

A thick black L-shaped frame surrounds the text. It starts at the top left, goes right, then down, then right again, and finally down to the bottom right corner.

# SUCCESSING 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.



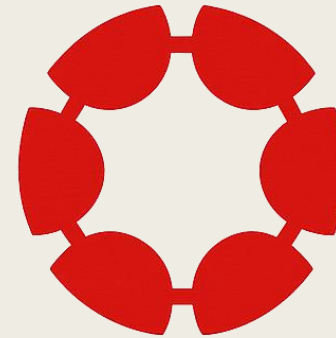
# What is this talk?

- 2<sup>nd</sup> 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**

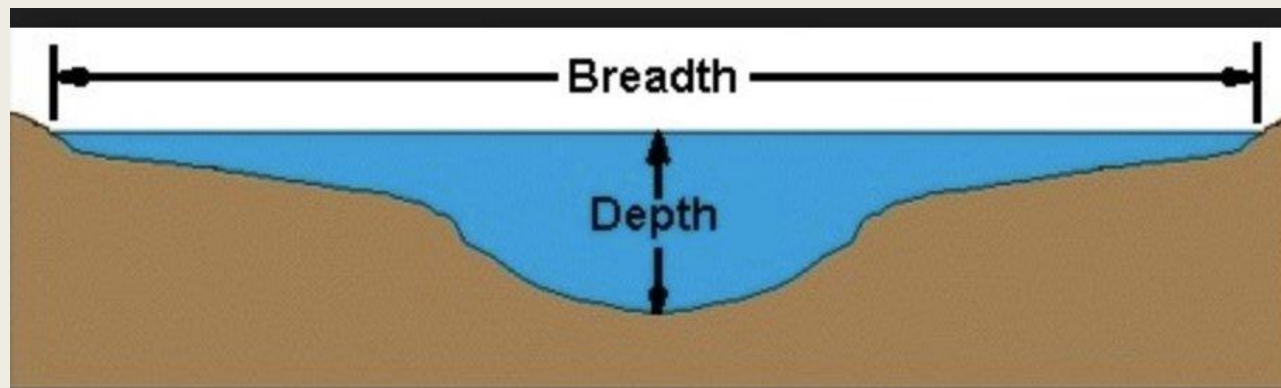
# How to get the most out of this

- 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

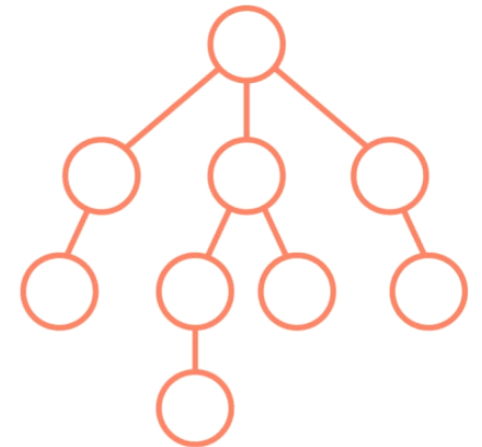
- Either we go breadth first and map a lot of attack surface
- Or we go depth first, straight into the main application



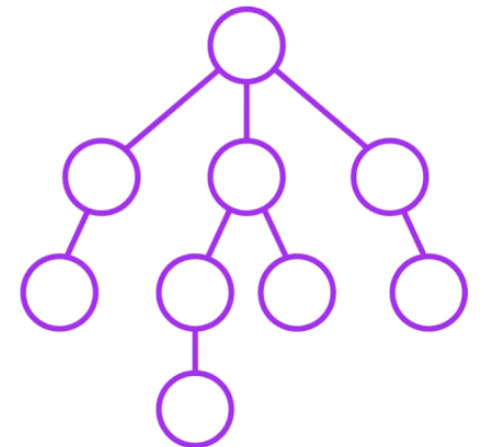
## Tree BFS vs. DFS

 DesignGurus.io

Breadth  
First  
Search



Depth  
First  
Search



# Recon based approach - BFS

- **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

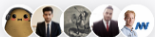
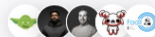




media  
dpkg

TARGET  
ACQUIRED

# This is a good target because...

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div><div></div><div><div>DPG Media</div><div>Algemeen Dagblad</div><div>Public</div></div></div> <div><div><div>€169</div><div>AVG PAID</div></div><div><div>&lt; 4 days</div><div>FIRST RESPONSE</div></div></div> <div><div><div>78</div><div>ACCEPTED</div></div><div><div>&lt; 2 days</div><div>LAST SUBMISSION</div></div></div> <div><div><div>4</div><div>1</div><div>IN SCOPE ASSETS</div></div><div><div></div><div><div>+319</div><div>RESEARCHERS</div></div></div><div>€25 - €2,200</div></div>      | <div><div></div><div><div>DPG Media</div><div>De Morgen</div><div>Public</div></div></div> <div><div><div>€172</div><div>AVG PAID</div></div><div><div>&lt; 4 days</div><div>FIRST RESPONSE</div></div></div> <div><div><div>31</div><div>ACCEPTED</div></div><div><div>&lt; 2 weeks</div><div>LAST SUBMISSION</div></div></div> <div><div><div>5</div><div>5</div><div>IN SCOPE ASSETS</div></div><div><div></div><div><div>+113</div><div>RESEARCHERS</div></div></div><div>€25 - €2,200</div></div>   | <div><div></div><div><div>DPG Media</div><div>De Volkskrant</div><div>Public</div></div></div> <div><div><div></div><div>AVG PAID</div></div><div><div>&lt; 4 days</div><div>FIRST RESPONSE</div></div></div> <div><div><div></div><div>ACCEPTED</div></div><div><div>&lt; 3 weeks</div><div>LAST SUBMISSION</div></div></div> <div><div><div>5</div><div>1</div><div>IN SCOPE ASSETS</div></div><div><div></div><div><div>+272</div><div>RESEARCHERS</div></div></div><div>€25 - €2,200</div></div> | <div><div></div><div><div>DPG Media</div><div>DPG Media</div><div>Public</div></div></div> <div><div><div></div><div>AVG PAID</div></div><div><div>&lt; 4 days</div><div>FIRST RESPONSE</div></div></div> <div><div><div>316</div><div>ACCEPTED</div></div><div><div>&lt; 4 hours</div><div>LAST SUBMISSION</div></div></div> <div><div><div>2</div><div>1</div><div>IN SCOPE ASSETS</div></div><div><div></div><div><div>+228</div><div>RESEARCHERS</div></div></div><div>€25 - €500</div></div>    |
| <div><div></div><div><div>DPG Media</div><div>Het Laatste Nieuws</div><div>Public</div></div></div> <div><div><div>€171</div><div>AVG PAID</div></div><div><div>&lt; 4 days</div><div>FIRST RESPONSE</div></div></div> <div><div><div>63</div><div>ACCEPTED</div></div><div><div>&lt; 2 weeks</div><div>LAST SUBMISSION</div></div></div> <div><div><div>5</div><div>3</div><div>IN SCOPE ASSETS</div></div><div><div></div><div><div>+145</div><div>RESEARCHERS</div></div></div><div>€25 - €2,200</div></div> | <div><div></div><div><div>DPG Media</div><div>Het Parool</div><div>Public</div></div></div> <div><div><div>€137</div><div>AVG PAID</div></div><div><div>&lt; 5 days</div><div>FIRST RESPONSE</div></div></div> <div><div><div>17</div><div>ACCEPTED</div></div><div><div>&lt; 4 days</div><div>LAST SUBMISSION</div></div></div> <div><div><div>6</div><div>5</div><div>IN SCOPE ASSETS</div></div><div><div></div><div><div>+104</div><div>RESEARCHERS</div></div></div><div>€25 - €2,200</div></div> | <div><div></div><div><div>DPG Media</div><div>Humo</div><div>Public</div></div></div> <div><div><div>€313</div><div>AVG PAID</div></div><div><div>&lt; 4 days</div><div>FIRST RESPONSE</div></div></div> <div><div><div>33</div><div>ACCEPTED</div></div><div><div>&lt; 1 week</div><div>LAST SUBMISSION</div></div></div> <div><div><div>5</div><div>5</div><div>IN SCOPE ASSETS</div></div><div><div></div><div><div>+136</div><div>RESEARCHERS</div></div></div><div>€25 - €2,200</div></div>   | <div><div></div><div><div>DPG Media</div><div>Libelle</div><div>Public</div></div></div> <div><div><div>€283</div><div>AVG PAID</div></div><div><div>&lt; 4 days</div><div>FIRST RESPONSE</div></div></div> <div><div><div>26</div><div>ACCEPTED</div></div><div><div>&lt; 3 days</div><div>LAST SUBMISSION</div></div></div> <div><div><div>5</div><div>1</div><div>IN SCOPE ASSETS</div></div><div><div></div><div><div>+50</div><div>RESEARCHERS</div></div></div><div>€25 - €2,200</div></div> |

# Its public and very very broad

[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



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 are 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

TARGET: DPGMEDIA.BE

and any other companies owned by DPG Media Group

# The goal – BFS FIRST

- 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

## projectdiscovery/ **subfinder**

Fast passive subdomain enumeration tool.



 102

Contributors

 8

Issues

 75

Discussions

 13k

Stars

 1k

Forks





projectdiscovery.io

```
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     | <a href="https://bevigil.com/osint-api">https://bevigil.com/osint-api</a>                                             |
| BinaryEdge  | <a href="https://binaryedge.io">https://binaryedge.io</a>                                                             |
| BufferOver  | <a href="https://tls.bufferover.run">https://tls.bufferover.run</a>                                                   |
| C99         | <a href="https://api.c99.nl/">https://api.c99.nl/</a>                                                                 |
| Censys      | <a href="https://censys.io">https://censys.io</a>                                                                     |
| CertSpotter | <a href="https://ssllmate.com/certspotter/api/">https://ssllmate.com/certspotter/api/</a>                             |
| Chaos       | <a href="https://chaos.projectdiscovery.io">https://chaos.projectdiscovery.io</a>                                     |
| Chinaz      | <a href="http://my.chinaz.com/ChinazAPI/DataCenter/MyDataApi">http://my.chinaz.com/ChinazAPI/DataCenter/MyDataApi</a> |
| DNSDB       | <a href="https://api.dnsdb.info">https://api.dnsdb.info</a>                                                           |
| Fofa        | <a href="https://fofa.info/static_pages/api_help">https://fofa.info/static_pages/api_help</a>                         |
| FullHunt    | <a href="https://fullhunt.io">https://fullhunt.io</a>                                                                 |
| GitHub      | <a href="https://github.com">https://github.com</a>                                                                   |
| Intelx      | <a href="https://intelx.io">https://intelx.io</a>                                                                     |

# Tool: DNSX

## projectdiscovery/ dnsx



dnsx is a fast and multi-purpose DNS toolkit allow to run multiple DNS queries of your choice with a list...

 29

Contributors

 345

Used by

 36

Discussions

 3k

Stars

 275

Forks



# Tool: DNSX



- 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
```

[illegible]

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
```

A stylized ASCII art representation of the word 'dnsx' using various symbols like underscores, pipes, and slashes.

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



## DNS RESPONSE SCENARIOS

### SCENARIO 1: RESOLVES TO IP

api.internal.dpgmedia.be → 104.22.15.87  
✓ Active host – enumerate & scan

### SCENARIO 2: EXISTS BUT NO IP (NOERROR, empty answer)

internal.dpgmedia.be → "Non-authoritative answer"  
⚠ No IP, but domain EXISTS – check for child subdomains!

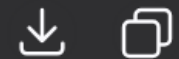
### SCENARIO 3: NXDOMAIN (doesn't exist)

fakeasdf123.dpgmedia.be → NXDOMAIN  
✗ Dead end – skip this branch entirely

# Premium tip: DNS responses may leak hidden domains



## Plaintext



dpgmedia.be

|                                |                                      |
|--------------------------------|--------------------------------------|
| — www.dpgmedia.be              | → 104.22.15.87 ✓ RESOLVES            |
| — mail.dpgmedia.be             | → 192.168.1.10 ✓ RESOLVES            |
| — internal.dpgmedia.be         | → (no IP) ⚠ EXISTS – CHECK CHILDREN! |
| — api.internal.dpgmedia.be     | → 10.0.0.5 ✓ RESOLVES                |
| — dev.internal.dpgmedia.be     | → 10.0.0.6 ✓ RESOLVES                |
| — staging.internal.dpgmedia.be | → 10.0.0.7 ✓ RESOLVES                |
| — corp.dpgmedia.be             | → (no IP) ⚠ EXISTS – CHECK CHILDREN! |
| — vpn.corp.dpgmedia.be         | → 203.0.113.50 ✓ RESOLVES            |
| — sso.corp.dpgmedia.be         | → 203.0.113.51 ✓ RESOLVES            |
| — fakeasdf123.dpgmedia.be      | → NXDOMAIN ✗ DEAD                    |

# 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 -follow-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

