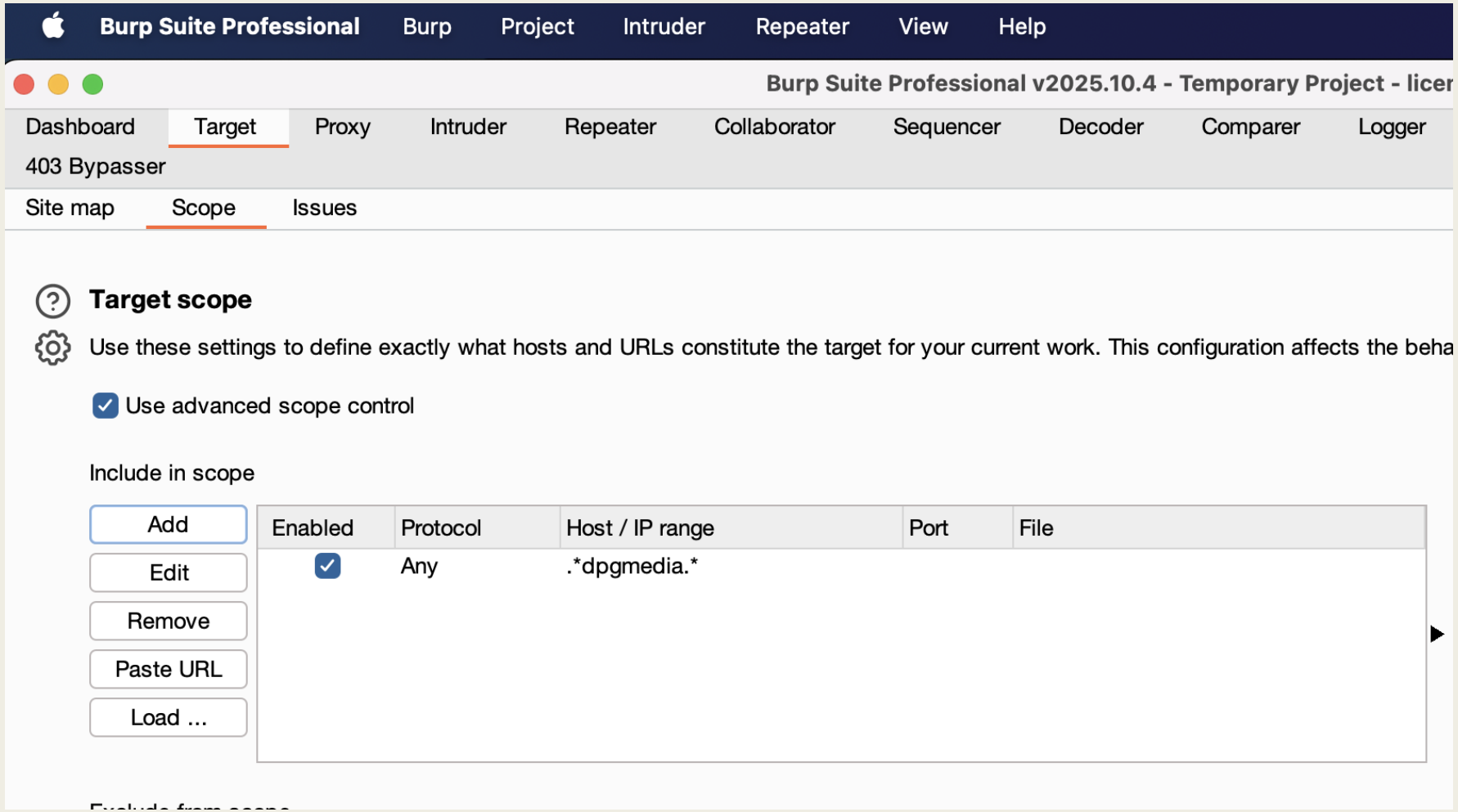
Understanding the application to break it

defend Denmark

Spin up your favourite tool

Burpsuite - scope

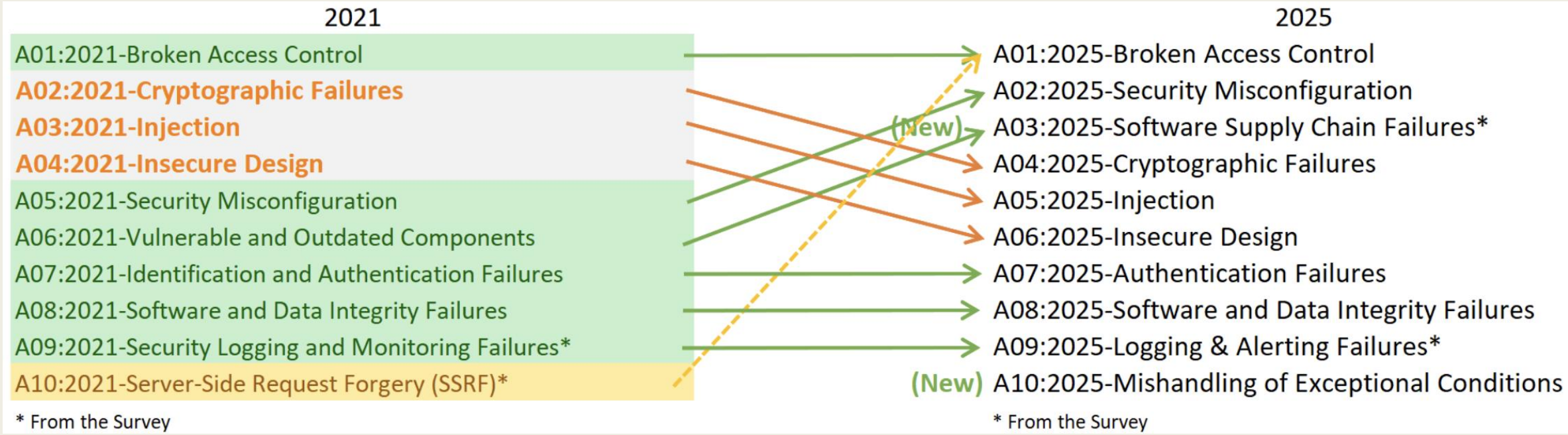
- Set this immediately to ensure you don't lose track in the overview



Our goal is to find deep complex functionality

- This is often behind auth
  - *Here is our chance to hack other users of the platform (usually higher impact)*
  - *We can test for **Access control issues***
- Also often behind payment, so we may have to spend some money on some product
  - *Fewer testers, more chance of bugs*
- If we can get accounts of different levels, this is desirable.
  - *Test privilege escalations*

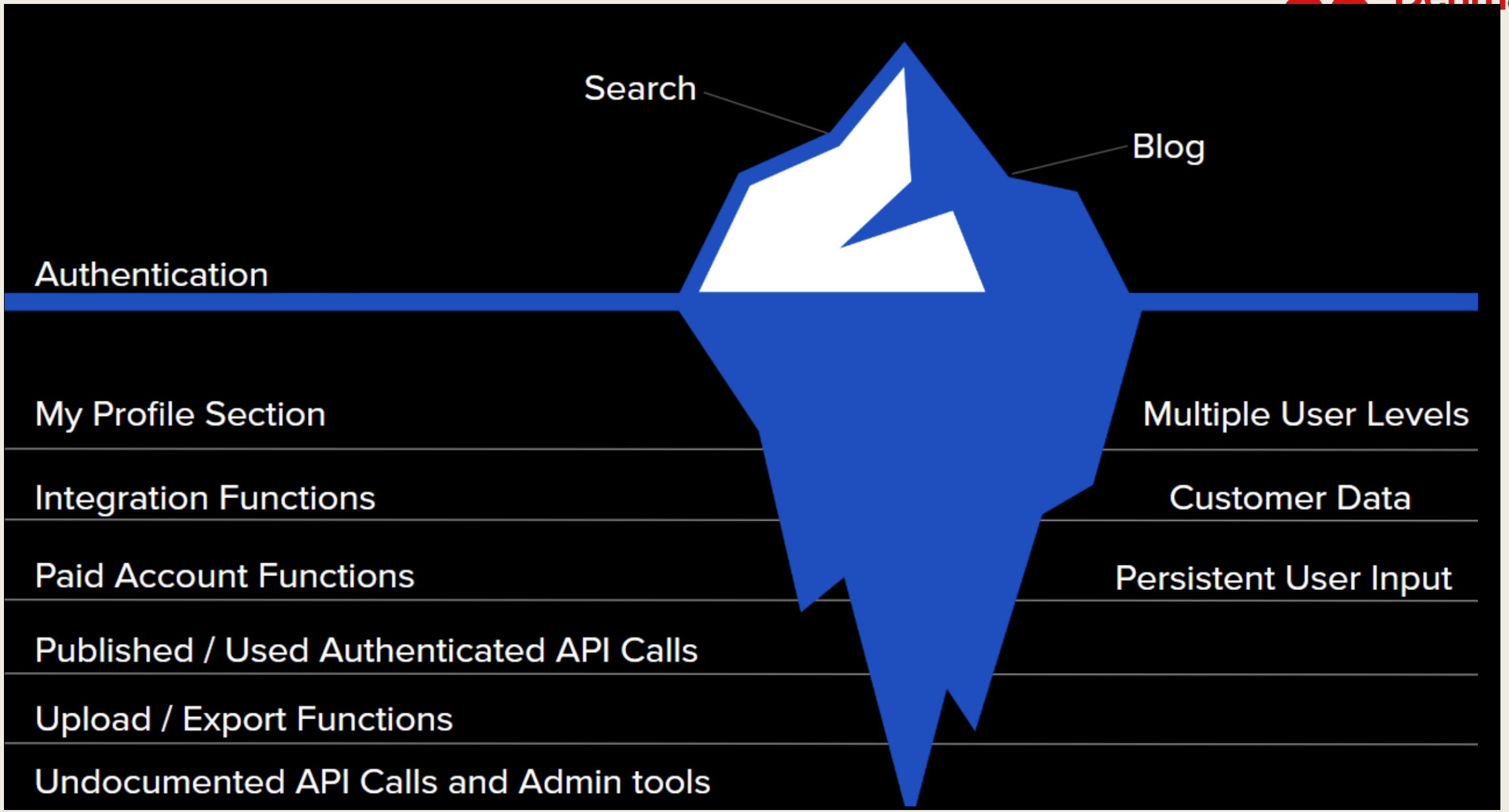
Look at these OWASP TOP 10 vulns



Access control still number 1, how hard can it be???

