PTN 9th Anniversary 🥳

30 July 2022, KTM

Automating Low hanging Bugs

By: Veshraj Ghimire

Little about the Presenter:

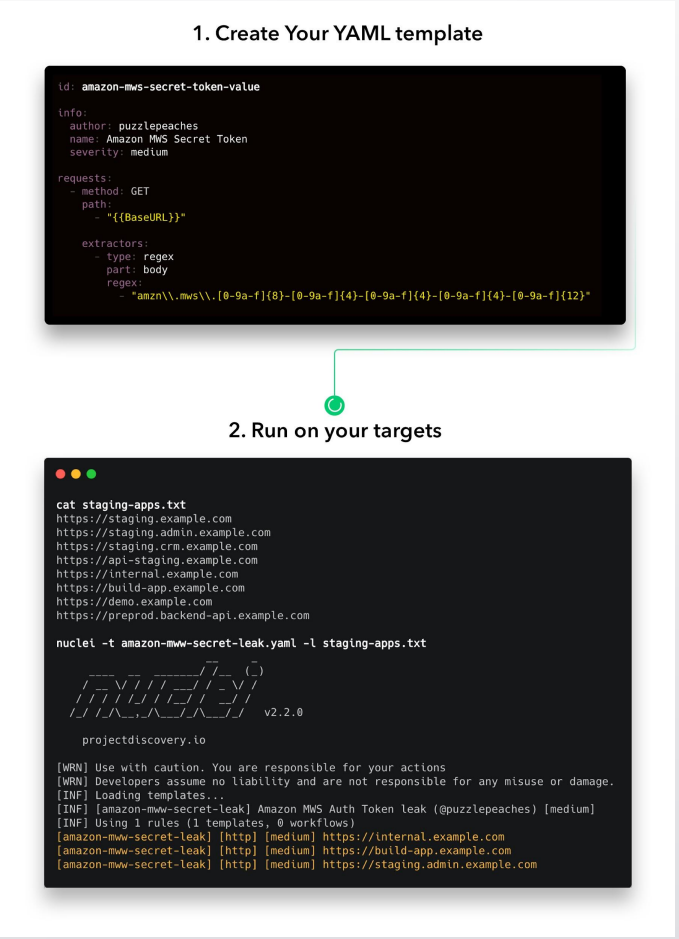
- Community Leader at Pentester Nepal
- Interested in offensive Security
- Part time bug bounty hunter
- #2 on Bugv All Time Leaderboard as of now
- Life long learner

List of tools to be discussed today

- Nuclei
- NtHiM
- Wpscan
- Gf with GAU
- Dalfox
- reNgine

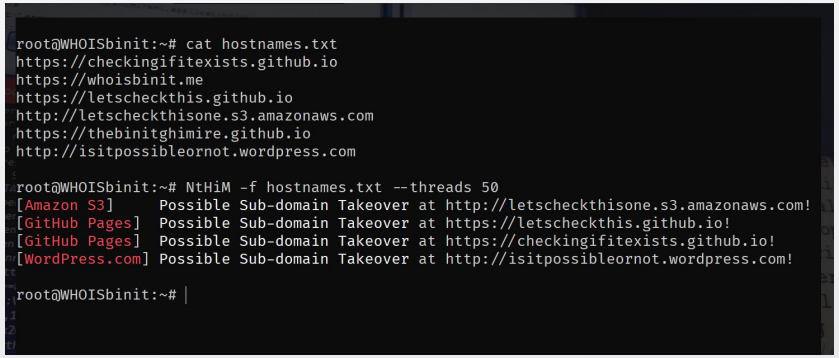
Nuclei

- By Project Discovery
- Fast and customizable vulnerability scanner based on simple YAML based DSL.
- https://github.com/projectdiscovery/nuclei



NtHiM

- By late Binit Ghimire
- Now, the Host is Mine! - Super Fast Sub-domain Takeover Detection!
- https://github.com/TheBinitGhimire/NtHiM