```
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/c
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] []
```



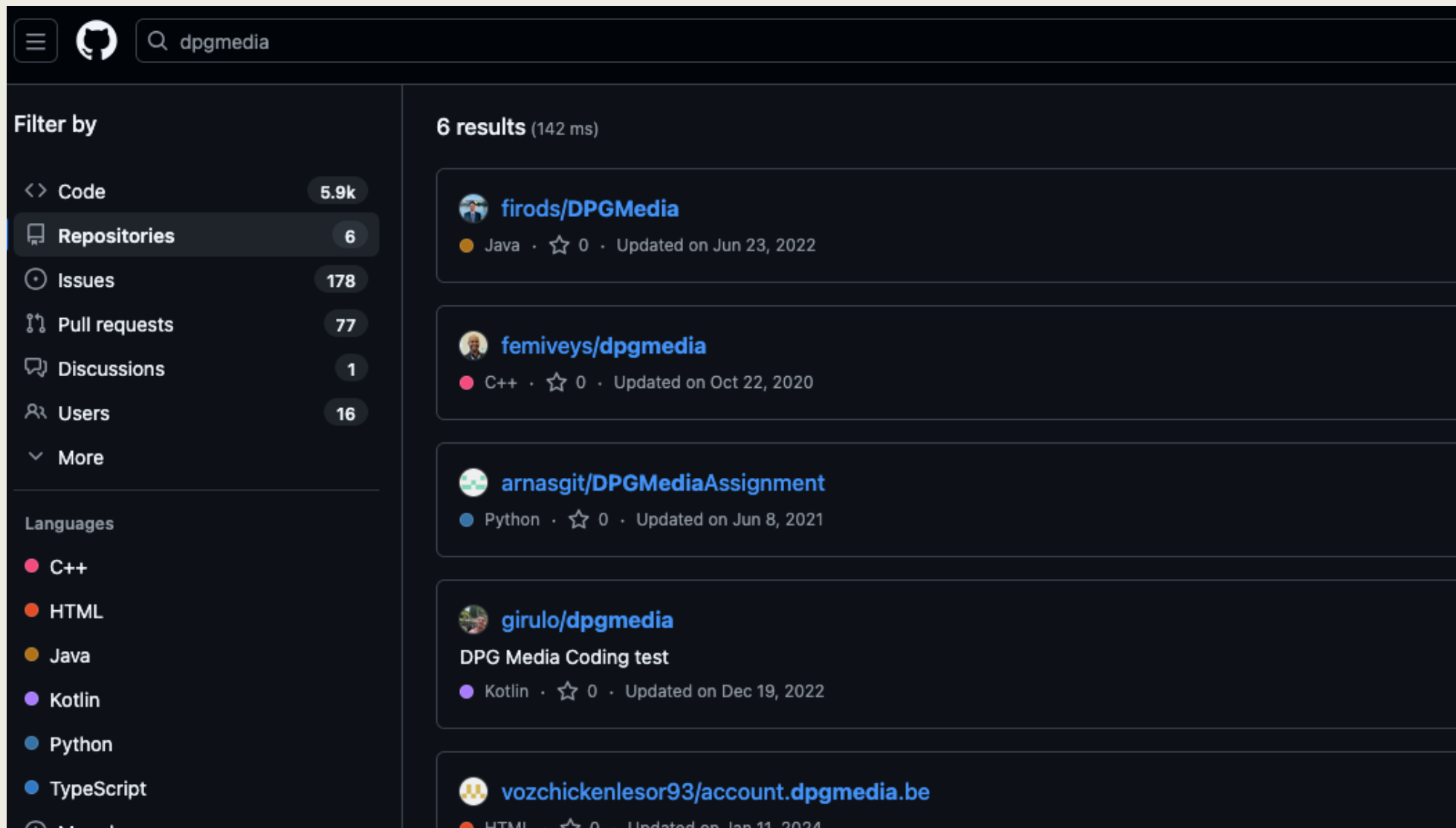
EXTRA TARGET: dpgmedia.net

# NEW TARGET: DPGMEDIA.NET

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

# Tool: GITHUB OSINT?

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

A screenshot of the GitHub search interface. The search bar at the top contains the text "dpgmedia". On the left, a sidebar shows filter options: "Filter by" with categories like Code (5.9k), Repositories (6), Issues (178), Pull requests (77), Discussions (1), Users (16), and More. Below this is a "Languages" section with colored dots for C++, HTML, Java, Kotlin, Python, and TypeScript. The main area displays "6 results (142 ms)". The results list includes:

- firods/DPGMedia**: Java, 0 stars, updated on Jun 23, 2022.
- femiveys/dpgmedia**: C++, 0 stars, updated on Oct 22, 2020.
- arnasgit/DPGMediaAssignment**: Python, 0 stars, updated on Jun 8, 2021.
- girulo/dpgmedia**: DPG Media Coding test, Kotlin, 0 stars, updated on Dec 19, 2022.
- vozchickenlesor93/account.dpgmedia.be**: HTML, 0 stars, updated on Jan 11, 2024.

# Premium tip: Dorking

## 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:index.of&sca\_esv=ce3b3adafce57907&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.

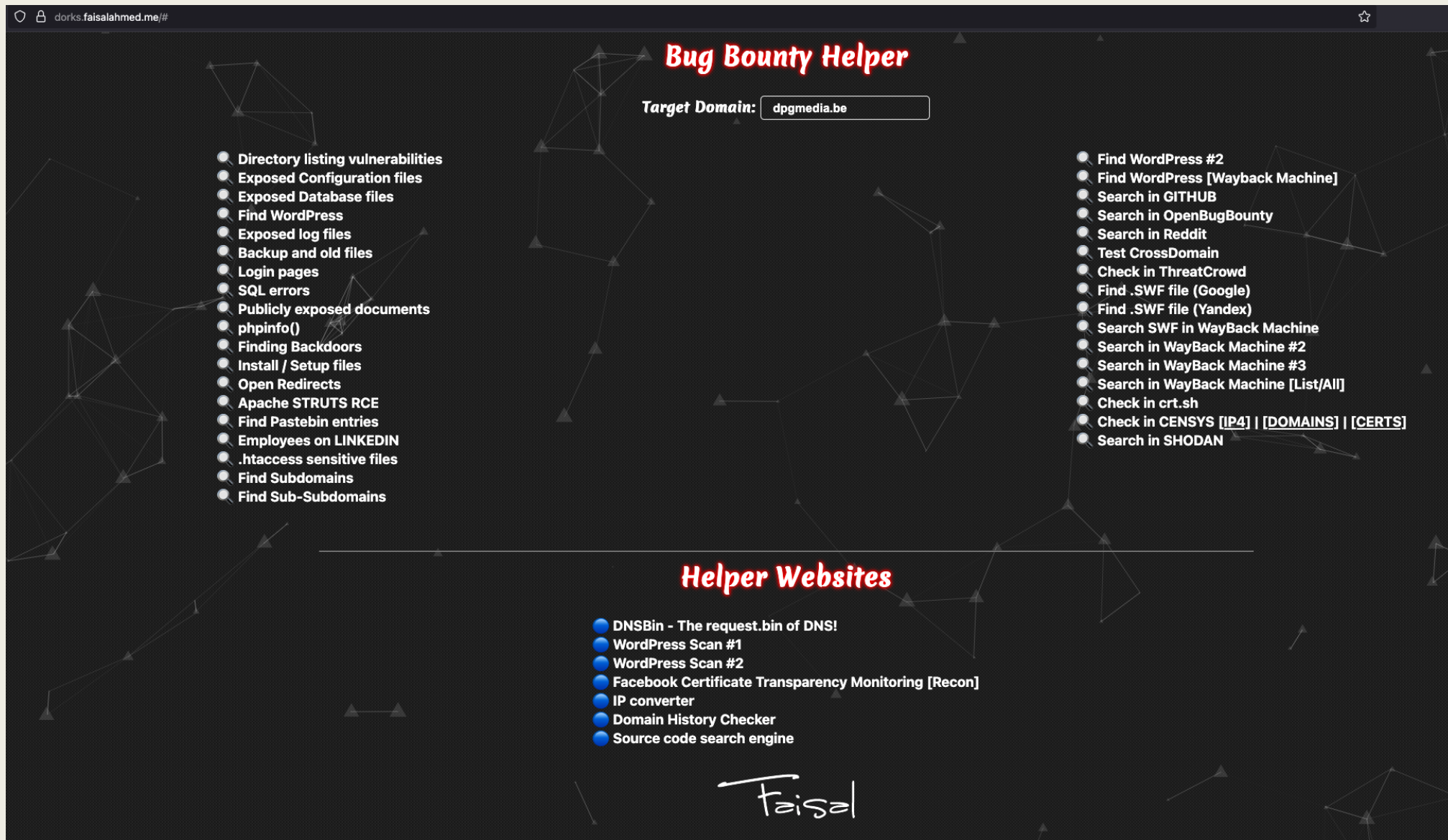
 **Dansk Lunge Cancer Gruppe**  
https://www.lungecancer.dk › wp-content › uploads

**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



The screenshot shows a web browser window with the address bar displaying `dorks.faisalahmed.me/#`. The page has a dark theme with a background of faint, interconnected nodes and lines. The main heading is "Bug Bounty Helper" in red. Below it, a "Target Domain:" label is followed by a text input field containing `dpgmedia.be`. The page is divided into three main sections: a left sidebar with a list of search categories, a central area with a list of specific search queries, and a bottom section titled "Helper Websites".

**Bug Bounty Helper**

Target Domain:

- Directory listing vulnerabilities
- Exposed Configuration files
- Exposed Database files
- Find WordPress
- Exposed log files
- Backup and old files
- Login pages
- SQL errors
- Publicly exposed documents
- phpinfo()
- Finding Backdoors
- Install / Setup files
- Open Redirects
- Apache STRUTS RCE
- Find Pastebin entries
- Employees on LINKEDIN
- .htaccess sensitive files
- Find Subdomains
- Find Sub-Subdomains

- Find WordPress #2
- Find WordPress [Wayback Machine]
- Search in GITHUB
- Search in OpenBugBounty
- Search in Reddit
- Test CrossDomain
- Check in ThreatCrowd
- Find .SWF file (Google)
- Find .SWF file (Yandex)
- Search SWF in WayBack Machine
- Search in WayBack Machine #2
- Search in WayBack Machine #3
- Search in WayBack Machine [List/All]
- Check in crt.sh
- Check in CENSYS [IP4] | [DOMAINS] | [CERTS]
- Search in SHODAN

**Helper Websites**

- DNSBin - The request.bin of DNS!
- WordPress Scan #1
- WordPress Scan #2
- Facebook Certificate Transparency Monitoring [Recon]
- IP converter
- Domain History Checker
- Source code search engine

Faisal

# Premium tip: Google dorking - 2026



Google

site:\*.lovable.app "dpgmedia"

AI Mode All Images News Videos Short videos Web More Tools

Abonnement Contact Kranten Eigenaar Belgium Opzeggen Antwerpen Nederland

These are results for site:\*.lovable.app "**dpg media**"  
Search instead for site:\*.lovable.app "dpgmedia"

 Lovable  
<https://nomadconsulting.lovable.app/dpg-media>

**Expert Project Management & Software Development**

Impact & OKRs Achieved. The platform achieved remarkable growth and adoption across **DPG Media**:  
20+. Business Domains. 1500+.

 Lovable  
<https://nomadconsulting.lovable.app/genai-projects>

**GenAI Projects**

Hands-on experience delivering Generative AI solutions, from strategy and architecture to production deployment. Featured Projects. **DPG Media** - ChatDPG ...

 Lovable  
<https://nomadconsulting.lovable.app/all-projects>

**Expert Project Management & Software Development**

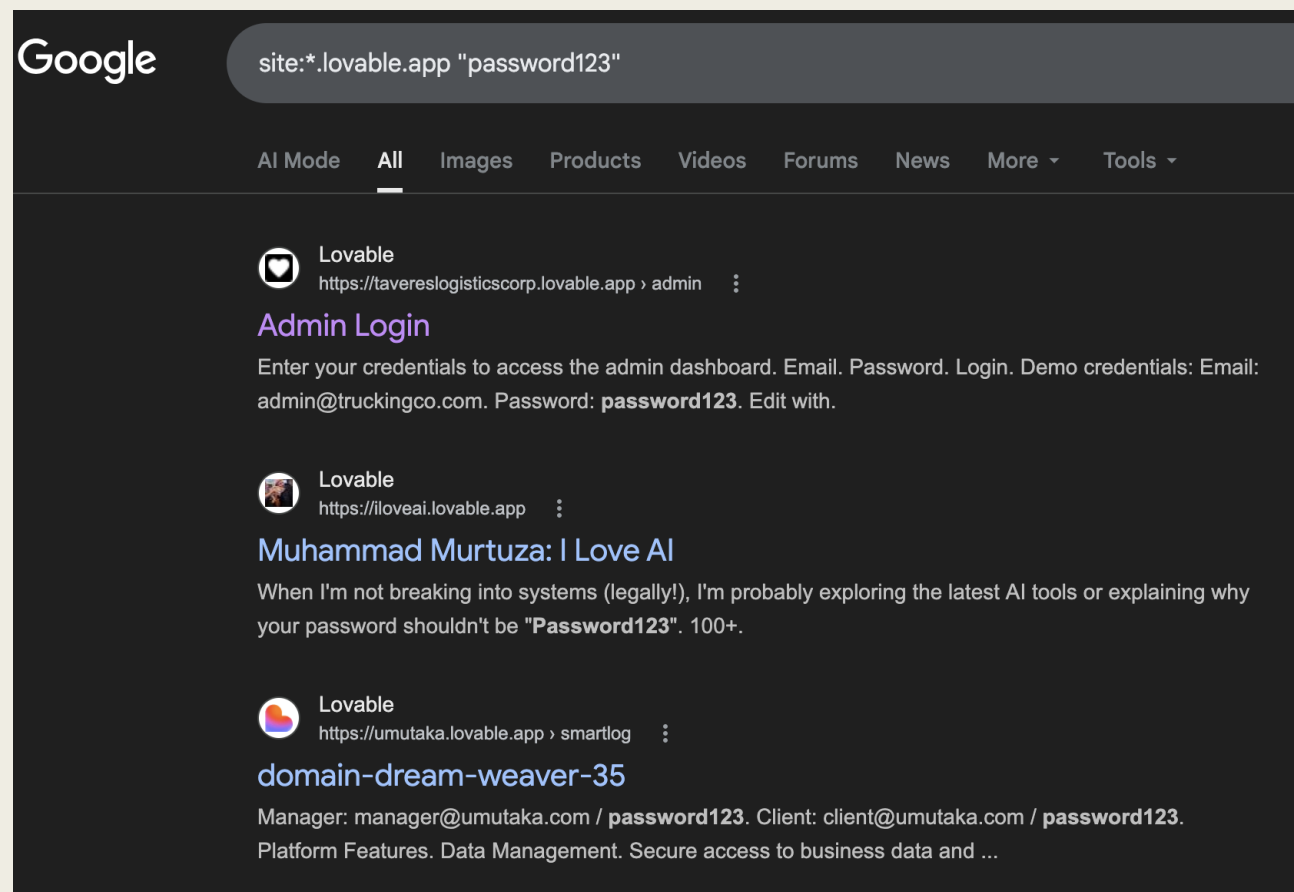
Project Timeline. ChatDPG. AI & GenAIMar 2024 - Jul 2024. **DPG Media**. AI tool for internal use at DPG.  
Agile Project ManagementChatGPTIT Project & Program ...

# Premium tip: Google dorking - 2026



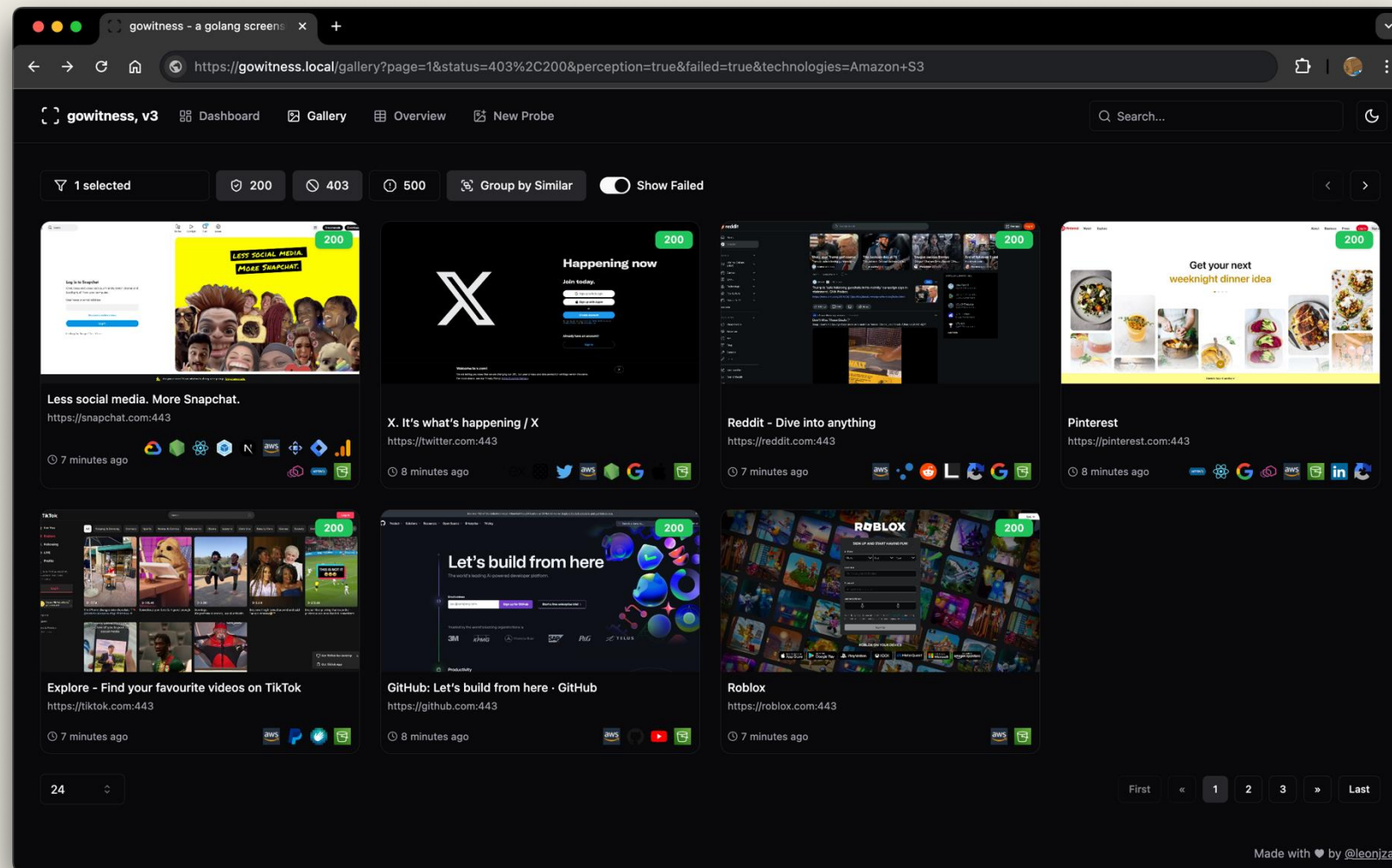
- Mange skubber vibe-coded produkter hurtigt ud i production
- Hvis de har opkobling til backend, så er der en mulighed for at udnytte dem
- Tjek de store vibe code platforme ud med google dorking:

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



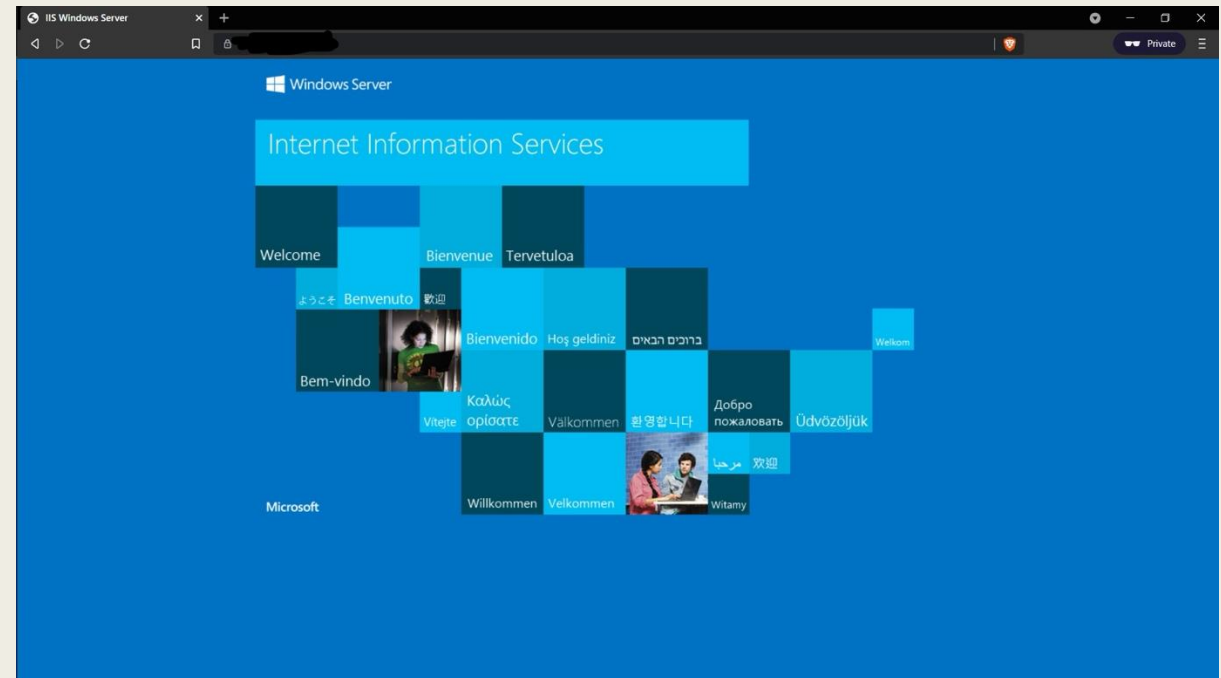
# Tool: Gowitness?

- 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