Apparantly it IS hard

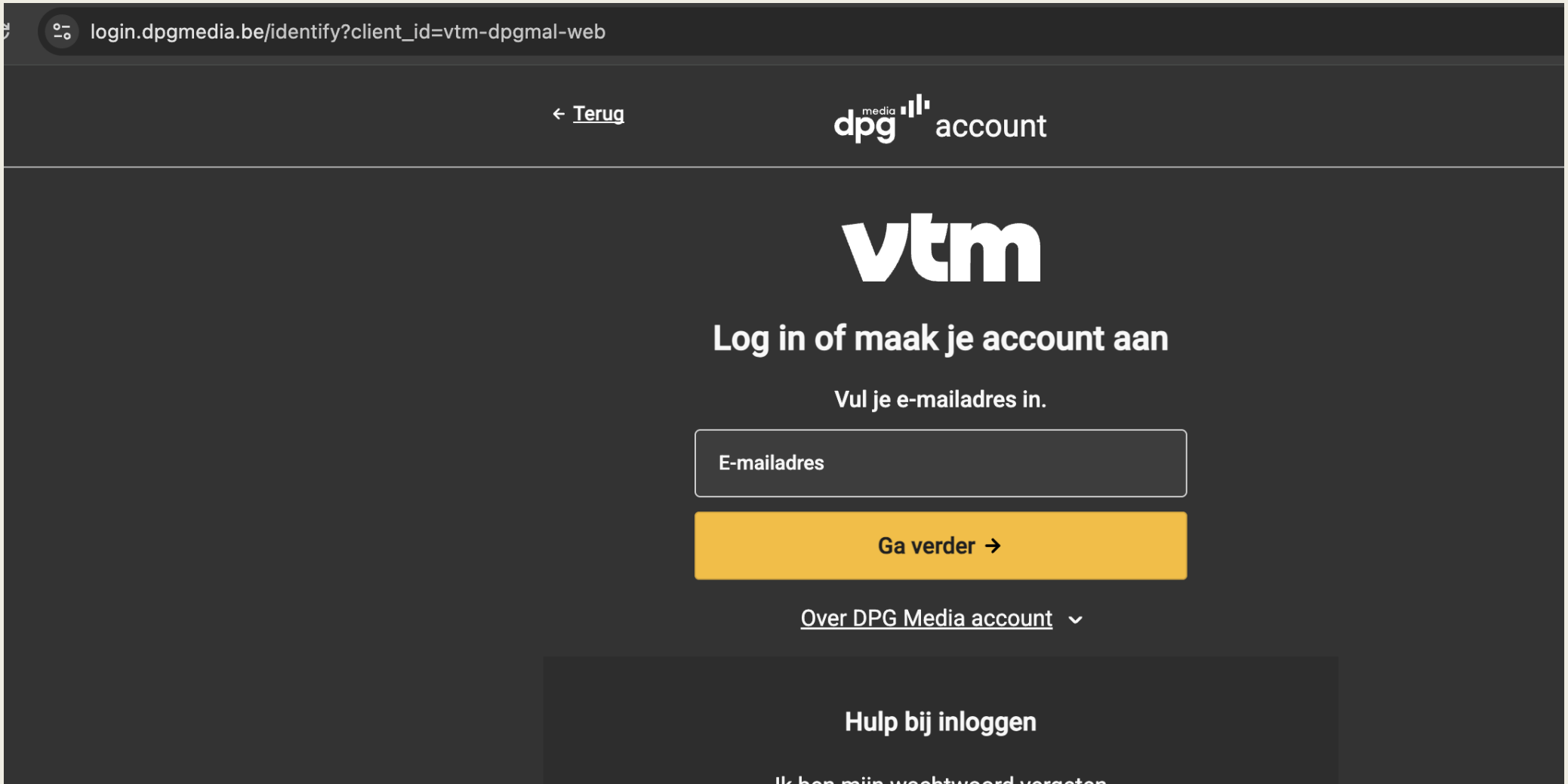
defend Denmark



Src jhaddix bbh mentality

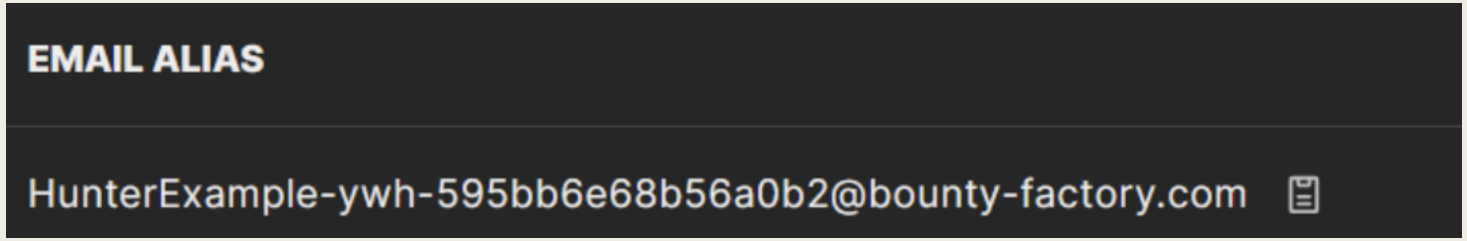
Lets create an account

https://login.dpgmedia.be/identify?client_id=vtm-dpgmal-web



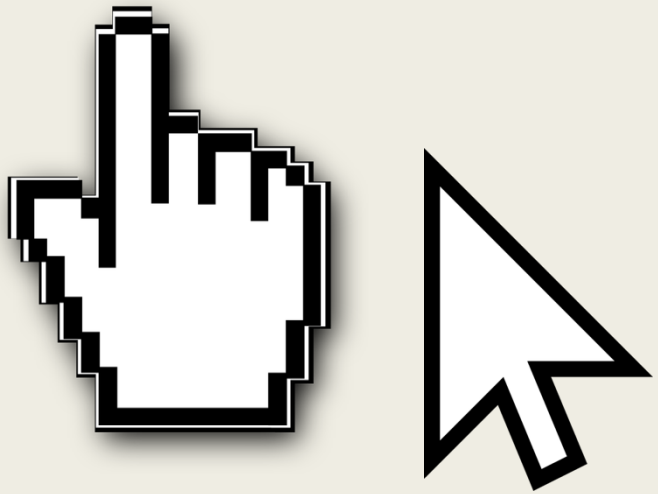
Lets create an account - Notice

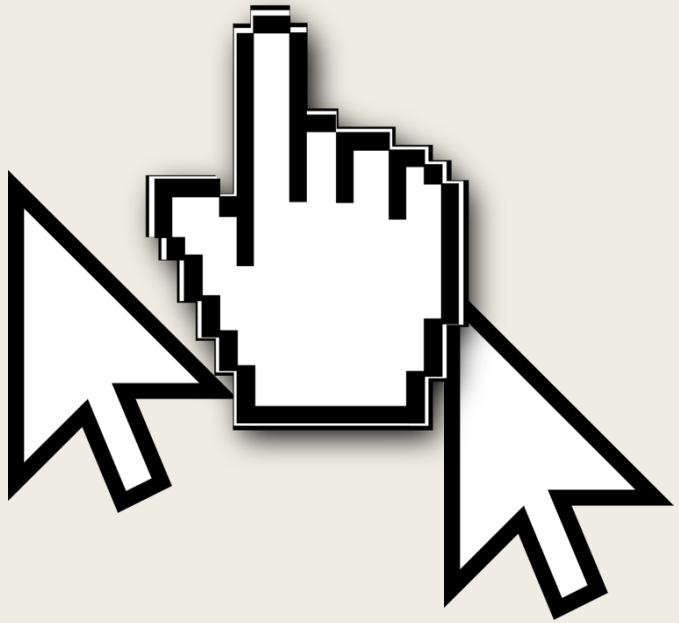
- Remember to use the email accounts from the platforms
- Remember to use the email accounts from the platforms
- They are essentially email forwarders
- Helps the defensive teams see you are doing good faith research
  - Intigriti: username@intigriti.me
  - Hackerone: username@wearehackerone.com
  - YWH: ?

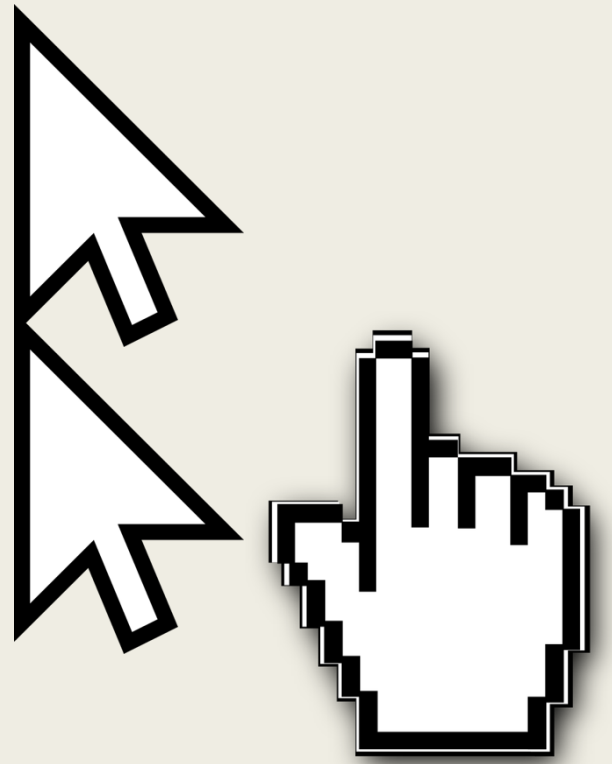


Now... CLICK EVERYTHING

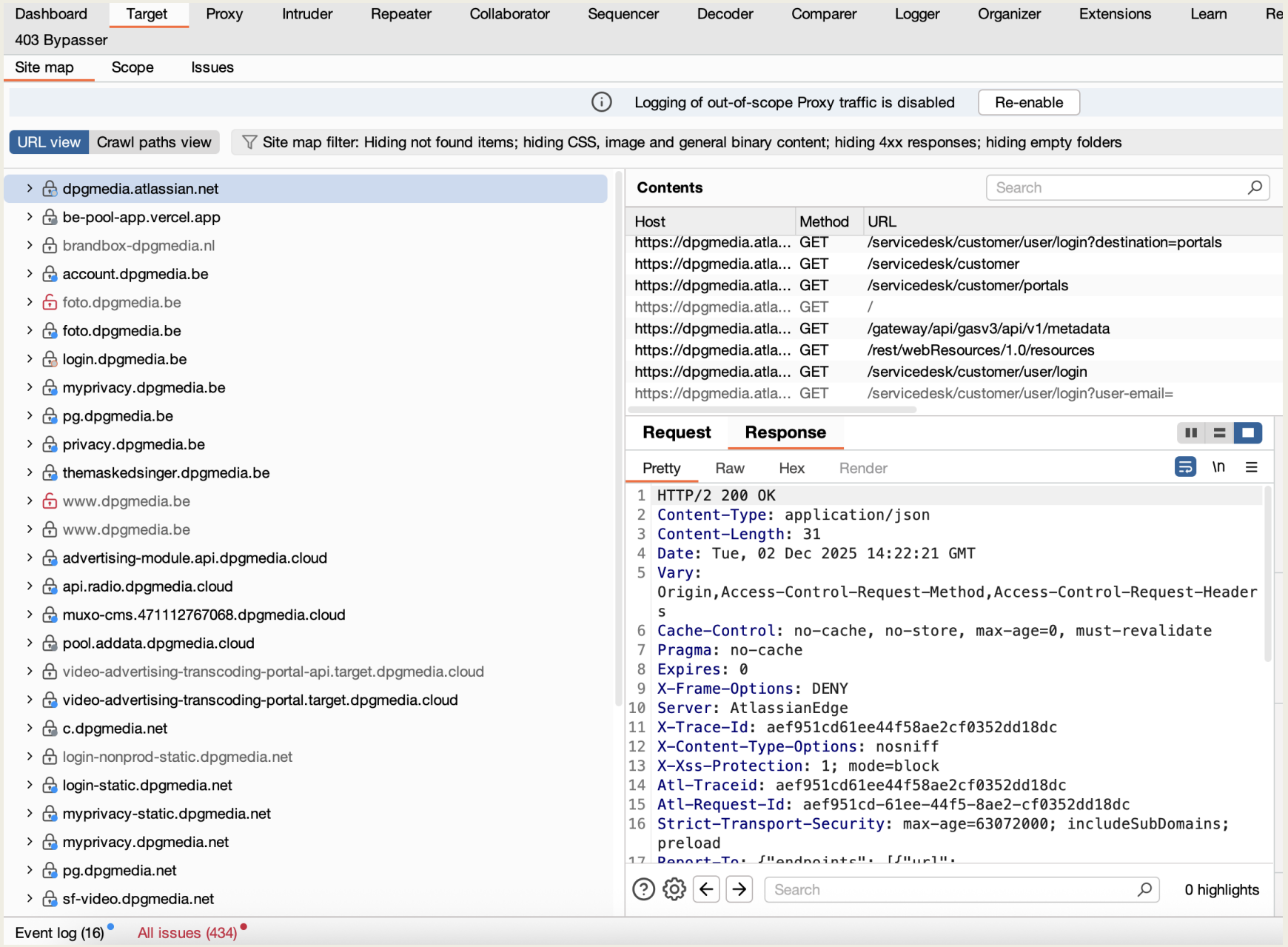
- Now its time to become a superuser of the application
- Click everywhere, while your proxy picks up information
- Try to just do everything there is to do in the application