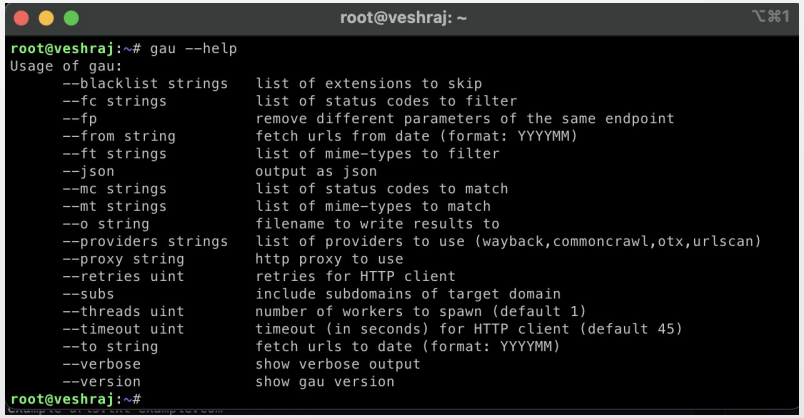


WpScan

- By wpscan Team
- WordPress security scanner. Written for security professionals and blog maintainers to test the security of their WordPress websites.
- https://github.com/wpscanteam/wpscan

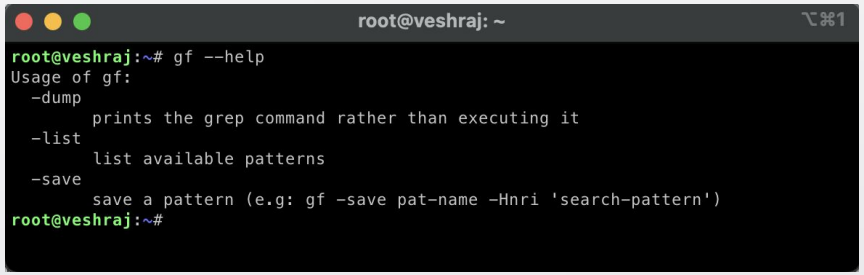
GAU

- By Corben Leo
- Fetch known URLs from AlienVault's Open Threat Exchange, the Way back Machine, and Common Crawl.
- https://github.com/lc/gau



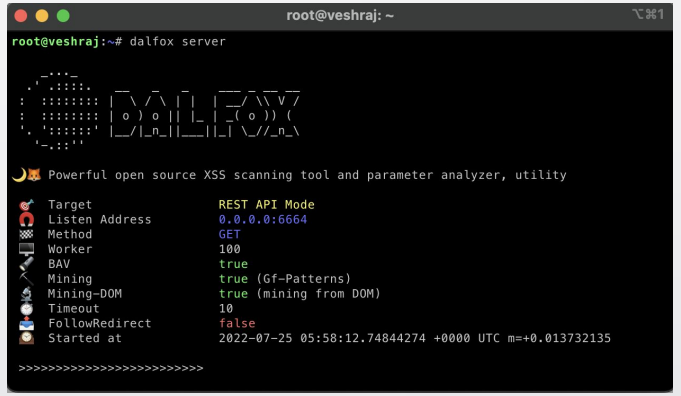
GF

- By Tomnomnom
- A wrapper around grep, to help you grep for things
- Patterns based on json
- https://github.com/tomnomnom/gf