```
arseniy@ptarch:release $ java -jar ./iis_shortname_scanner.jar 20 8 'https://[redacted]/bin::$INDEX_ALLOCATION/'
# IIS Short Name (8.3) Scanner version 2023.4 - scan initiated 2024/02/25 19:41:27
Target: https://[redacted]/bin::$INDEX_ALLOCATION/
|_ Result: Vulnerable!
|_ Used HTTP method: DEBUG
|_ Suffix (magic part): /~1/.rem
|_ Extra information:
|_   Number of sent requests: 4560
|_   Identified directories: 1
|_     E6AC~1
|_       Actual directory name = E6AC
|_   Identified files: 39
|_     ANTLR3~1.DLL
|_     ENTITY~1.DLL
|_     GOOGLE~1.DLL
|_     MICROS~1.DLL
|_     MICROS~2.DLL
|_     MICROS~3.DLL
|_     NEWTON~1.DLL
|_     SY031B~1.DLL
|_     SY076E~1.DLL
|_     SY0F57~1.DLL
|_     SY1167~1.DLL
|_     SY1A15~1.DLL
|_     SY2F55~1.DLL
|_     SY4918~1.DLL
|_     SY598E~1.DLL
```

# Premium tip: IIS Tilde Enumeration scan

Target URL:

☒ Exploit the vulnerability (opt out for only checking)  Status: Ready to scan

```
[+] Started scan for URL "https://www.msbsvet.edu.in/"

[*] Trying method "OPTIONS" with magic final part "/~1/.rem"
[*] Trying method "POST" with magic final part "/~1/.rem"
[*] Trying method "DEBUG" with magic final part "/~1/.rem"

[+] Host "https://www.msbsvet.edu.in/" is vulnerable!
[+] Used HTTP method: DEBUG
[+] Suffix (magic part): /~1/.rem

[*] Starting filename and directory bruteforce on "https://www.msbsvet.edu.in/"
[i] Dir: ASPNET~1

[+] Bruteforce completed in 8 seconds
[+] Total time elapsed: 11 seconds
[+] Requests sent: 187

[+] Identified directories: 1
    |_ ASPNET~1

[-] No files found
|
```

# Hack IIS servers when you find them



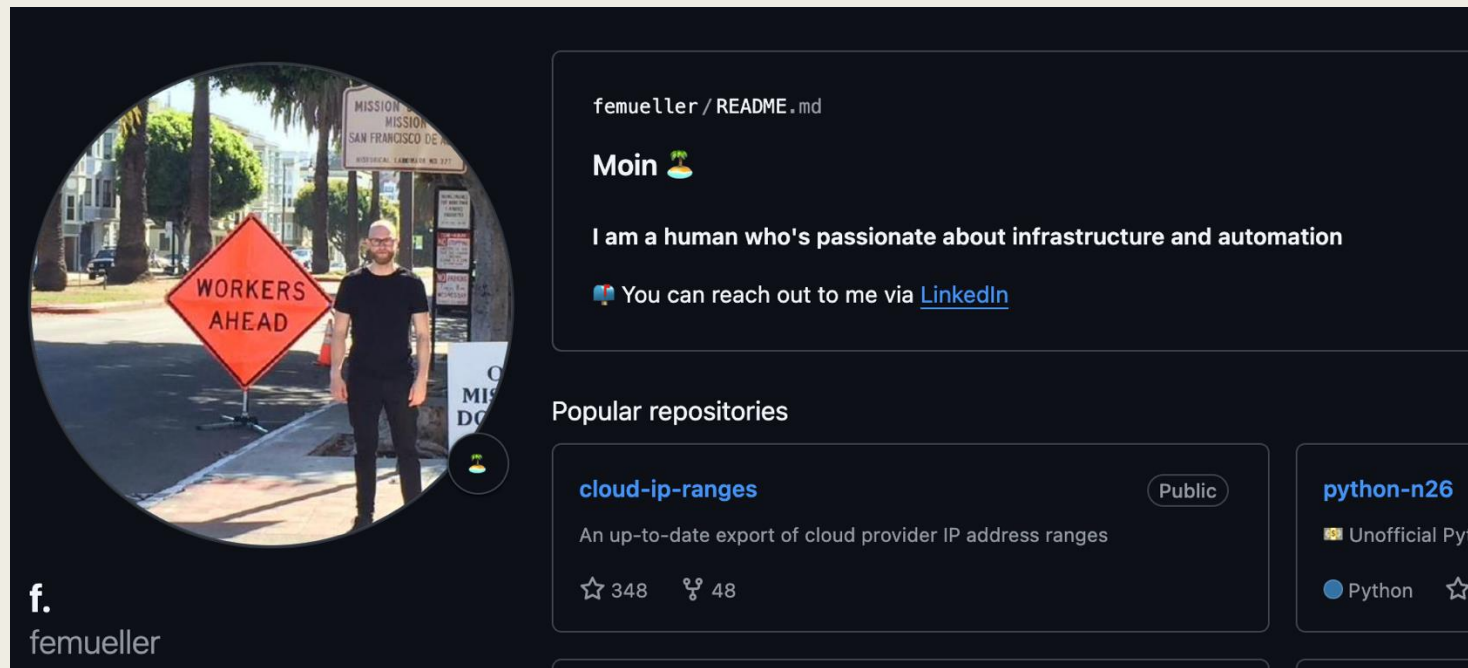
# Extra cloud recon

- 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](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>

A screenshot of a GitHub profile for a user named 'femueller'. The profile picture shows a man standing on a sidewalk next to a red 'WORKERS AHEAD' diamond-shaped road sign. The background of the profile header is a dark blue gradient. The bio reads: 'femueller / README.md', 'Moin 🌴', 'I am a human who's passionate about infrastructure and automation', and 'You can reach out to me via [LinkedIn](#)'. Below the bio, the 'Popular repositories' section is visible, featuring 'cloud-ip-ranges' (Public, 348 stars, 48 forks) and 'python-n26' (Unofficial Python, 1 star).

# 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
pmportal.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
pmportal.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
```

```
~/Research/Caduceus_cloud_scans  
waymore -i dpgmedia.cloud -mode U
```

```
Waymore  
by Xnl-h4ck3r
```

```
Current waymore version 6.6 (latest)
```

```
Getting links from Wayback Machine (archive.org) with one request (this can take a while for some domains)...
```

# Tool: Waymore



Waymore  
by Xnl-h4ck3r

Current waymore version 6.6 (latest)

Links found on Wayback Machine (archive.org): 49636

[ ERR ] Common Crawl connection error for index <https://index.commoncrawl.org/CC-MAIN-2023-50-index>

Extra links found on commoncrawl.org: 10

Extra links found on alienvault.com: 81

Extra links found on urlscan.io: 103

Extra links found on virustotal.com: 82

Links found for \*.dpgmedia.cloud: 49912 🙌

✅ Want to buy me a coffee? ☺️ <https://ko-fi.com/xnlh4ck3r> 🙌

# Tool: Waymore - Filtering

```
https://alarmeringen.api.dpgmedia.cloud/prod/counter/message/52690357  
https://alarmeringen.api.dpgmedia.cloud/prod/counter/message/52647011  
https://advertising-cdn.dpgmedia.cloud/header-bidding/nonprod/bndestem/7919a15a11e743e71164f3add686ec75f18aa929  
https://alarmeringen.api.dpgmedia.cloud/prod/counter/message/52423525  
https://alarmeringen.api.dpgmedia.cloud/prod/counter/message/52691976  
https://alarmeringen.api.dpgmedia.cloud/prod/counter/message/52543021  
https://alarmeringen.api.dpgmedia.cloud/prod/counter/message/52423990  
https://alarmeringen.api.dpgmedia.cloud/prod/counter/message/52504115  
https://alarmeringen.api.dpgmedia.cloud/prod/counter/message/52561922  
https://alarmeringen.api.dpgmedia.cloud/prod/counter/message/52375684  
https://alarmeringen.api.dpgmedia.cloud/prod/counter/message/52516779  
https://alarmeringen.api.dpgmedia.cloud/prod/counter/message/52706545  
https://alarmeringen.api.dpgmedia.cloud/prod/counter/message/52558400
```