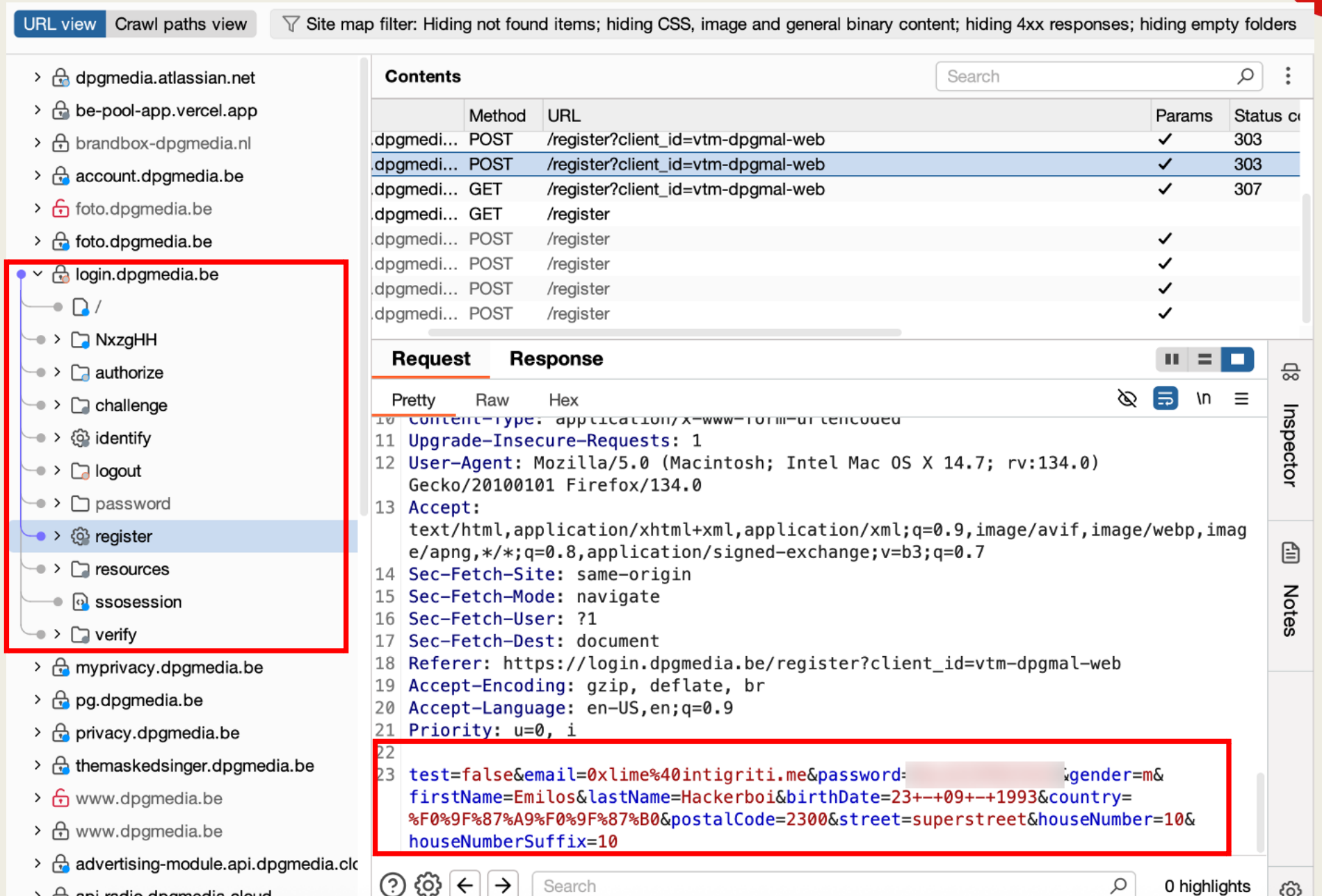




Deep Dive Data in Burpsuite -- Target view



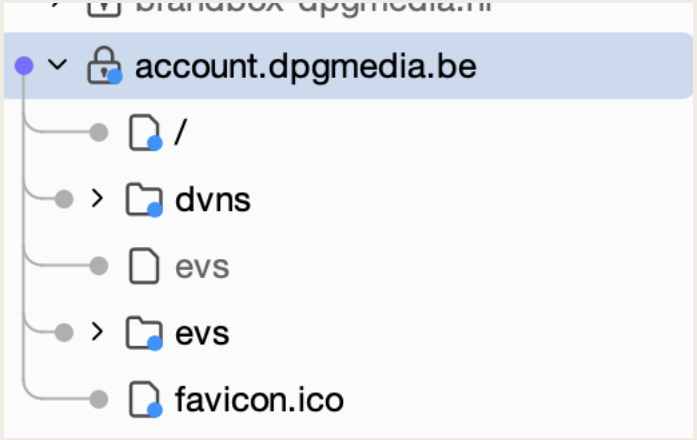
Registering flow



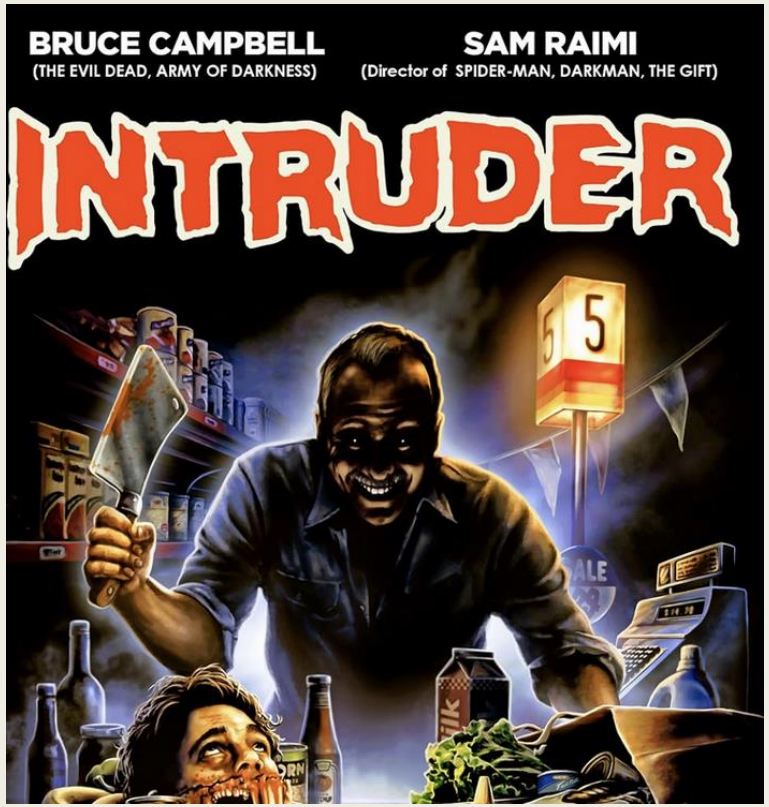
BURP PLUGINS AND TOOLS THAT I LIKE

My favourite tools for analysis
Burp Intruder

- The account.dpgmedia.be is quite sparse:



- Lets use intruder to see if we can find more endpoints



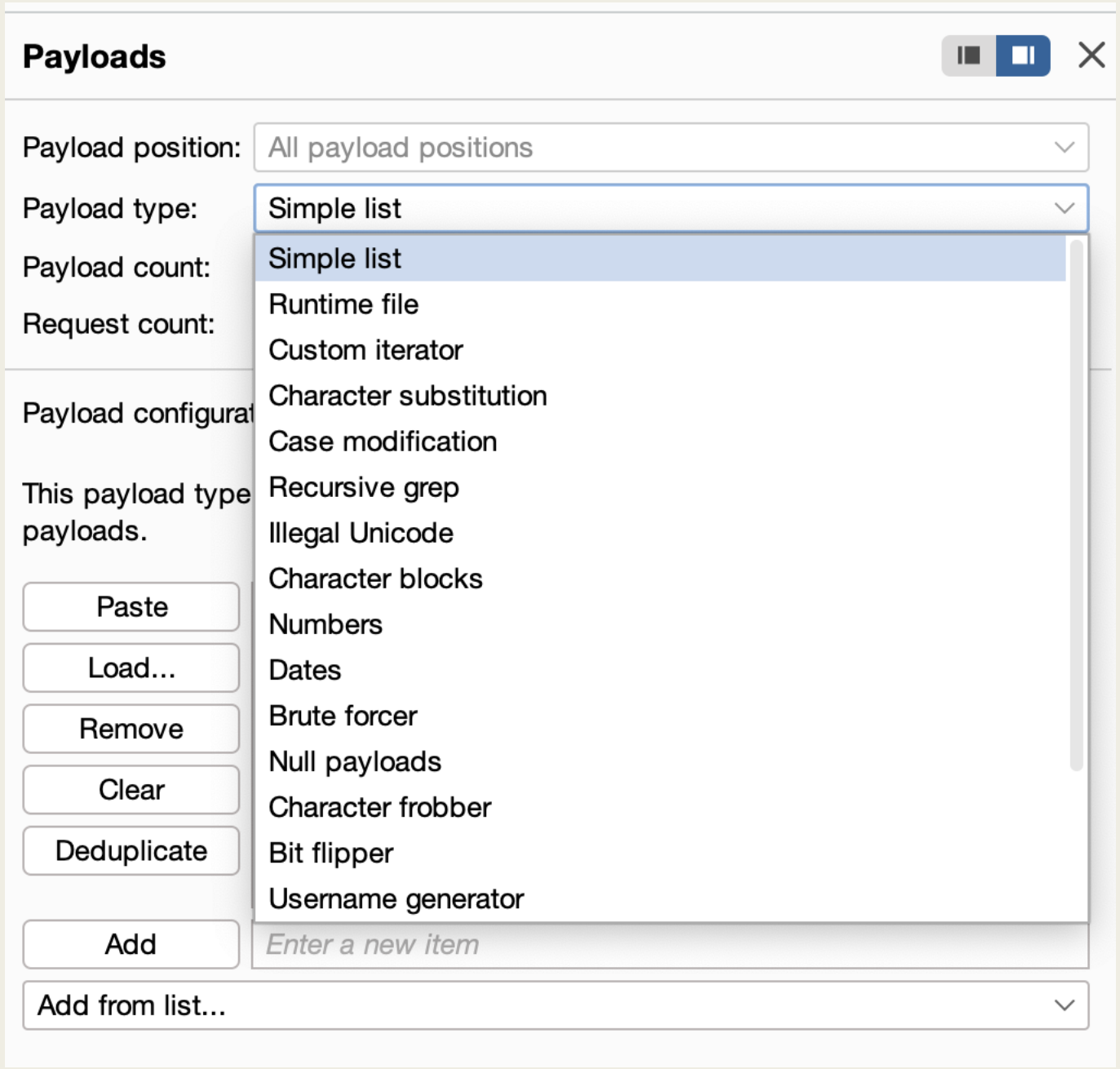
defend Denmark

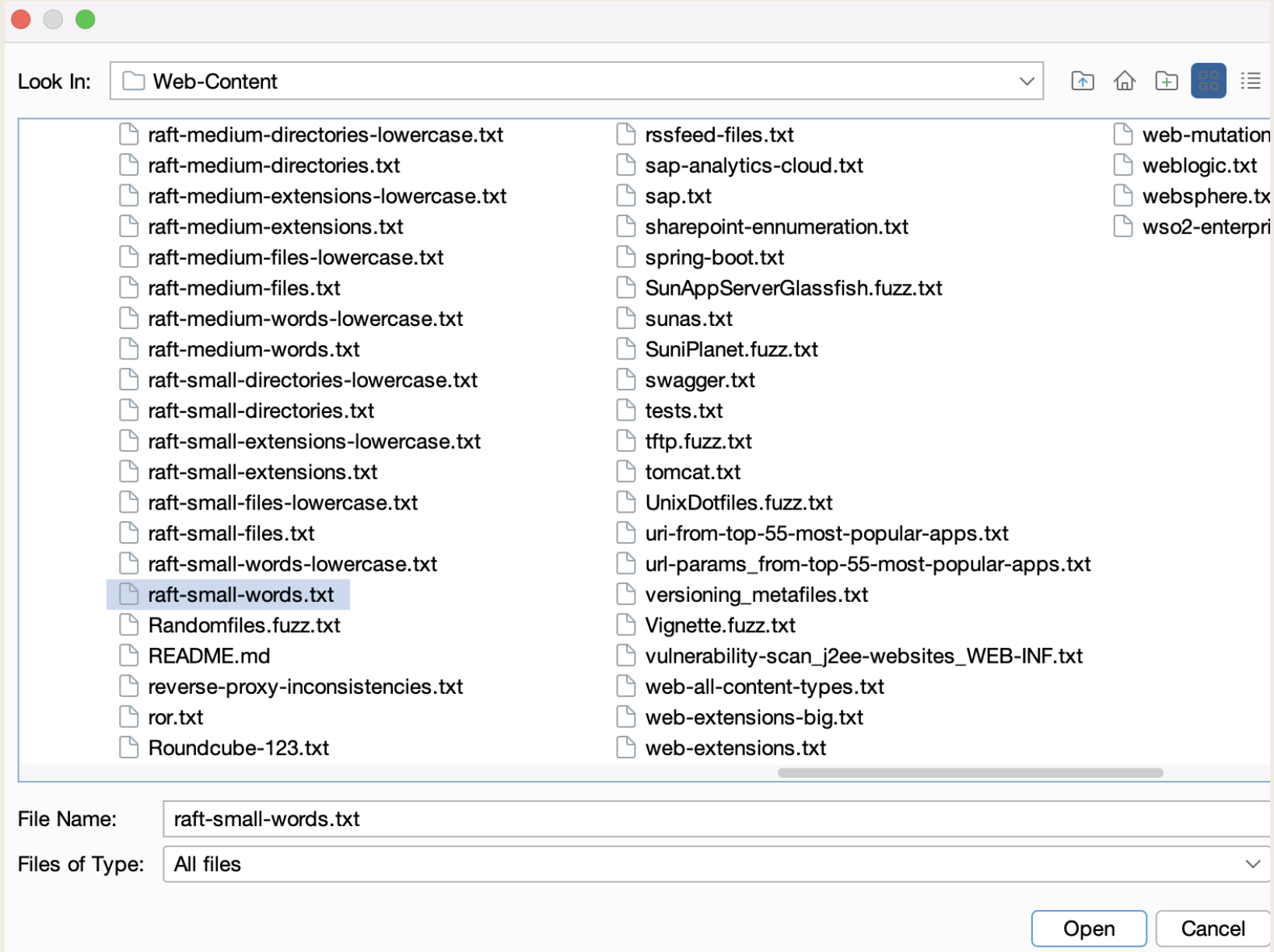
Sniper attack

Target https://account.dpgmedia.be

Positions Add § Clear § Auto §

```
1 GET /§§ HTTP/1.1
2 Host: account.dpgmedia.be
3 Cookie: _vwo_uuid_v2=D901420110C14D6B80AA4D40AF9CD393D|a529425529a61126540
  =
  448D71BD2A220E6F83F2B99C41D7C5F7~000000000000000000000000000000~YAAQb5tkXy
  dacrZOZZJfSXNrzjbEEGvVUPgLd0TltSc6usPfvTynML9CwjrIvdysTtaT8wFiGP4vYDOT2x7F
  eshAUMj98mn7ATGsyC/4Vnc5Jq4fYj7XzbgBW1+aKOpDsmeFIV+NK9uBowvadaK92tWp+oL8xp
  kBHlk8Kx4BcUAjXF7QN9dbAuGo64c0glBkHwMo2AS+pwJYx79xD+I3tHcV7QwygrjDsIsJkbDE
  AF3lLF/t5hXN;  sp_ses.ed2c=*;  _ga=GA1.2.1684826722.1764693284;  _gid=GA1.2.
```





Pick up the list at: https://github.com/danielmiessler/SecLists

defend Denmark

5. Intruder attack of https://account.dpgmedia.be

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

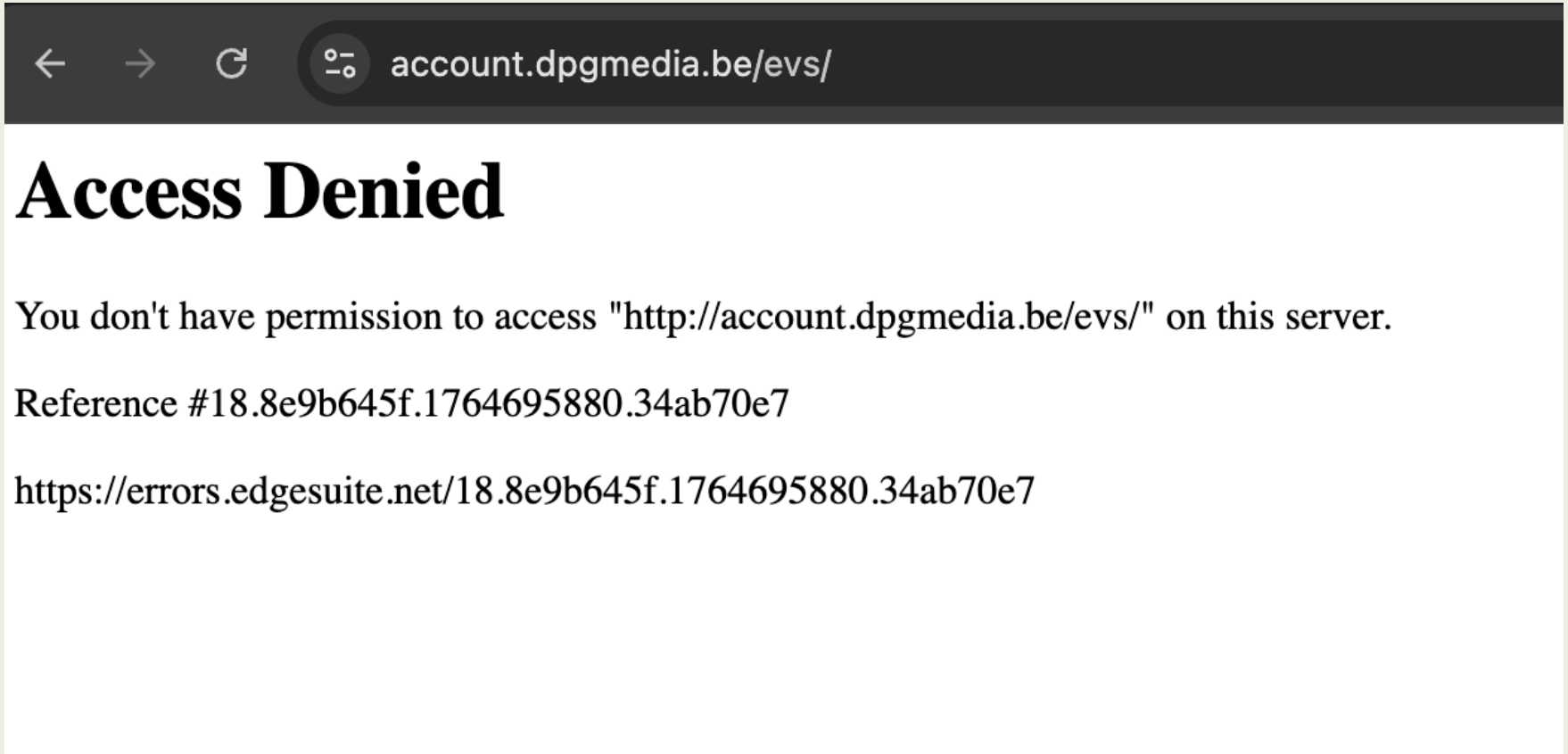
Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
203	Login	404	73			3860	
0		503	48			1785	
1	.php	503	53			1785	
2	cgi-bin	503	37			1785	
3	images	503	40			1785	
4	admin	503	36			1785	
5	includes	503	38			1785	
6	search	503	45			1785	
7	.html	503	53			1785	
8	cache	503	40			1785	
10	modules	503	35			1785	
11	templates	503	37			1785	
12	plugins	503	39			1785	
13	wp-admin	503	43			1785	