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

cat waymore.txt | waymore.txt 

# 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

```
~/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%2F eindhoven%2Fde-verdwintruc-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%2F binnenland%2Fterrorisme-via-tiktok-14-jarigen-verspreiden-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%2F sport%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%2F bi [] [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%2F rotterdam%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%2F eindhoven%2F graffiti-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

# Spin up your favourite tool

 **Burp Suite** **CAIDO**

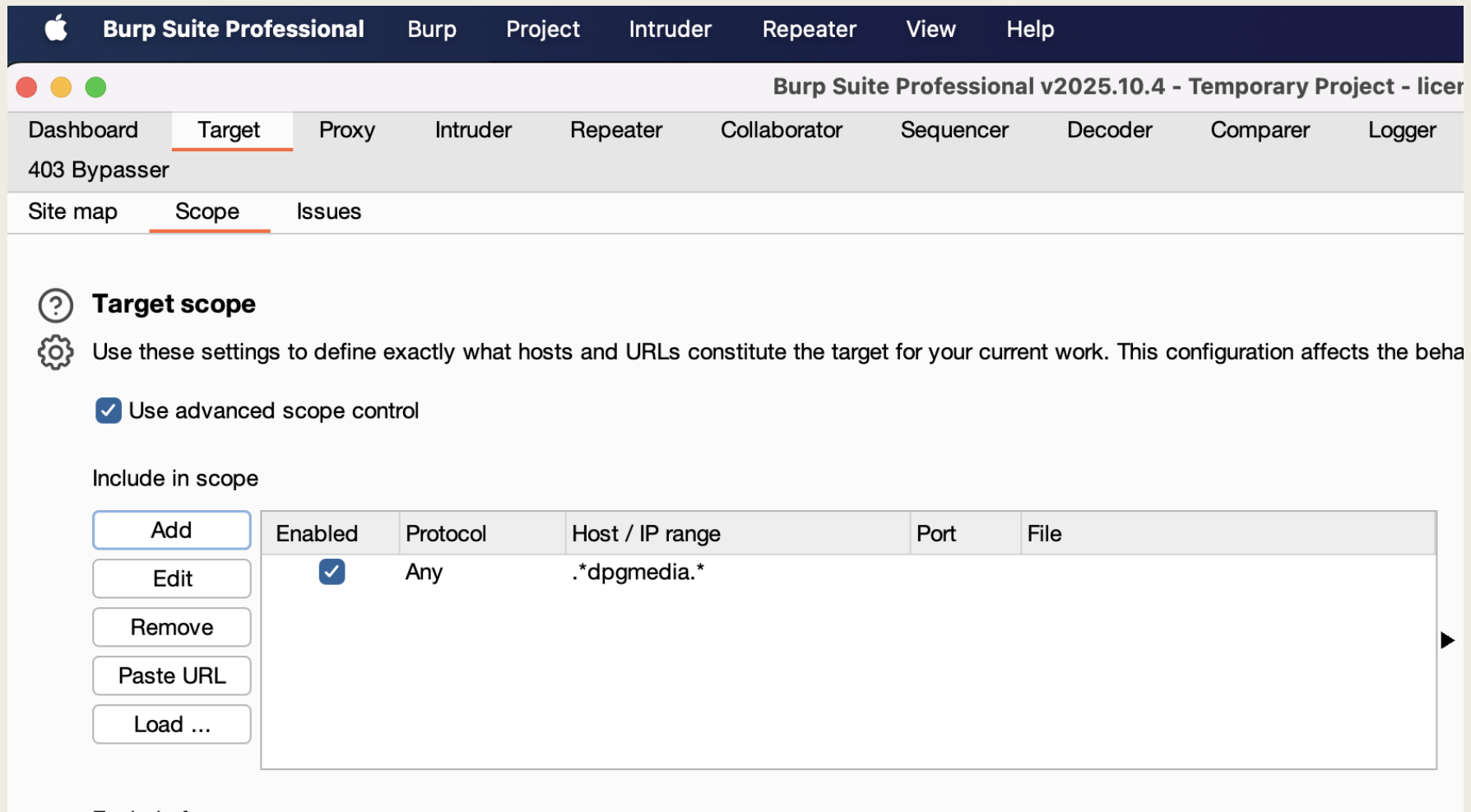
**OWASP**  
Zed Attack Proxy



**Chrome**  
DevTools

# Burpsuite - scope

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



The screenshot shows the Burp Suite Professional interface. The top menu bar includes Apple logo, Burp Suite Professional, Burp, Project, Intruder, Repeater, View, and Help. The main window title is "Burp Suite Professional v2025.10.4 - Temporary Project - license". The left sidebar has tabs for Dashboard, Target (selected), Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, and Logger. Below these are Site map, Scope (selected), and Issues. The main content area shows the "Target scope" settings. A gear icon is next to the title. Below it, a description states: "Use these settings to define exactly what hosts and URLs constitute the target for your current work. This configuration affects the behavior of the tool." A checkbox labeled "Use advanced scope control" is checked. Under the heading "Include in scope", there is a table with columns: Enabled, Protocol, Host / IP range, Port, and File. The table contains one row with a checked checkbox, "Any" for Protocol, and ".\*dpgmedia.\*" for Host / IP range. To the left of the table are buttons: Add, Edit, Remove, Paste URL, and Load ....

**Target scope**

Use these settings to define exactly what hosts and URLs constitute the target for your current work. This configuration affects the behavior of the tool.

☒ Use advanced scope control

Include in scope

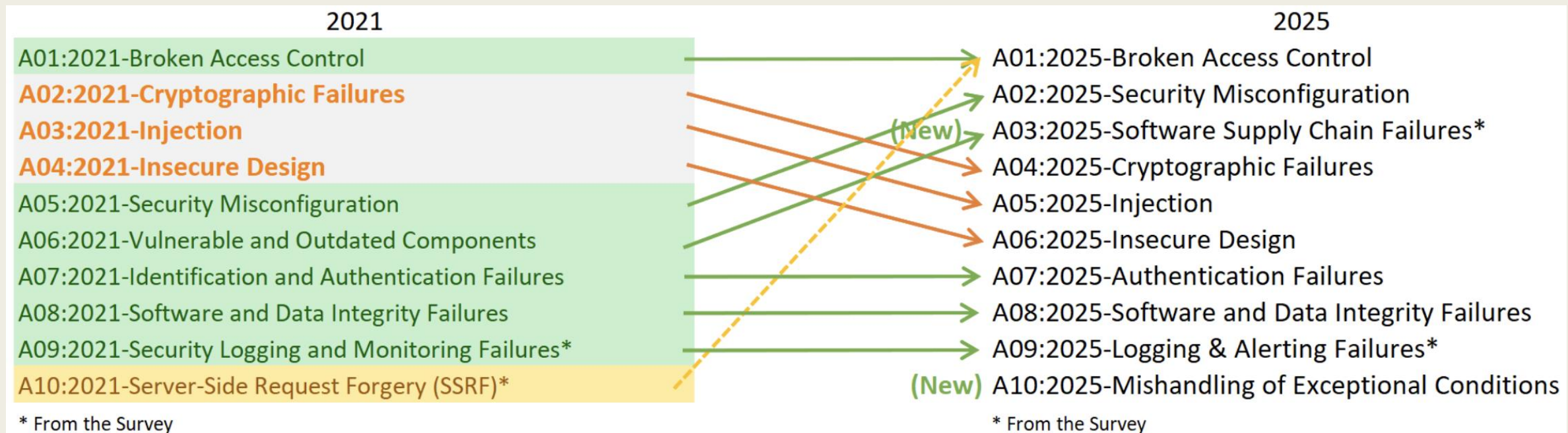
| Enabled                             | Protocol | Host / IP range | Port | File |
|-------------------------------------|----------|-----------------|------|------|
| <input checked="" type="checkbox"/> | Any      | .*dpgmedia.*    |      |      |

Buttons: Add, Edit, Remove, Paste URL, Load ...

# Our goal is to find deep complex functionality

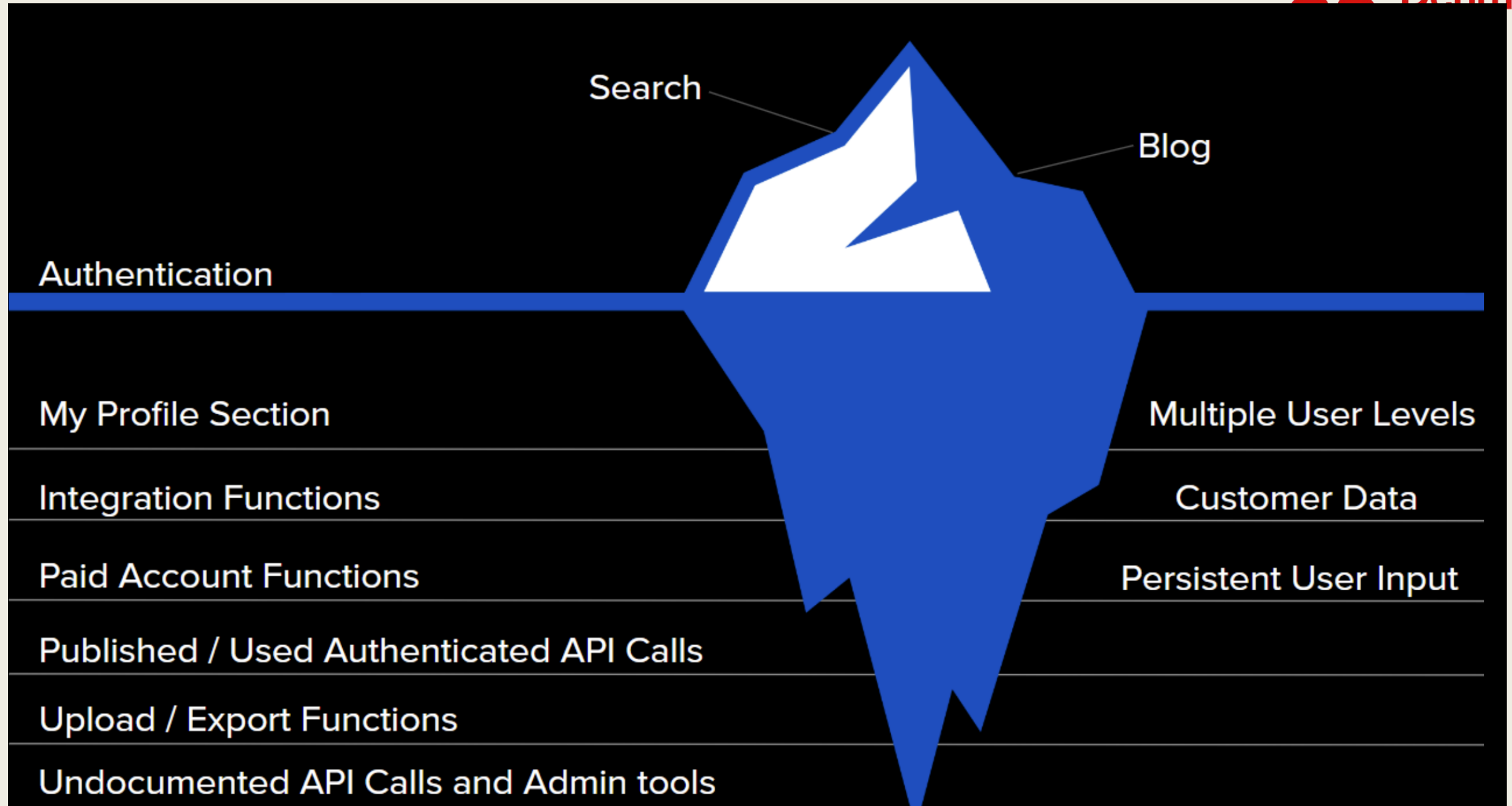
- This is often behind auth
  - *Here is our chance to hack other users of the platform (usually higher impact)*
  - *We can test for **Access control issues***
- Also often behind payment, so we may have to spend some money on some product
  - *Fewer testers, more chance of bugs*
- If we can get accounts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

# Look at these OWASP TOP 10 vulns



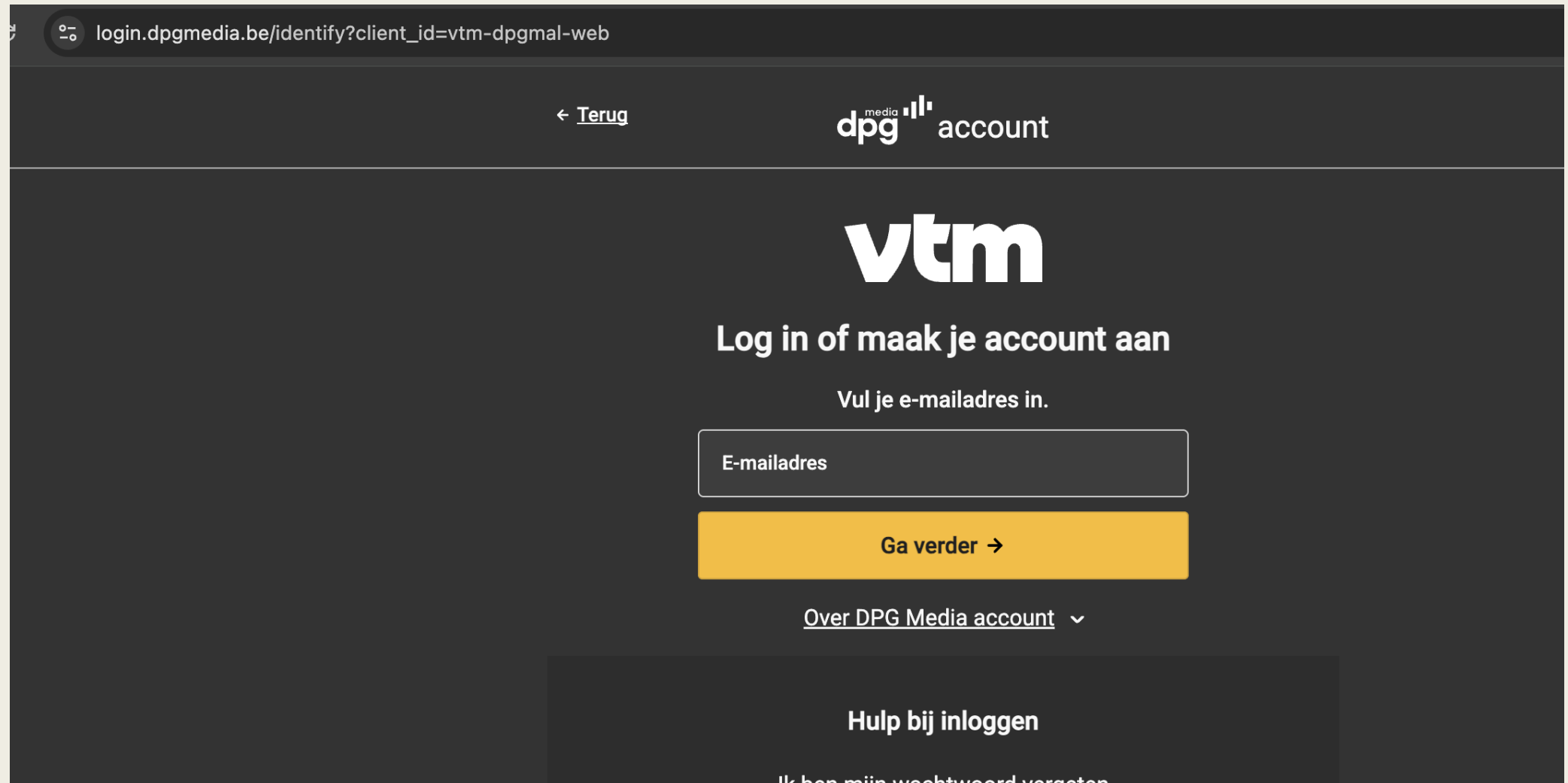
Access control still number 1, how hard can it be???

*Apparantly it IS hard*



# Lets create an account

[https://login.dpgmedia.be/identify?client\\_id=vtm-dpgmal-web](https://login.dpgmedia.be/identify?client_id=vtm-dpgmal-web)

A screenshot of a web browser showing the login page for VTM. The browser's address bar displays the URL 'login.dpgmedia.be/identify?client\_id=vtm-dpgmal-web'. The page has a dark grey background. At the top, there is a navigation bar with a back arrow and the text 'Terug' on the left, and the 'dpg media account' logo on the right. The 'dpg media' logo consists of the letters 'dpg' in a bold, lowercase font, followed by 'media' in a smaller font, and 'account' in a larger, bold font. Below the navigation bar, the 'vtm' logo is prominently displayed in a large, white, lowercase font. Underneath the logo, the text 'Log in of maak je account aan' is written in a white, sans-serif font. Below this, the instruction 'Vul je e-mailadres in.' is shown. A white rectangular input field with the placeholder text 'E-mailadres' is positioned next. Below the input field is a large, orange rectangular button with the text 'Ga verder →' in a white, sans-serif font. At the bottom of the page, there is a link 'Over DPG Media account' followed by a downward-pointing chevron icon. A dark grey footer bar at the very bottom contains the text 'Hulp bij inloggen' in a white, sans-serif font, and below it, the text 'Ik ben mijn wachtwoord vergeten' is partially visible.

# Lets create an account - Notice

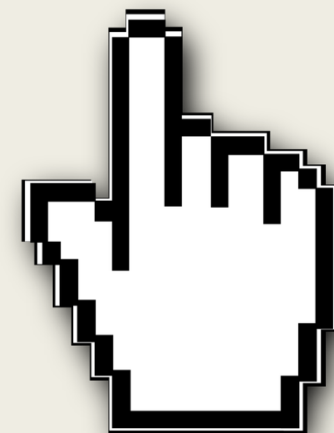
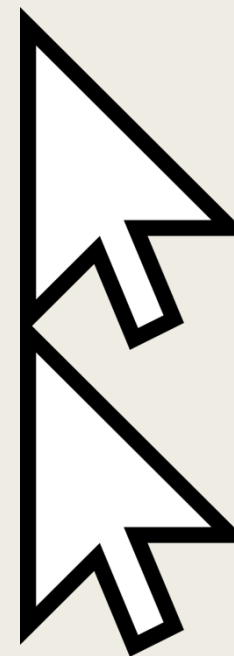
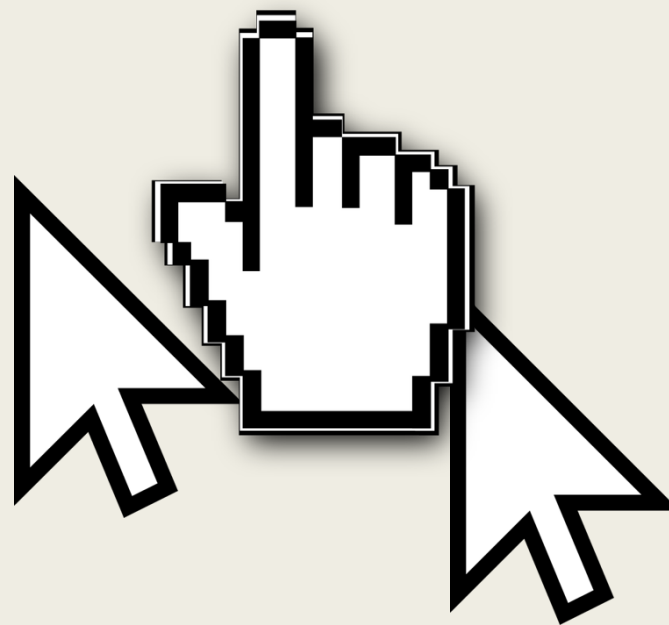
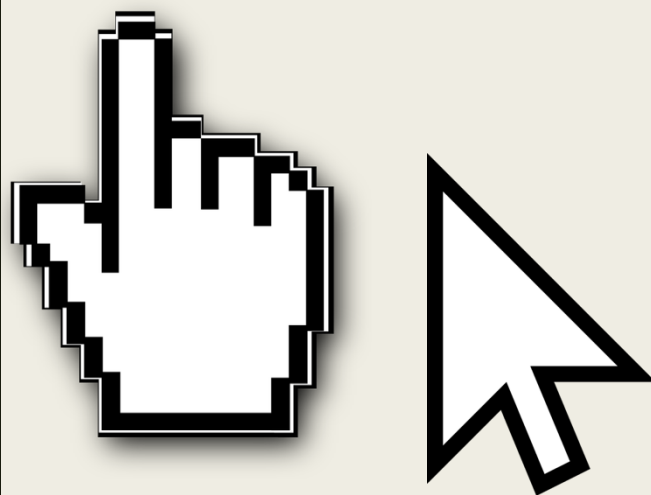
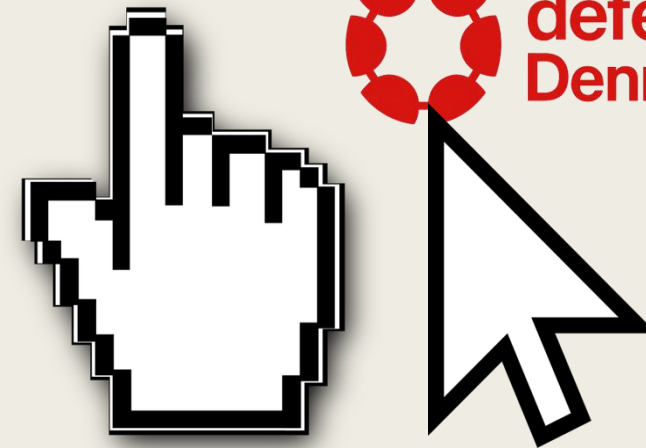
- Remember to use the email accounts from the platforms
- Remember to use the email accounts from the platforms
- They are essentially email forwarders
- Helps the defensive teams see you are doing good faith research
  - Intigrity: [username@intigrity.me](mailto:username@intigrity.me)
  - Hackerone: [username@wearehackerone.com](mailto:username@wearehackerone.com)
  - YWH: ?

## EMAIL ALIAS

HunterExample-ywh-595bb6e68b56a0b2@bounty-factory.com 

# 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 -- Targetview



Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Comparer

Logger

Organizer

Extensions

Learn

Re

403 Bypasser

Site map

Scope

Issues

Logging of out-of-scope Proxy traffic is disabled

Re-enable

URL view

Crawl paths view

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

> dpgmedia.atlassian.net

> be-pool-app.vercel.app

> brandbox-dpgmedia.nl

> account.dpgmedia.be

> foto.dpgmedia.be

> foto.dpgmedia.be

> login.dpgmedia.be

> myprivacy.dpgmedia.be

> pg.dpgmedia.be

> privacy.dpgmedia.be

> themaskedsinger.dpgmedia.be

> www.dpgmedia.be

> www.dpgmedia.be

> advertising-module.api.dpgmedia.cloud

> api.radio.dpgmedia.cloud

> muxo-cms.471112767068.dpgmedia.cloud

> pool.addata.dpgmedia.cloud

> video-advertising-transcoding-portal-api.target.dpgmedia.cloud

> video-advertising-transcoding-portal.target.dpgmedia.cloud

> c.dpgmedia.net

> login-nonprod-static.dpgmedia.net

> login-static.dpgmedia.net

> myprivacy-static.dpgmedia.net

> myprivacy.dpgmedia.net

> pg.dpgmedia.net

> sf-video.dpgmedia.net

Contents

Search

| Host                     | Method | URL                                                  |
|--------------------------|--------|------------------------------------------------------|
| https://dpgmedia.atla... | GET    | /servicedesk/customer/user/login?destination=portals |
| https://dpgmedia.atla... | GET    | /servicedesk/customer                                |
| https://dpgmedia.atla... | GET    | /servicedesk/customer/portals                        |
| https://dpgmedia.atla... | GET    | /                                                    |
| https://dpgmedia.atla... | GET    | /gateway/api/gasv3/api/v1/metadata                   |
| https://dpgmedia.atla... | GET    | /rest/webResources/1.0/resources                     |
| https://dpgmedia.atla... | GET    | /servicedesk/customer/user/login                     |
| https://dpgmedia.atla... | GET    | /servicedesk/customer/user/login?user-email=         |

Request

Response

Pause

Full Screen

Pretty

Raw

Hex

Render

Copy

Find

Menu

1 HTTP/2 200 OK

2 Content-Type: application/json

3 Content-Length: 31

4 Date: Tue, 02 Dec 2025 14:22:21 GMT

5 Vary: Origin,Access-Control-Request-Method,Access-Control-Request-Header

6 Cache-Control: no-cache, no-store, max-age=0, must-revalidate

7 Pragma: no-cache

8 Expires: 0

9 X-Frame-Options: DENY

10 Server: AtlassianEdge

11 X-Trace-Id: aef951cd61ee44f58ae2cf0352dd18dc

12 X-Content-Type-Options: nosniff

13 X-Xss-Protection: 1; mode=block

14 Atl-Traceid: aef951cd61ee44f58ae2cf0352dd18dc

15 Atl-Request-Id: aef951cd-61ee-44f5-8ae2-cf0352dd18dc

16 Strict-Transport-Security: max-age=63072000; includeSubDomains; preload

17 Report-To: {\"endpoints\": [\"url\"]}

Help

Settings

Previous

Next

Search

0 highlights

Event log (16) All issues (434)

# Registering flow



URL view Crawl paths view Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Contents

|             | Method | URL                                | Params | Status code |
|-------------|--------|------------------------------------|--------|-------------|
| dpgmedia... | POST   | /register?client_id=vtm-dpgmal-web | ✓      | 303         |
| dpgmedia... | POST   | /register?client_id=vtm-dpgmal-web | ✓      | 303         |
| dpgmedia... | GET    | /register?client_id=vtm-dpgmal-web | ✓      | 307         |
| dpgmedia... | GET    | /register                          |        |             |
| dpgmedia... | POST   | /register                          | ✓      |             |
| dpgmedia... | POST   | /register                          | ✓      |             |
| dpgmedia... | POST   | /register                          | ✓      |             |
| dpgmedia... | POST   | /register                          | ✓      |             |

Request Response

Pretty Raw Hex

```
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 14.7; rv:134.0)
    Gecko/20100101 Firefox/134.0
13 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://login.dpgmedia.be/register?client_id=vtm-dpgmal-web
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Priority: u=0, i
22
23 test=false&email=0xlime%40intigrity.me&password=[REDACTED]&gender=m&
    firstName=Emilos&lastName=Hackerboi&birthDate=23+-+09+-+1993&country=
    %F0%9F%87%A9%F0%9F%87%B0&postalCode=2300&street=superstreet&houseNumber=10&
    houseNumberSuffix=10
```

Inspector Notes

0 highlights

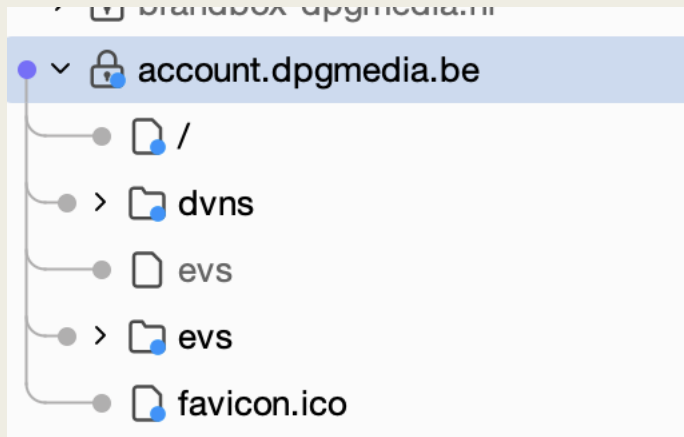


# BURP PLUGINS AND TOOLS THAT I LIKE

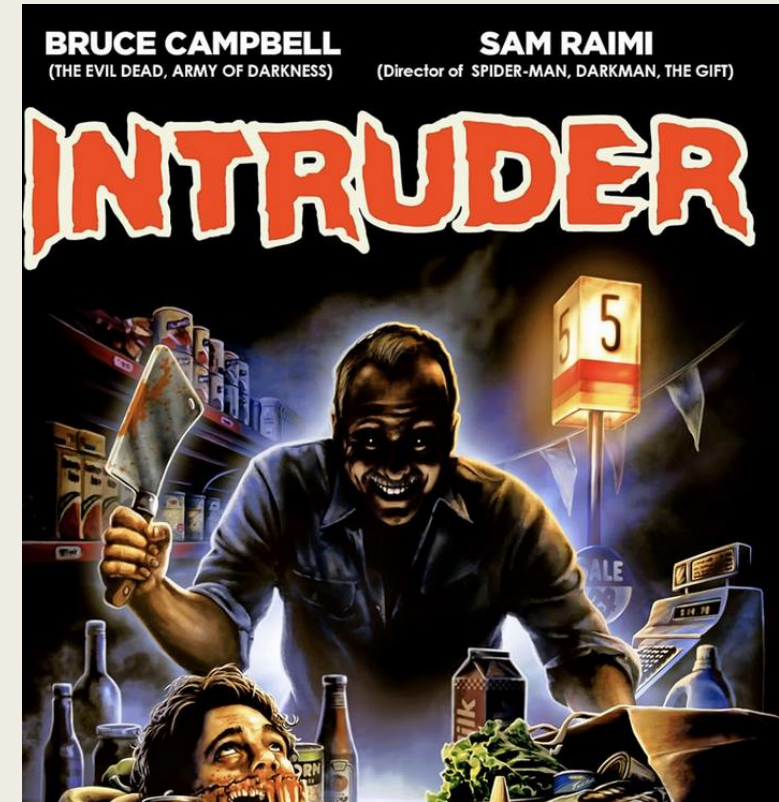
# My favourite tools for analysis

## Burp Intruder

- The account.dpgmedia.be is quite sparse:



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





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
=
448D71BD2A220E6F83F2B99C41D7C5F7~00000000000000000000000000000000~YAAQb5tkXy
dacrZ0ZZJfSXNrzjbEEGvVUPgLd0TltSc6usPfvTynML9Cwj rIvdysTtaT8wFiGP4vYD0T2x7F
eshAUMj98mn7ATGsyC/4Vnc5Jq4fYj7XzbgBW1+aK0pDsmeFIV+NK9uBowvadaK92tWp+oL8xp
kBHlk8Kx4BcUAjXF7QN9dbAuGo64c0glBkHwMo2AS+pwJYx79xD+I3tHcV7QwygrjDsIsJkbDE
AF3lLF/t5hXN:  sn ses.ed2c=*:  aa=GA1.2.1684826722.1764693284:  aid=GA1.2.
```