Request Response

Pretty Raw Hex Render

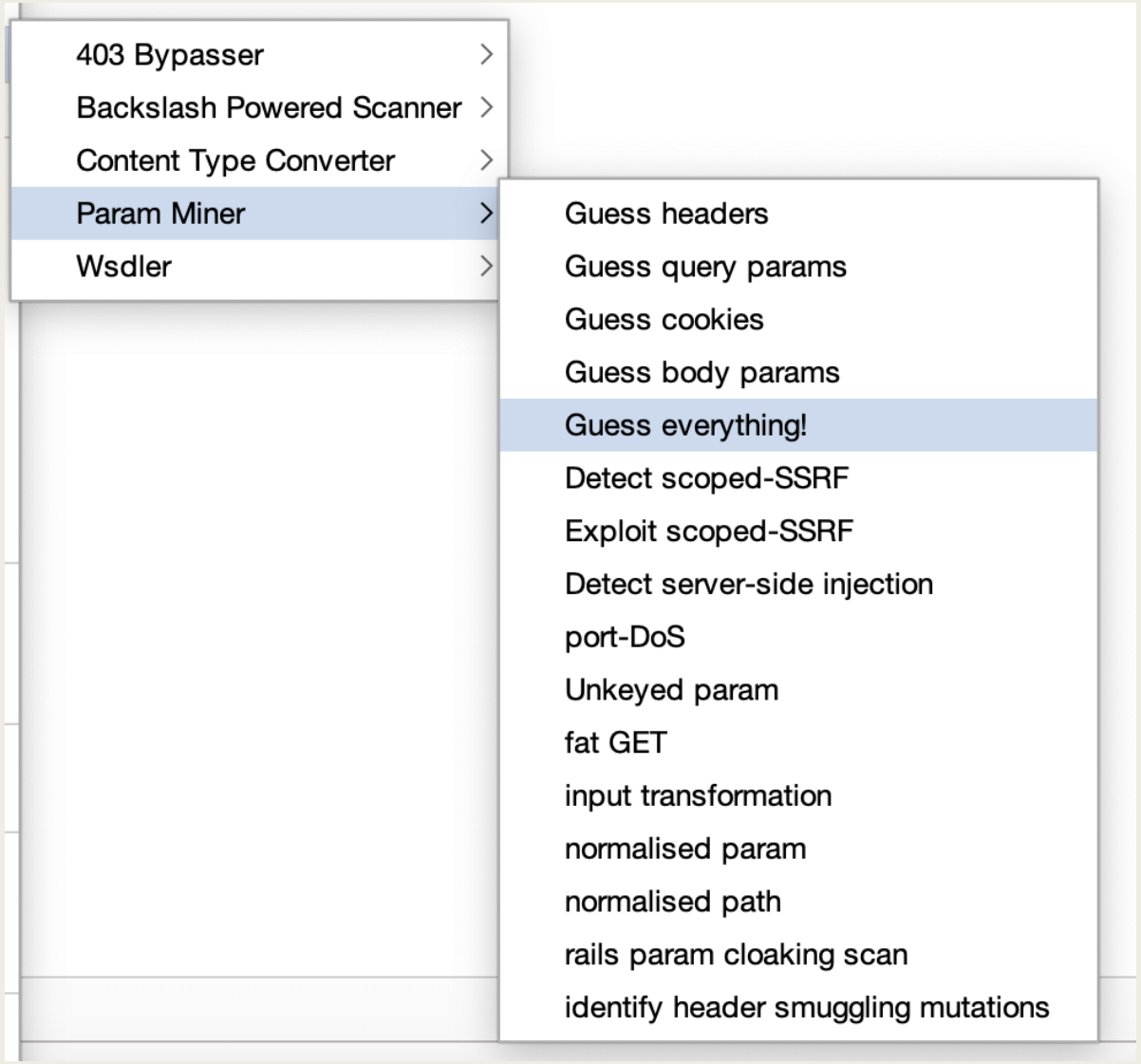
```
1 HTTP/1.1 404 Not Found
2 Content-Type: text/html;charset=UTF-8
```

Just don’t go too fast, or Akamai / Cloudflare will block you :-(

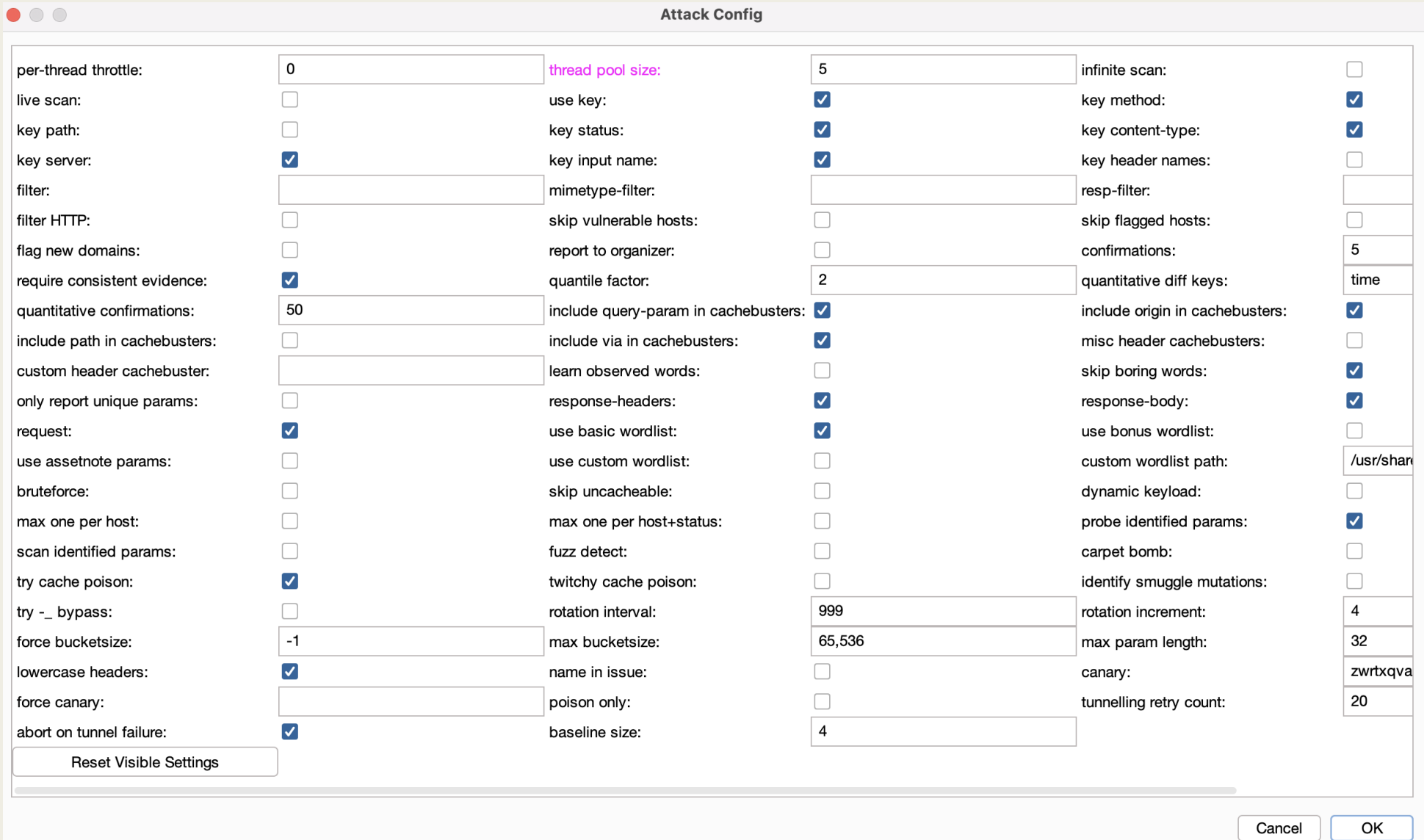


Burp Param Miner

- Helps you find hidden gems
- Information that is given by the user that the backend will react to
- GET PARAMS
- POST PARAMS
- HIDDEN HEADERS
- HIDDEN COOKIES