**Payloads**⌵⌵✕

Payload position:

Payload type:

Payload count:

Request count:

Payload configuration

This payload type  
payloads.

Paste

Load...

Remove

Clear

Deduplicate

Add

All payload positions

Simple list

Simple list

Runtime file

Custom iterator

Character substitution

Case modification

Recursive grep

Illegal Unicode

Character blocks

Numbers

Dates

Brute forcer

Null payloads

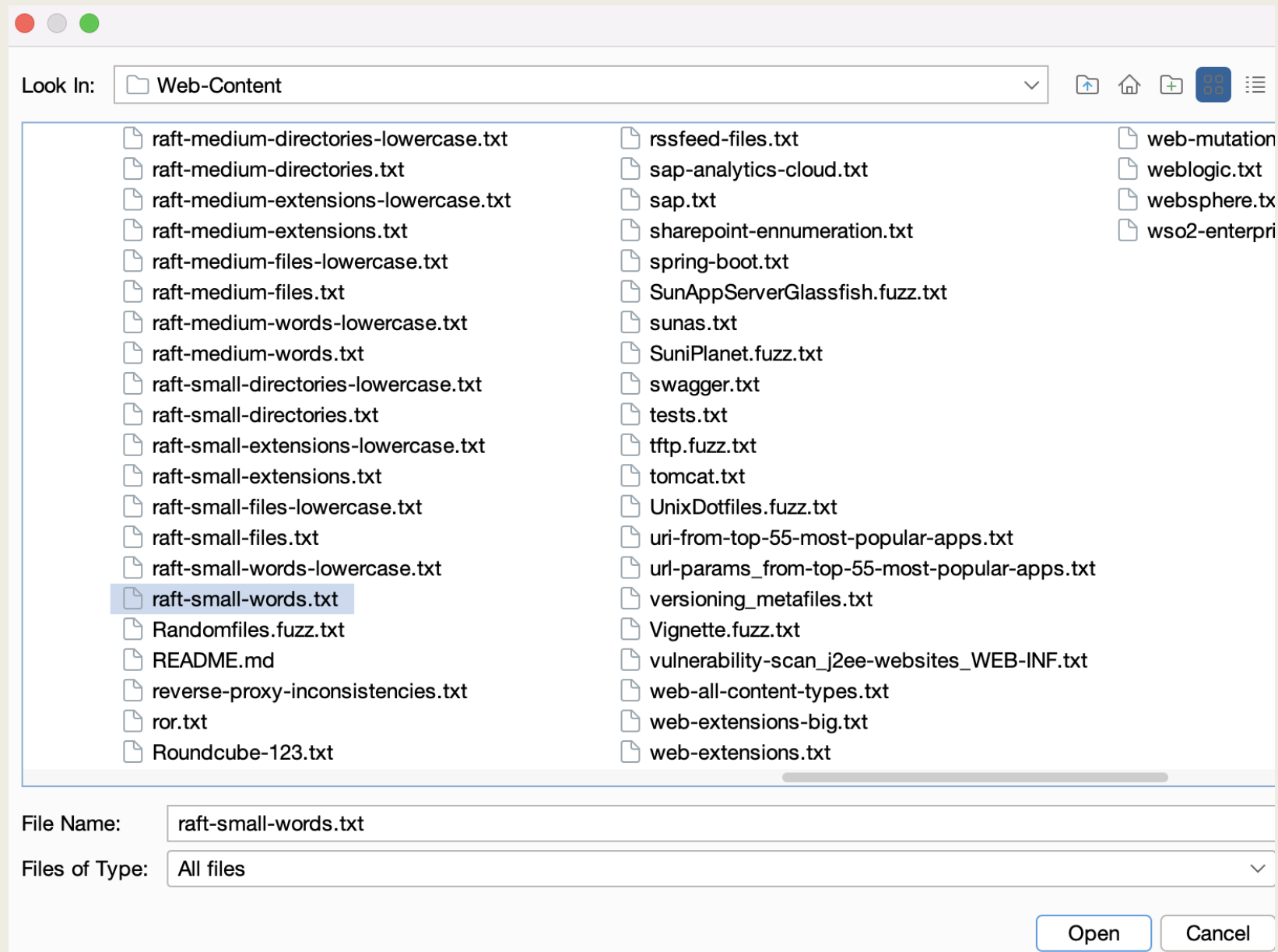
Character frobber

Bit flipper

Username generator

Enter a new item

Add from list...



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

## 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

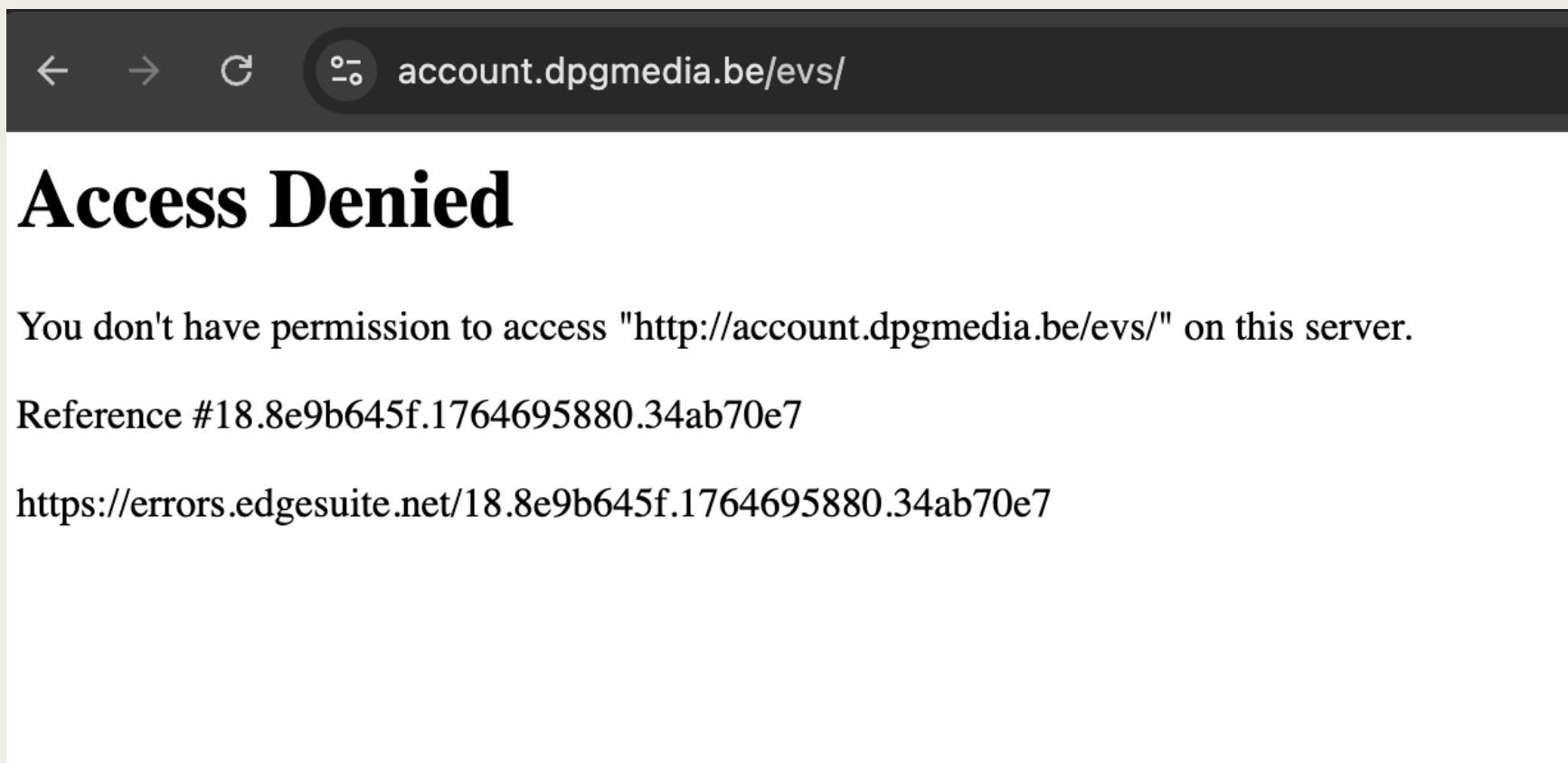
Pretty Raw Hex Render

```

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

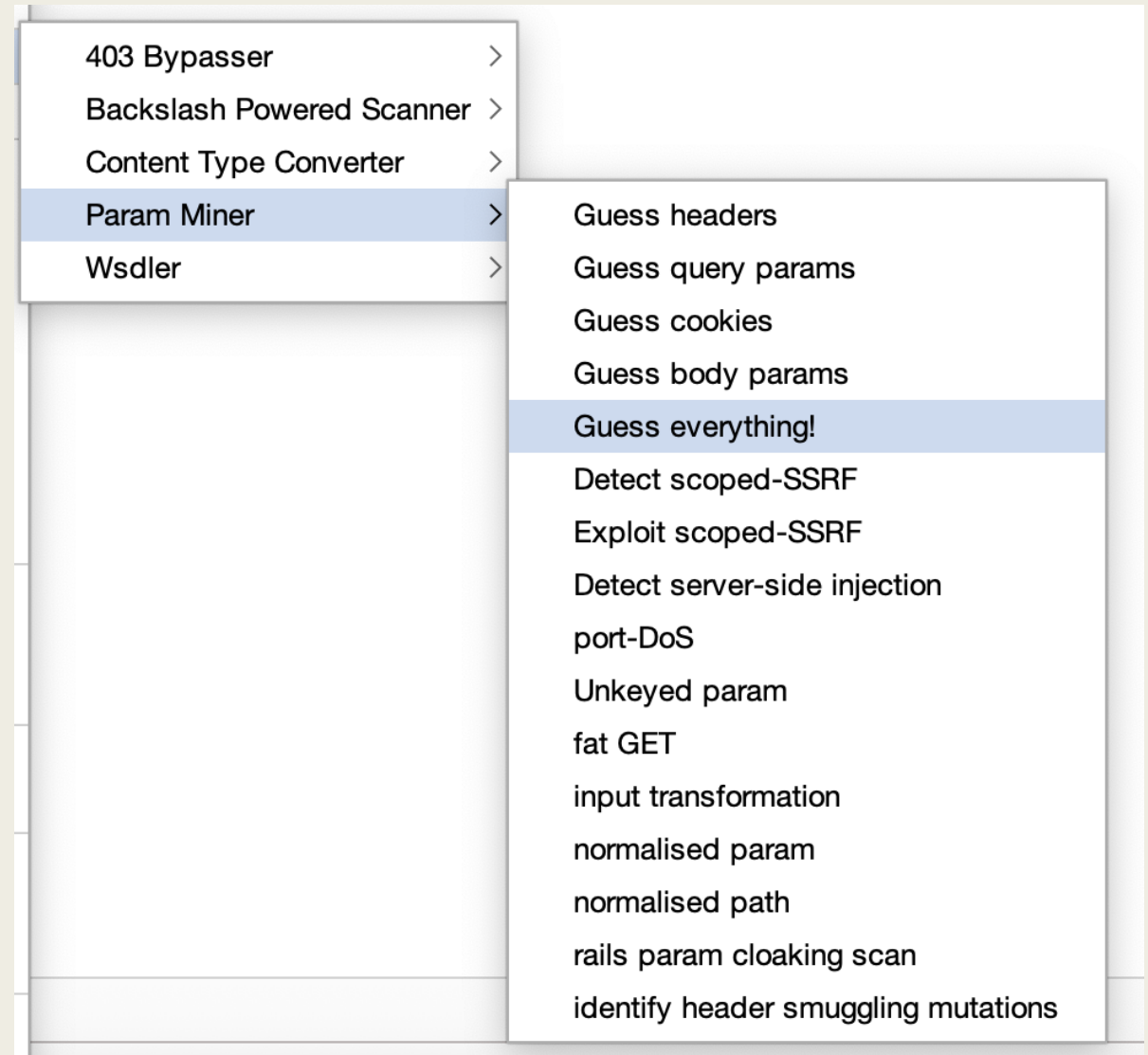
```

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

Attack Config

|                               |                                     |                                      |                                     |                                 |                                     |
|-------------------------------|-------------------------------------|--------------------------------------|-------------------------------------|---------------------------------|-------------------------------------|
| per-thread throttle:          | 0                                   | thread pool size:                    | 5                                   | infinite scan:                  | <input type="checkbox"/>            |
| live scan:                    | <input type="checkbox"/>            | use key:                             | <input checked="" type="checkbox"/> | key method:                     | <input checked="" type="checkbox"/> |
| key path:                     | <input type="checkbox"/>            | key status:                          | <input checked="" type="checkbox"/> | key content-type:               | <input checked="" type="checkbox"/> |
| key server:                   | <input checked="" type="checkbox"/> | key input name:                      | <input checked="" type="checkbox"/> | key header names:               | <input type="checkbox"/>            |
| filter:                       |                                     | mimetype-filter:                     |                                     | resp-filter:                    |                                     |
| filter HTTP:                  | <input type="checkbox"/>            | skip vulnerable hosts:               | <input type="checkbox"/>            | skip flagged hosts:             | <input type="checkbox"/>            |
| flag new domains:             | <input type="checkbox"/>            | report to organizer:                 | <input type="checkbox"/>            | confirmations:                  | 5                                   |
| require consistent evidence:  | <input checked="" type="checkbox"/> | quantile factor:                     | 2                                   | quantitative diff keys:         | time                                |
| quantitative confirmations:   | 50                                  | include query-param in cachebusters: | <input checked="" type="checkbox"/> | include origin in cachebusters: | <input checked="" type="checkbox"/> |
| include path in cachebusters: | <input type="checkbox"/>            | include via in cachebusters:         | <input checked="" type="checkbox"/> | misc header cachebusters:       | <input type="checkbox"/>            |
| custom header cachebuster:    |                                     | learn observed words:                | <input type="checkbox"/>            | skip boring words:              | <input checked="" type="checkbox"/> |
| only report unique params:    | <input type="checkbox"/>            | response-headers:                    | <input checked="" type="checkbox"/> | response-body:                  | <input checked="" type="checkbox"/> |
| request:                      | <input checked="" type="checkbox"/> | use basic wordlist:                  | <input checked="" type="checkbox"/> | use bonus wordlist:             | <input type="checkbox"/>            |
| use assetnote params:         | <input type="checkbox"/>            | use custom wordlist:                 | <input type="checkbox"/>            | custom wordlist path:           | /usr/share                          |
| bruteforce:                   | <input type="checkbox"/>            | skip uncacheable:                    | <input type="checkbox"/>            | dynamic keyload:                | <input type="checkbox"/>            |
| max one per host:             | <input type="checkbox"/>            | max one per host+status:             | <input type="checkbox"/>            | probe identified params:        | <input checked="" type="checkbox"/> |
| scan identified params:       | <input type="checkbox"/>            | fuzz detect:                         | <input type="checkbox"/>            | carpet bomb:                    | <input type="checkbox"/>            |
| try cache poison:             | <input checked="" type="checkbox"/> | twitchy cache poison:                | <input type="checkbox"/>            | identify smuggle mutations:     | <input type="checkbox"/>            |
| try -_ bypass:                | <input type="checkbox"/>            | rotation interval:                   | 999                                 | rotation increment:             | 4                                   |
| force bucketsize:             | -1                                  | max bucketsize:                      | 65,536                              | max param length:               | 32                                  |
| lowercase headers:            | <input checked="" type="checkbox"/> | name in issue:                       | <input type="checkbox"/>            | canary:                         | zwrtxqva                            |
| force canary:                 |                                     | poison only:                         | <input type="checkbox"/>            | tunnelling retry count:         | 20                                  |
| abort on tunnel failure:      | <input checked="" type="checkbox"/> | baseline size:                       | 4                                   |                                 |                                     |

Reset Visible Settings

Cancel

OK

# Burp Param Miner



Burp Suite Professional v2024.6-29931 (Early Adopter) - Temporary Project - licensed to Vulscan Digital Security [single user license]

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Logger++ Search Settings

Installed BApp Store APIs BChecks Extensions settings

Total estimated system impact: **Medium**

### Burp extensions

Extensions let you customize Burp's behavior using your own or third-party code.

Add Remove Up Down

| Loaded                              | Type | Name                    | System impact |
|-------------------------------------|------|-------------------------|---------------|
| <input type="checkbox"/>            | Java | Sensitive Data Detector | Low           |
| <input checked="" type="checkbox"/> | Java | API Discovery           | Low           |
| <input checked="" type="checkbox"/> | Java | Param Miner             | Low           |
| <input checked="" type="checkbox"/> | Java | Distribute Damage       | Low           |

Details Output Errors

☐ Output to system console

☐ Save to file:

☒ Show in UI:

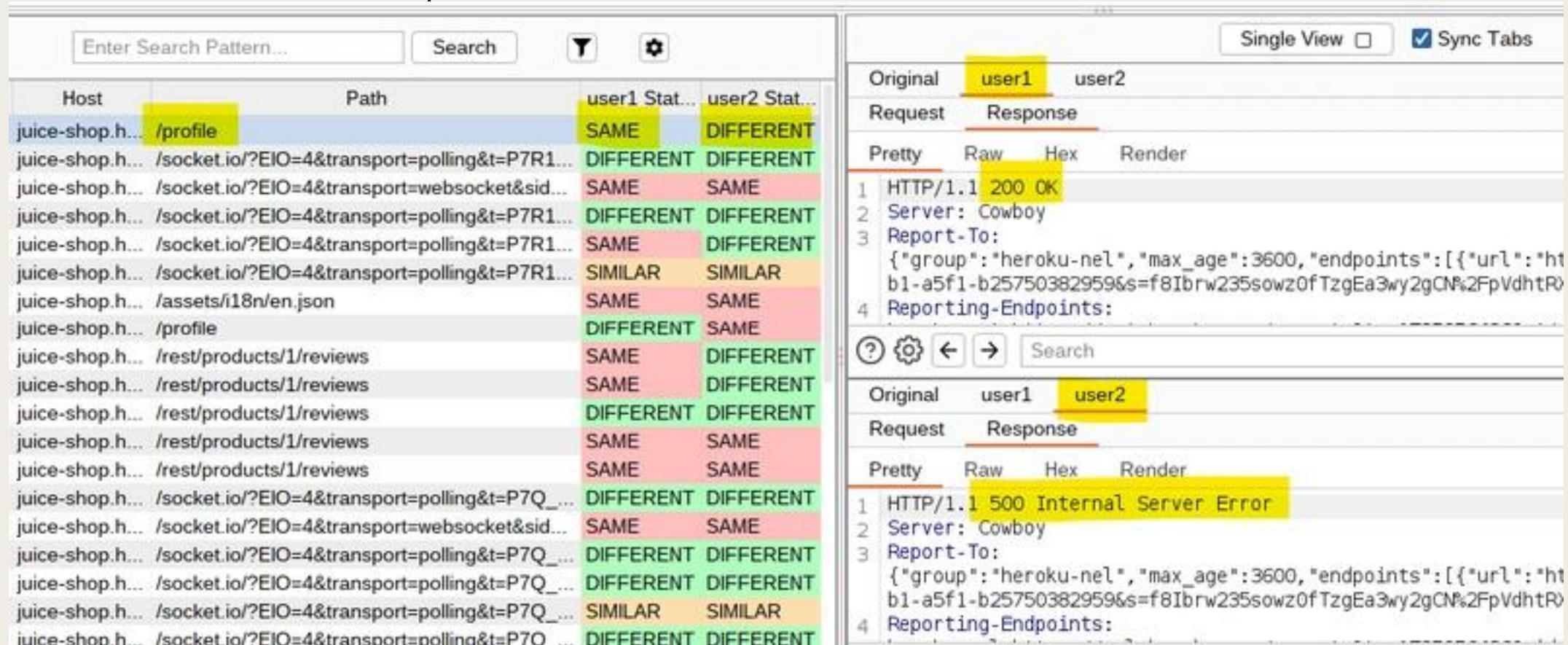
```
1 Using albinowaxUtils v1.03
2 This extension should be run on the latest version of Burp Suite. Using an older version of Burp may cause impaired functionality.
3 Loaded Param Miner v1.4f
4 Updating active thread pool size to 8
5 Queued 1 attacks
6 Updating active thread pool size to 8
7 Queued 1 attacks
8 Updating active thread pool size to 8
9 Queued 1 attacks
10 Updating active thread pool size to 8
11 Queued 1 attacks
12 Setting bucketSize to 8 due to slow response
13 Initiating header bruteforce on crapi.apisec.ai
14 Setting bucketSize to 16 due to slow response
15 Initiating cookie bruteforce on crapi.apisec.ai
16 Initiating url bruteforce on crapi.apisec.ai
17 Initiating url bruteforce on crapi.apisec.ai
18 Updating active thread pool size to 8
19 Queued 1 attacks
20 Setting bucketSize to 16 due to slow response
21 Unrecognised type: 6
22 Initiating json bruteforce on crapi.apisec.ai
23 Identified parameter on crapi.apisec.ai: password
24
```

Clear Search 0 highlights

Memory: 242.3MB

# 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



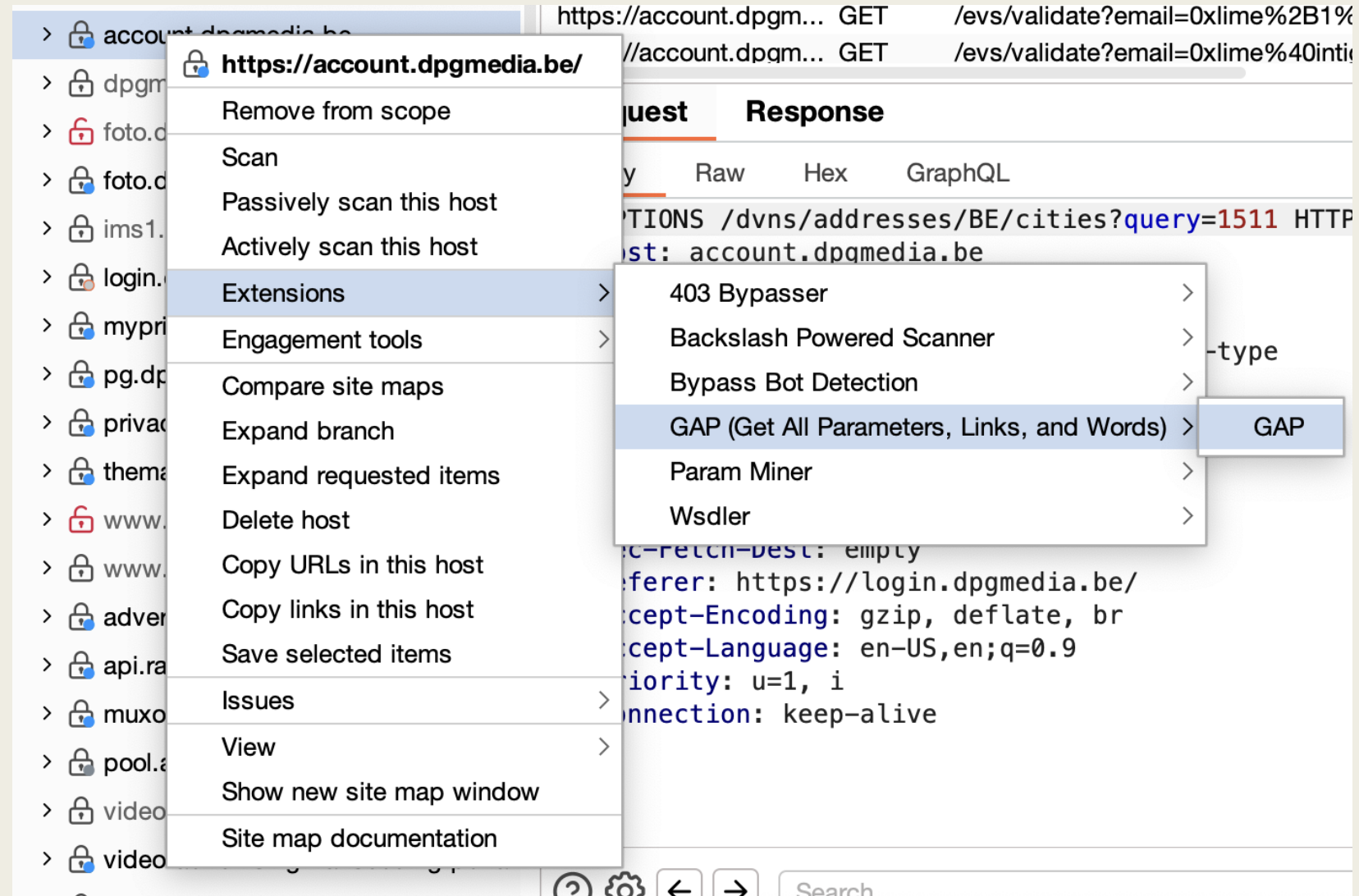
The screenshot displays the Burp Auth Analyzer interface. The main table compares the status of various requests for two users, user1 and user2. The table has columns for Host, Path, user1 Stat..., and user2 Stat....

| Host            | Path                                          | user1 Stat... | user2 Stat... |
|-----------------|-----------------------------------------------|---------------|---------------|
| juice-shop.h... | /profile                                      | SAME          | DIFFERENT     |
| juice-shop.h... | /socket.io/?EIO=4&transport=polling&t=P7R1... | DIFFERENT     | DIFFERENT     |
| juice-shop.h... | /socket.io/?EIO=4&transport=websocket&sid...  | SAME          | SAME          |
| juice-shop.h... | /socket.io/?EIO=4&transport=polling&t=P7R1... | DIFFERENT     | DIFFERENT     |
| juice-shop.h... | /socket.io/?EIO=4&transport=polling&t=P7R1... | SAME          | DIFFERENT     |
| juice-shop.h... | /socket.io/?EIO=4&transport=polling&t=P7R1... | SIMILAR       | SIMILAR       |
| juice-shop.h... | /assets/i18n/en.json                          | SAME          | SAME          |
| juice-shop.h... | /profile                                      | DIFFERENT     | SAME          |
| juice-shop.h... | /rest/products/1/reviews                      | SAME          | DIFFERENT     |
| juice-shop.h... | /rest/products/1/reviews                      | SAME          | DIFFERENT     |
| juice-shop.h... | /rest/products/1/reviews                      | DIFFERENT     | DIFFERENT     |
| juice-shop.h... | /rest/products/1/reviews                      | SAME          | SAME          |
| juice-shop.h... | /rest/products/1/reviews                      | SAME          | SAME          |
| juice-shop.h... | /socket.io/?EIO=4&transport=polling&t=P7Q...  | DIFFERENT     | DIFFERENT     |
| juice-shop.h... | /socket.io/?EIO=4&transport=websocket&sid...  | SAME          | SAME          |
| juice-shop.h... | /socket.io/?EIO=4&transport=polling&t=P7Q...  | DIFFERENT     | DIFFERENT     |
| juice-shop.h... | /socket.io/?EIO=4&transport=polling&t=P7Q...  | DIFFERENT     | DIFFERENT     |
| juice-shop.h... | /socket.io/?EIO=4&transport=polling&t=P7Q...  | SIMILAR       | SIMILAR       |
| juice-shop.h... | /socket.io/?EIO=4&transport=polling&t=P7O...  | DIFFERENT     | DIFFERENT     |

Below the table, two detailed views of HTTP requests and responses are shown. The top view shows a successful response (200 OK) for user1, and the bottom view shows an internal server error (500 Internal Server Error) for user2. Both views include tabs for Original, Request, Response, Pretty, Raw, Hex, and Render.