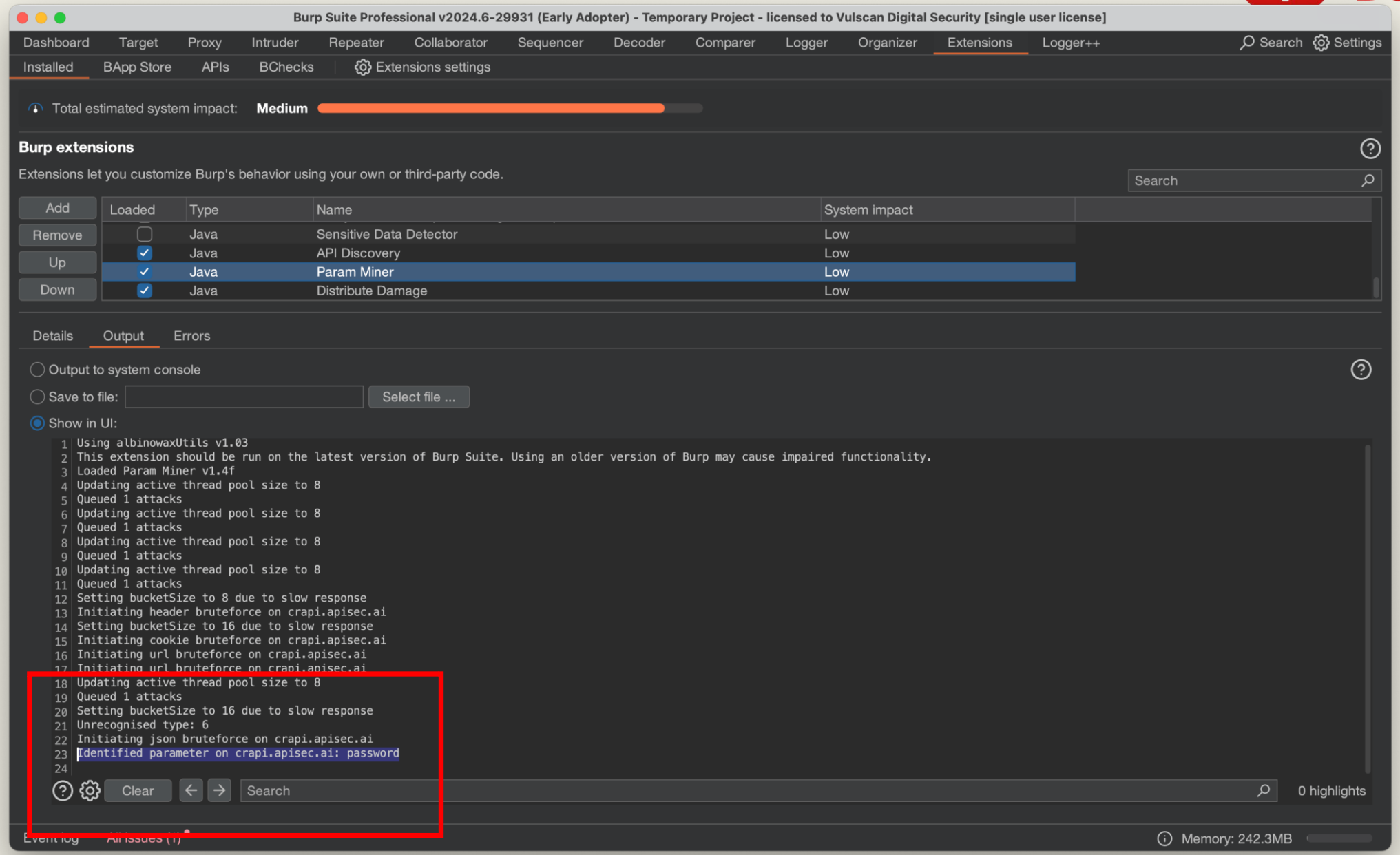


Burp Param Miner



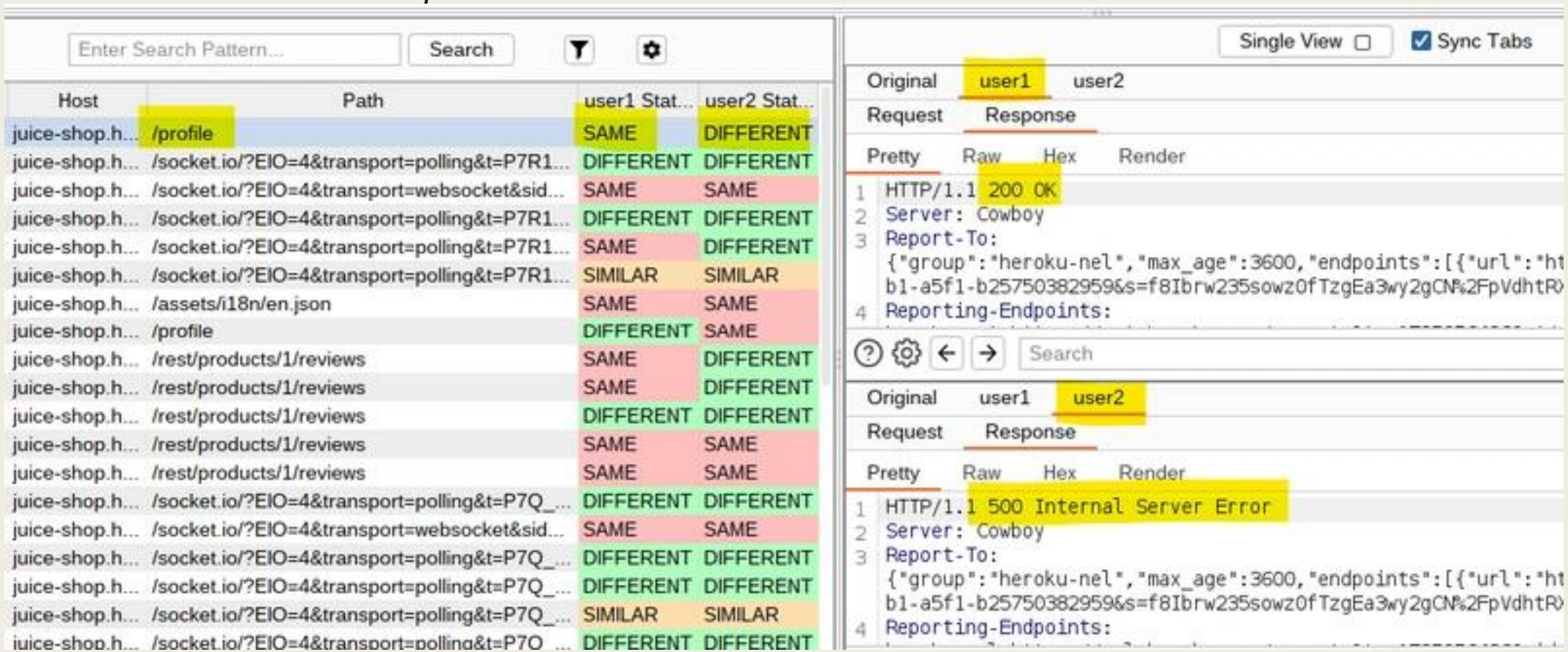
Burp Param Miner

defend Denmark



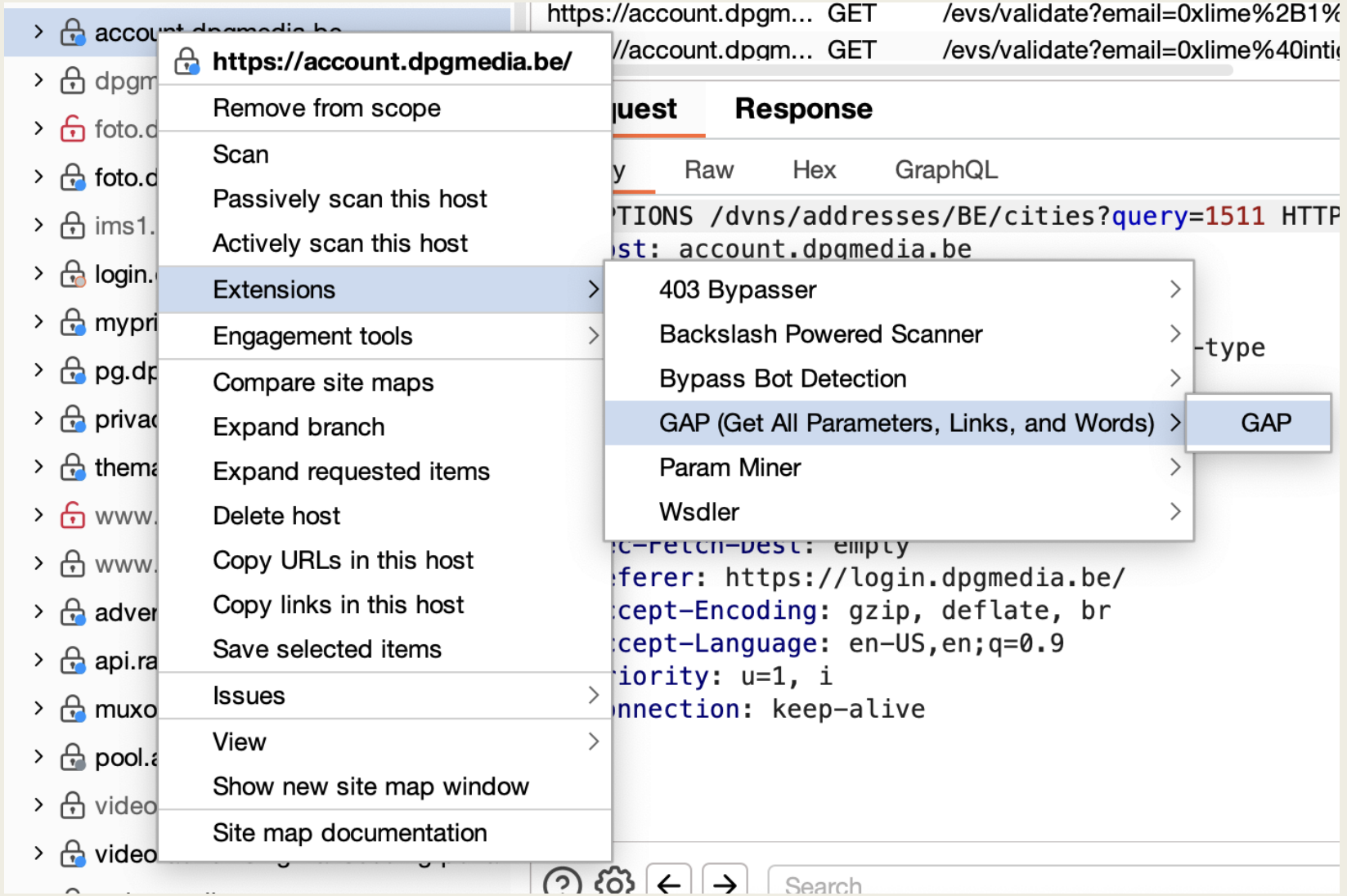
Burp Auth Analyzer

- Helps to check for access control issues (OWASP top 1)
- Resends all requests
  - *But switches out or removes cookies / auth headers*
  - *Checks if responses are the same or similar*

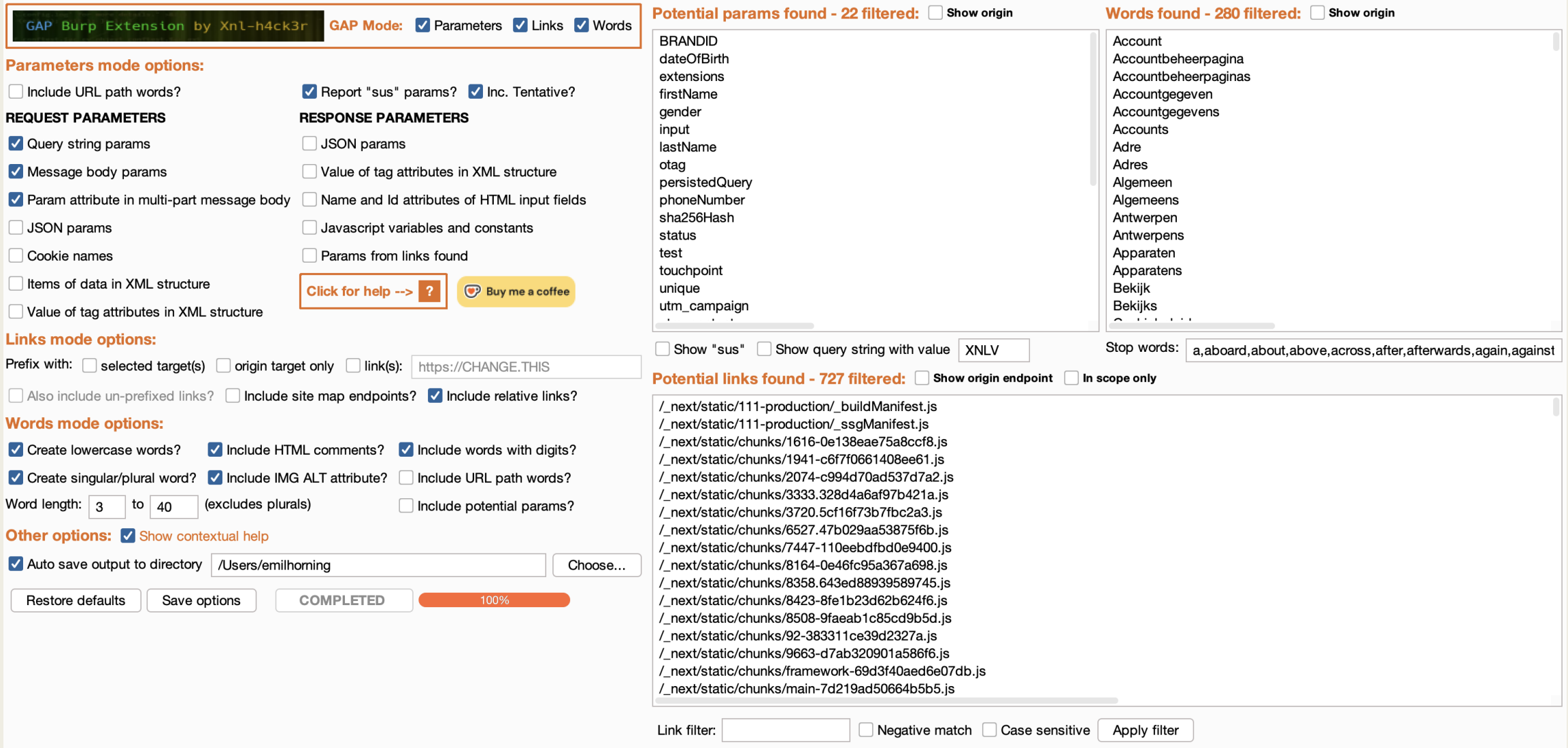


GAP – Get All Parameters

- Really nice tool to get links
- To get words for a wordlist
- Specifically for your target, take it from the targets tab



GAP – Get All Parameters

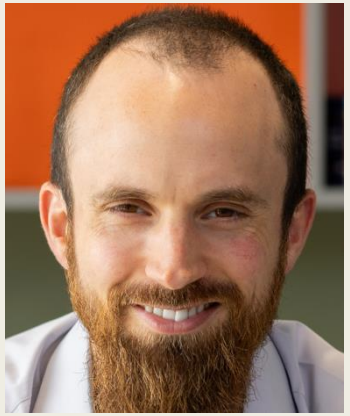


LEARNING FROM MY FINDINGS / REPORTS

Disclosing some of my reports – Race conditions

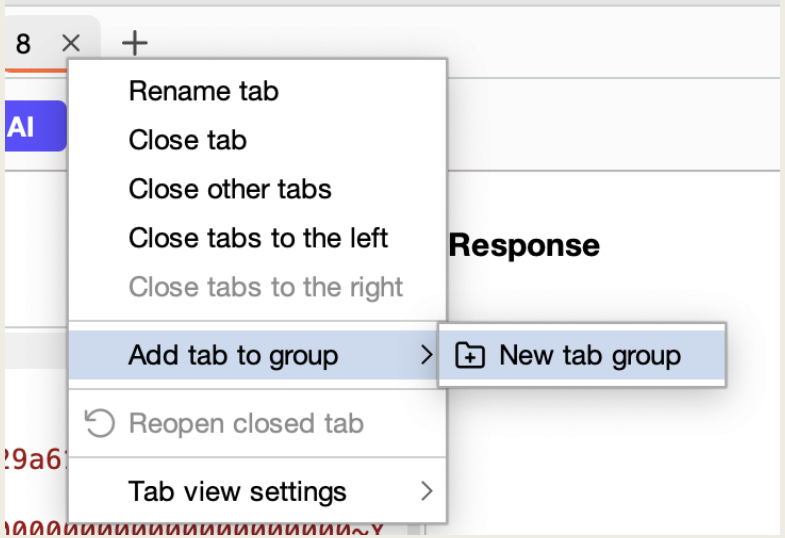
- **Title:** Fast concurrent requests can lead to more than allowed number of starred articles on *********
- The platform allowed selling items and marking specific items as **Starred***
- But you could only have 5 items starred.
- There was a POST request to
  - `/api/*****/listings/7bc9c7dd-6365-426c-b8c0-07f1a23c6095/starmark`
- Where the **UUID** was our listing for an item.
- What if we ask to star 20 of our items ***AT THE EXACT SAME TIME!***

How to do it in BURP

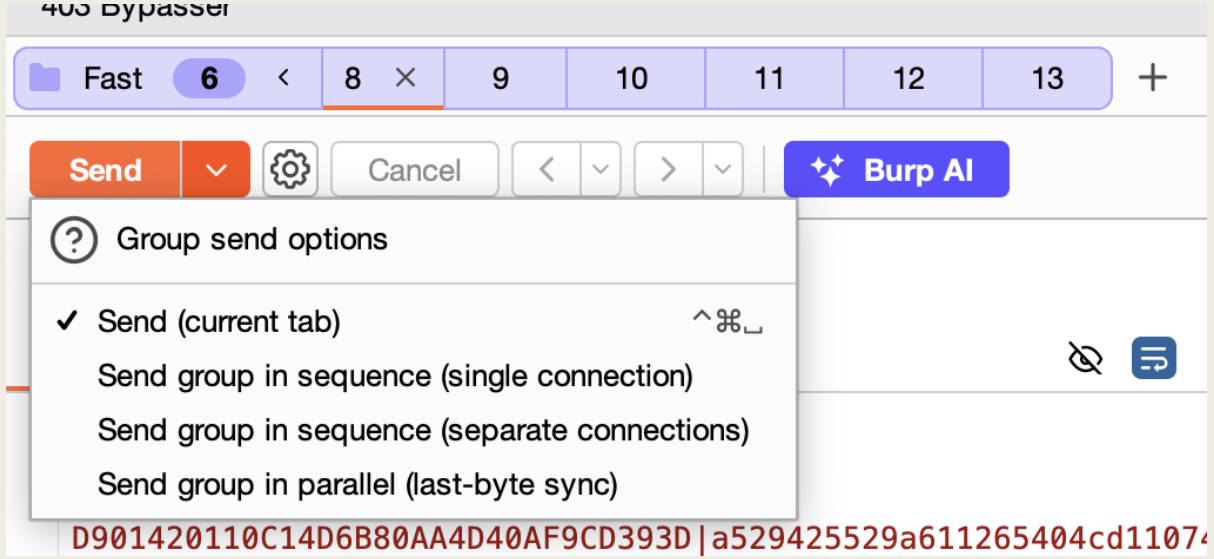


defend Denmark

- Take all the requests you want to send at the same time, send them to repeater.
- Create a group in repeater and put them all in the group
- Send requests in parallel (Last byte sync)



------>



defend Denmark

When to look for race condition bugs?

- Anywhere where there is potential for some race condition
- Anywhere some amount of tokens is deducted / you only have a certain amount of credits
- In password reset forms (What if the reset token is time based?)

Disclosing some of my reports – Mass Assignments

- **Title:** Mass assignment leading to privilege escalation in the application
- The platform had normal users, and admin users.
- You can request (**GET**) your user object and also update it (**PATCH**) at
  - `/api/users/1234 (your id)`
- The frontend added only the fields you were allowed to edit
- But you could manually add them to override sensitive fields.

Mass Assignment

1. Initial User State (GET Request)

GET

/api/users/123

```
Host: example.com Authorization: Bearer your_token_here
Content-Type: application/json
```

HTTP/1.1 200 OK

```
Content-Type: application/json
```

```
{
  "id": 123,
  "name": "John Doe",
  "email": "john@example.com",
  "role": "user"
}
```

Mass Assignment

2. Legitimate Update (Intended PUT Request)

PUT

/api/users/123

```
Host: example.com Authorization: Bearer your_token_here
Content-Type: application/json
```

```
{
  "name": "John Updated",
  "email": "john.updated@example.com"
}
```

HTTP/1.1 200 OK

```
Content-Type: application/json
```

```
{
  "id": 123,
  "name": "John Updated",
  "email": "john.updated@example.com",
  "role": "user"
}
```

Mass Assignment

3. Mass Assignment Attack (Exploitative PUT Request) ⚠️

PUT

/api/users/123

```
Host: example.com Authorization: Bearer your_token_here
Content-Type: application/json
```

```
{
  "name": "John Updated",
  "email": "john.updated@example.com",
  "role": "admin"
}
```

HTTP/1.1 200 OK

```
Content-Type: application/json
```

```
{
  "id": 123,
  "name": "John Updated",
  "email": "john.updated@example.com",
  "role": "admin"
}
```

Mass Assignment

4. Verification (Follow-up GET Request)

GET

/api/users/123

```
Host: example.com Authorization: Bearer your_token_here
Content-Type: application/json
```

HTTP/1.1 200 OK

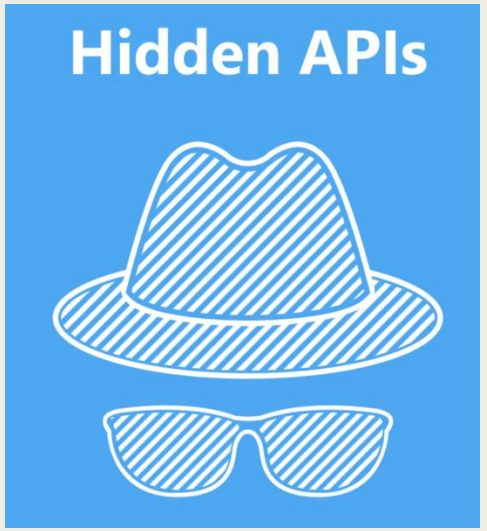
```
Content-Type: application/json
```

```
{
  "id": 123,
  "name": "John Updated",
  "email": "john.updated@example.com",
  "role": "admin"
}
```

When to look for mass assignments?

- Anywhere where you can see the object being returned
  - `GET /api/user/me`
- And where you also have the possibility to update it
  - `PATCH /api/user/me`
- Or where you are allowed to create new objects
  - `POST /api/user/new`

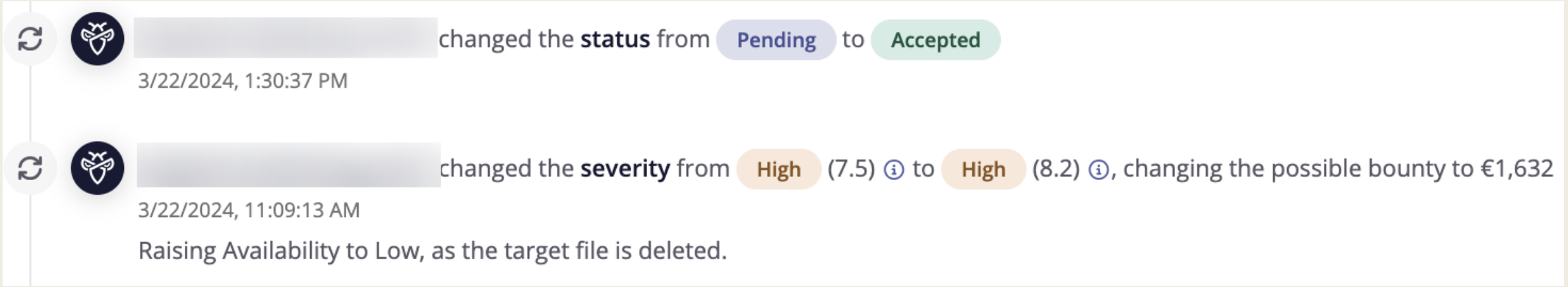
Disclosing some of my reports – Hidden API --> Delete others files



- **Title:** Undocumented API leads to deleting other users files
- The platform allowed users to host files to be shared with others.
- The platform used incremental ID's for files (1001, 1002, 1003…)
- The platform used strong access control!
- But in the javascript files for the frontend, there was an undocumented api call
  - `DELETE /api/overturn/file/1234 (your id)`
- This **overturn** section was never referenced!