# 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

GAP Burp Extension by XnL-h4ck3r

GAP Mode: ☒ Parameters ☒ Links ☒ Words

Parameters mode options:

☐ Include URL path words?

☒ Report "sus" params? ☒ Inc. Tentative?

REQUEST PARAMETERS

☒ Query string params

☒ Message body params

☒ Param attribute in multi-part message body

☐ JSON params

☐ Cookie names

☐ Items of data in XML structure

☐ Value of tag attributes in XML structure

RESPONSE PARAMETERS

☐ JSON params

☐ Value of tag attributes in XML structure

☐ Name and Id attributes of HTML input fields

☐ Javascript variables and constants

☐ Params from links found

Click for help --> ?

Buy me a coffee

Links mode options:

Prefix with: ☐ selected target(s) ☐ origin target only ☐ link(s):

☐ Also include un-prefixed links? ☐ Include site map endpoints? ☒ Include relative links?

Words mode options:

☒ Create lowercase words? ☒ Include HTML comments? ☒ Include words with digits?

☒ Create singular/plural word? ☒ Include IMG ALT attribute? ☐ Include URL path words?

Word length:  to  (excludes plurals) ☐ Include potential params?

Other options: ☒ Show contextual help

☒ Auto save output to directory

Restore defaults

Save options

COMPLETED

100%

Potential params found - 22 filtered: ☐ Show origin

BRANDID

dateOfBirth

extensions

firstName

gender

input

lastName

otag

persistedQuery

phoneNumber

sha256Hash

status

test

touchpoint

unique

utm\_campaign

...

Show "sus" ☐ Show query string with value

Stop words:

Potential links found - 727 filtered: ☐ Show origin endpoint ☐ In scope only

/\_next/static/111-production/\_buildManifest.js

/\_next/static/111-production/\_ssgManifest.js

/\_next/static/chunks/1616-0e138eae75a8ccf8.js

/\_next/static/chunks/1941-c6f7f0661408ee61.js

/\_next/static/chunks/2074-c994d70ad537d7a2.js

/\_next/static/chunks/3333.328d4a6af97b421a.js

/\_next/static/chunks/3720.5cf16f73b7fbc2a3.js

/\_next/static/chunks/6527.47b029aa53875f6b.js

/\_next/static/chunks/7447-110eebdfbd0e9400.js

/\_next/static/chunks/8164-0e46fc95a367a698.js

/\_next/static/chunks/8358.643ed88939589745.js

/\_next/static/chunks/8423-8fe1b23d62b624f6.js

/\_next/static/chunks/8508-9faeab1c85cd9b5d.js

/\_next/static/chunks/92-383311ce39d2327a.js

/\_next/static/chunks/9663-d7ab320901a586f6.js

/\_next/static/chunks/framework-69d3f40aed6e07db.js

/\_next/static/chunks/main-7d219ad50664b5b5.js

...

Link filter:

☐ Negative match ☐ Case sensitive

# LEARNING FROM MY FINDINGS / REPORTS

# Disclosing some of my reports – Race conditions



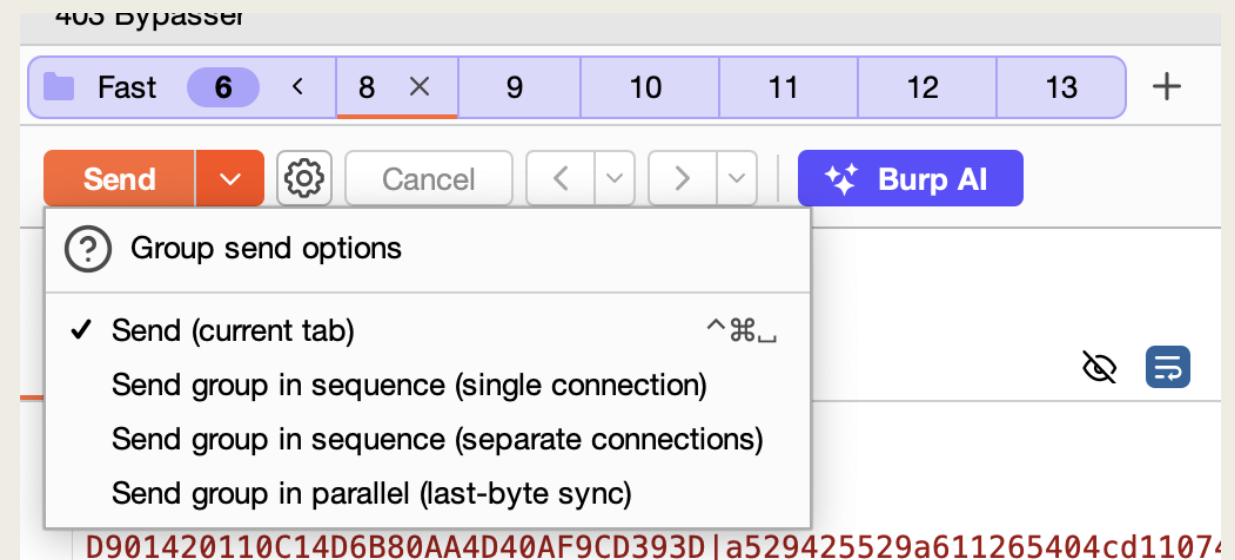
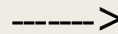
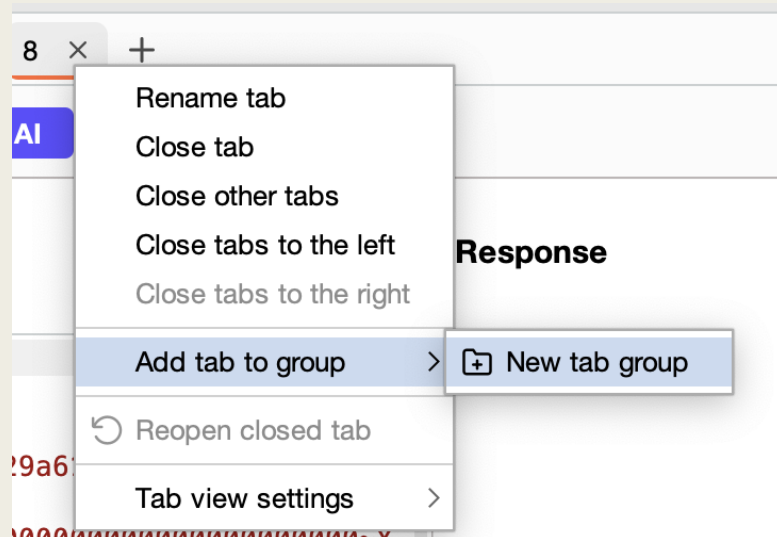
- **Title:** Fast concurrent requests can lead to more than allowed number of starred articles on  
\*\*\*\*\*
- The platform allowed selling items and marking specific items as **Starred\***
- But you could only have 5 items starred.
- There was a POST request to
  - `/api/*****/listings/7bc9c7dd-6365-426c-b8c0-07f1a23c6095/starmark`
- 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

- 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)



# 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"  
}
```

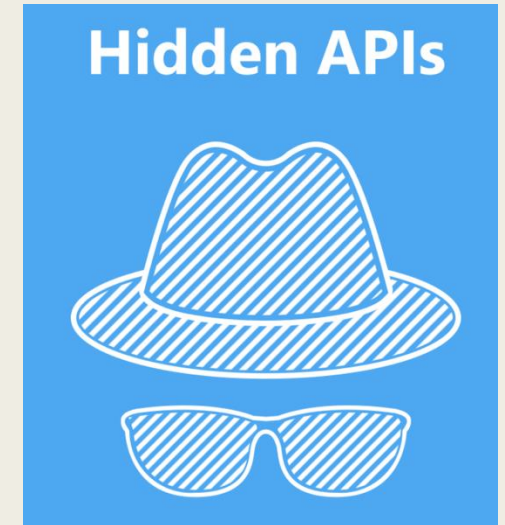
# When to look for mass assignments?

- 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



changed the **status** from **Pending** to **Accepted**

3/22/2024, 1:30:37 PM



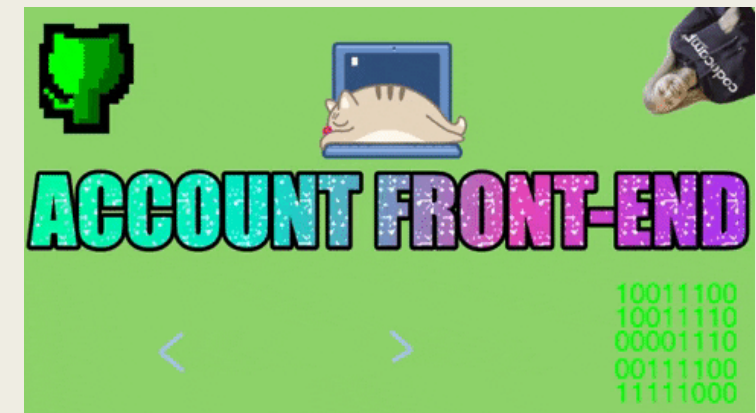
changed the **severity** from **High** (7.5) ⓘ to **High** (8.2) ⓘ, changing the possible bounty to €1,632

3/22/2024, 11:09:13 AM

Raising Availability to Low, as the target file is deleted.

# 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”



**Chrome**  
DevTools



U bent er bijna!



## Accountgegevens

E-mailadres

0xlime+1@intigriti.me

[Wijzig e-mailadres](#)

Wachtwoord

\*\*\*\*\*

[Wijzig wachtwoord](#)

Naam

Meneer Emila Hackerrrrrrrr

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...

```
trailingSlash: "/" !== e ? e.endsWith
};
r && (0,
o.pathHasPrefix)(u.pathname, r) && (u
a.removePathPrefix)(u.pathname, r),
u.basePath = r);
let l = u.pathname;
if (u.pathname.startsWith("/_next/data
let e = u.pathname.replace(/^\/_ne
u.buildId = e[0],
l = "index" !== e[1] ? `/${e.slice
!0 === t.parseData && (u.pathname
}
if (i) {
let e = t.i18nProvider ? t.i18nPro
n.normalizeLocalePath)(u.pathname,
u.locale = e.detectedLocale,
u.pathname = e.pathname ?? u.path
!e.detectedLocale && u.buildId &&
n.normalizeLocalePath)(l, i.local
}
return u
}
},
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";
```

Wappalyzer - Technology profiler

api 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 won't 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*

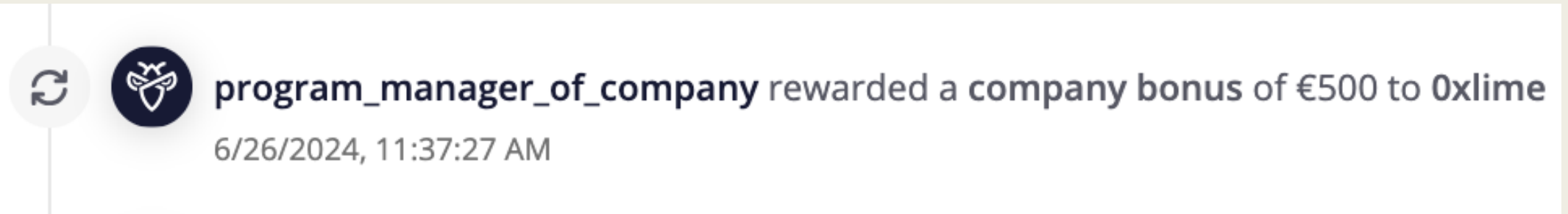
---

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*

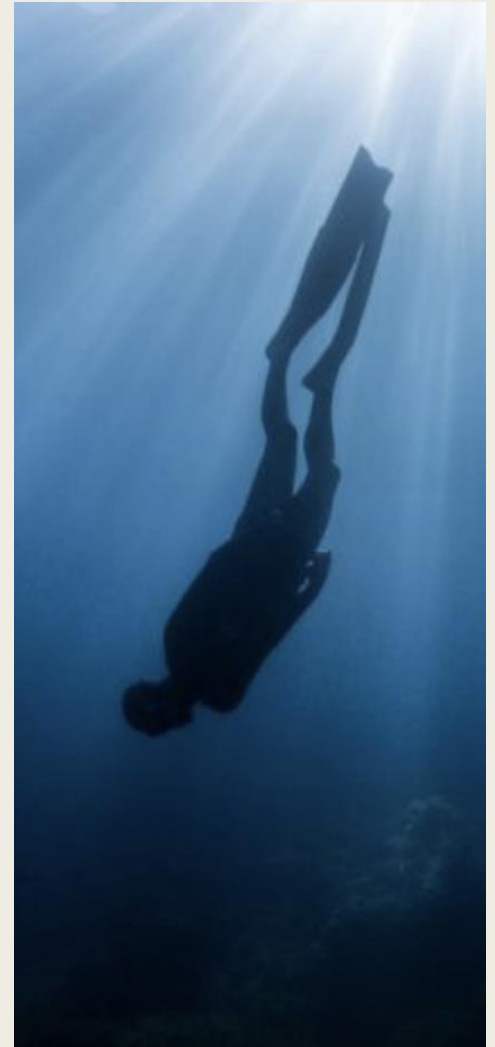


# So to summarize recon When finding a new target:

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](https://kortlink.dk/2tnre)



✨ Add me on LinkedIn ✨