Disclosing some of my reports – Hidden API --> Delete others files

- Nice bounty



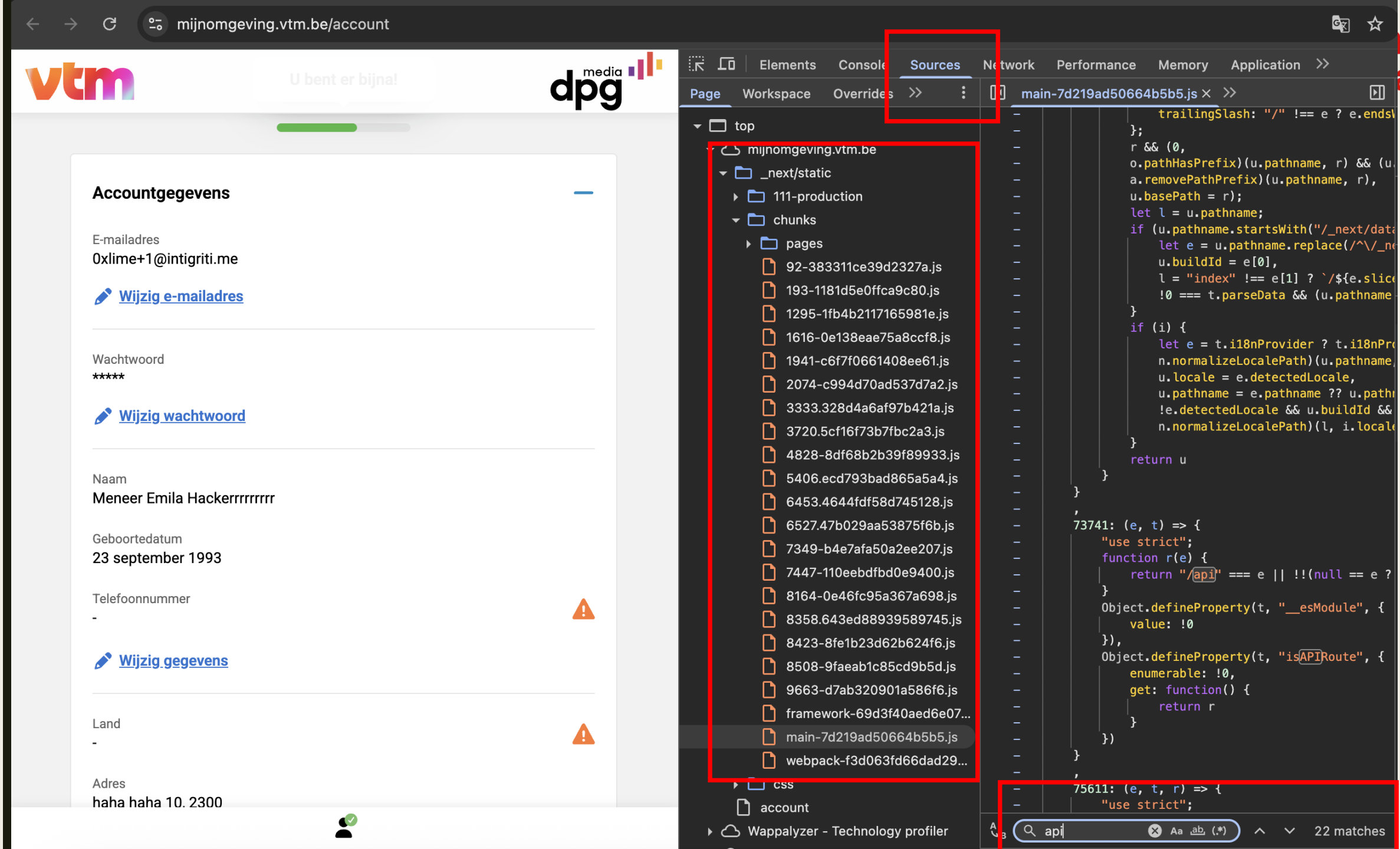
defend Denmark

Found via js analysis

- All sites (most) use Javascript in the frontend to render what the browser sees
- Many modern frameworks (react,vue etc) allow you to create dynamic and nice webpages
- And many of them embed all the backend functionality into the frontend
- So the frontend knows exactly what to send to the backend
- We want to investigate this!!!!

Js analysis, just your browser.

- Your browser will show the sites js to the best of its ability under the devtools
  - Right click → inspect
- Look for the main site and then find files ending in **.js**
- These files usually look like shit, and are not easy to read, but we can use them still to get some idea.
- Look for calls to apis by just searching for “api”


mijnomgeving.vtm.be/account
vtm
dpg media
Accountgegevens
E-mailadres
0xlime+1@intigriti.me
Wijzig e-mailadres
Wachtwoord
*****
Wijzig wachtwoord
Naam
Meneer Emila Hackerrrrrrrrr
Geboortedatum
23 september 1993
Telefoonnummer
-
Wijzig gegevens
Land
-
Adres
haha haha 10, 2300
Elements
Console
Sources
Network
Performance
Memory
Application
Page
Workspace
Overrides
main-7d219ad50664b5b5.js
top
mijnomgeving.vtm.be
_next/static
111-production
chunks
pages
92-383311ce39d2327a.js
193-1181d5e0ffca9c80.js
1295-1fb4b2117165981e.js
1616-0e138eae75a8ccf8.js
1941-c6f7f0661408ee61.js
2074-c994d70ad537d7a2.js
3333.328d4a6af97b421a.js
3720.5cf16f73b7fbc2a3.js
4828-8df68b2b39f89933.js
5406.ecd793bad865a5a4.js
6453.4644fdf58d745128.js
6527.47b029aa53875f6b.js
7349-b4e7afa50a2ee207.js
7447-110eebdfbd0e9400.js
8164-0e46fc95a367a698.js
8358.643ed88939589745.js
8423-8fe1b23d62b624f6.js
8508-9faeab1c85cd9b5d.js
9663-d7ab320901a586f6.js
framework-69d3f40aed6e07...
main-7d219ad50664b5b5.js
webpack-f3d063fd66dad29...
css
account
Wappalyzer - Technology profiler
73741: (e, t) => {
"use strict";
function r(e) {
return "/api" === e || !!(null == e ?
}
Object.defineProperty(t, "__esModule", {
value: !0
}),
Object.defineProperty(t, "isAPIRoute", {
enumerable: !0,
get: function() {
return r
}
})
}
,
75611: (e, t, r) => {
"use strict";
api
Aa
22 matches

TIPS ON WRITING REPORTS

Writing reports

- The report is your **main tool** for getting paid
- You can have the best bug in the world, but…
  - *If your report sucks then the triage wont pass it on*
  - *If your report is incoherent the triager won't understand*
  - *If your report does not explain proper impact, the program manager may not care*
- Without a proper report, you cannot expect a proper response

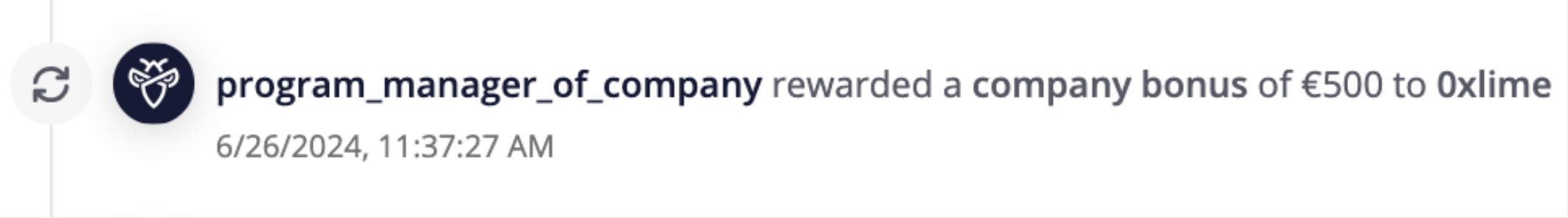
Report sections suggested approach

Executive summary	*A short summary of what the report means, for a non technical audience*
Proof of concept	*Step by step for reproduction, many screenshots, video also suggested, ALL details.*
Impact statement	*What can an attacker do with this, how can it be misused, why is it bad.*
Remediation Suggestions	*Suggest a fix, link to some articles, try to help the program manager*

AND LASTLY… ALWAYS BE POLITE AND PROFESSIONAL

On tempering your mood

- Many triagers / program managers deal with rude, desperate and disrespectful hunters
- Being overly kind and professional does in my experience lead to better experiences with program managers
- If you don't feel you get this back from them, just switch to another program.
- On many occasions I have been asked to help understand the vulnerability
  - *I always tell them that it is up to them if they think its valuable research*

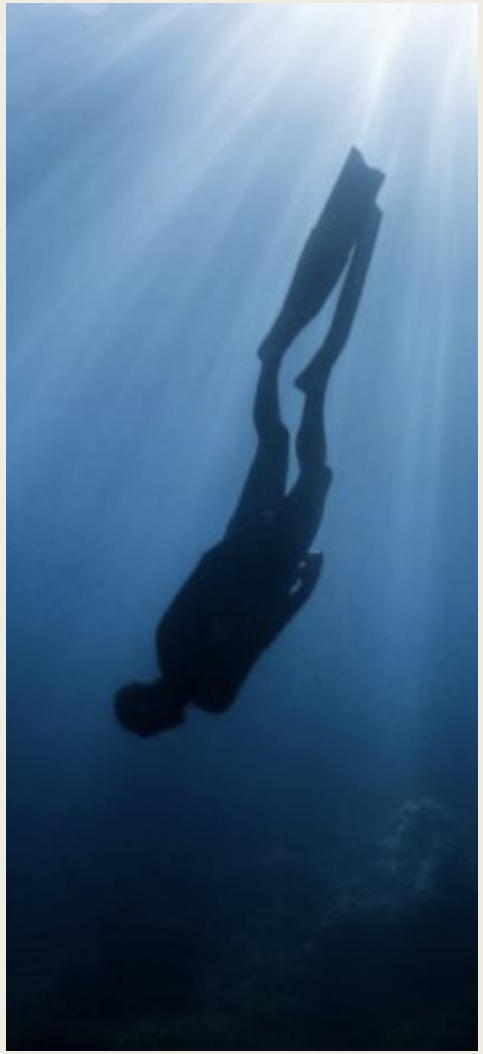


So to summarize recon
When finding a new target:

1. Read the SCOPE, so you don't submit out of scope
2. Find APEX domains (target.com, targetsite.dk, targetmedia.be)
3. Find SUBDOMAINS
    1. *Investigate subdomains with various tools, DNSX, HTTPX, GoWitness*
4. Find LINKS with waymore
5. Investigate cloud providers
6. Google Dorking
7. DO EVERYTHING YOU CAN TO FIND ENDPOINTS / SUBDOMAINS THAT ARE WELL HIDDEN

So to summarize deep dive
When finding a new target:

1. Edit the scope in burp, to not let it fill up with garbage
2. CLICK EVERYWHERE
3. Use tools to find hidden stuff
    1. *Parameters that the server responds differently to*
    2. *Endpoints that the server responds differently to*
4. ALWAYS TEST FOR ACCESS CONTROL
    1. *Can an **unauthenticated user** see the same as your user?*
    2. *Can another user with another **session id** see the same as yours?*
    3. *Can you access objects / data across users?*



Questions?

Download the recon data here:
kortlink.dk/2tnre

✨Add me on Linkedin✨