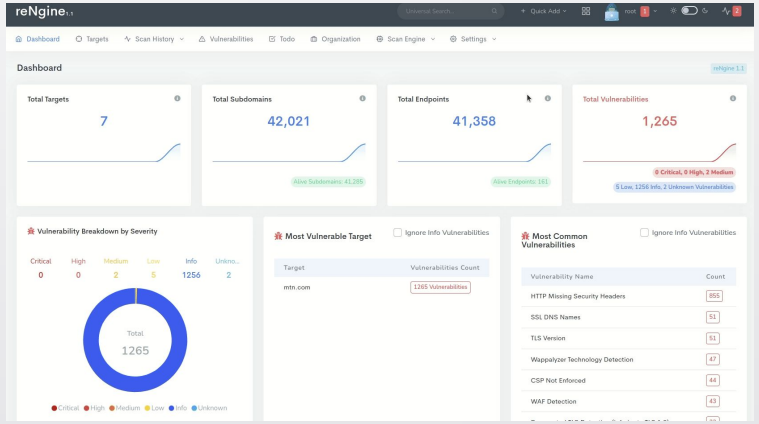
Dalfox

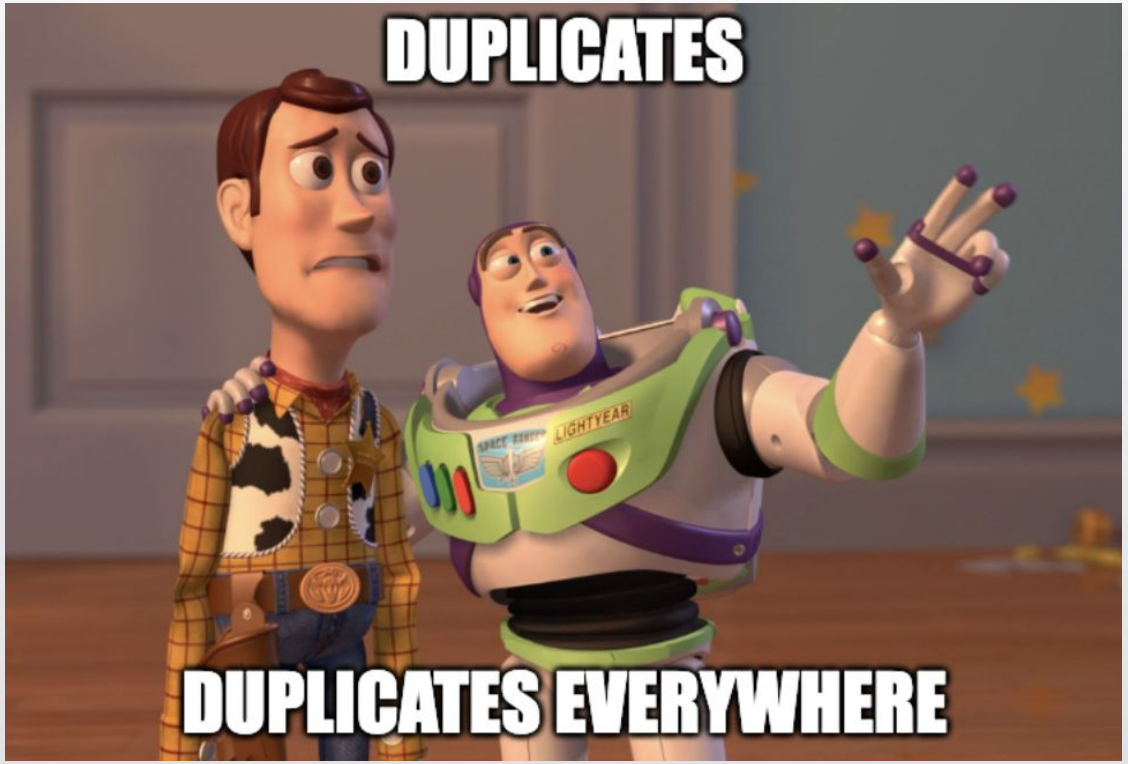
- By Hahwul
- Powerful open source XSS scanning tool and parameter analyzer, utility
- https://github.com/hahwul/dalfox



reNgine

- By Yogesh Ojha
- Automated reconnaissance framework for web applications with a focus on highly configurable streamlined recon process via Engines, recon data correlation and organization, continuous monitoring, backed by a database, and simple yet intuitive User Interface.
- https://github.com/yogeshojha/rengine




DUPLICATES
LIGHTYEAR
DUPLICATES EVERYWHERE

Some tips to avoid duplicates:

- Modify existing/ build Own Templates
- Combine tools
- Build custom wordlist
- Explore full features/ Don’t just run on default settings
- Don’t just depend upon tools

The End ☺

You can ping me on twitter if you need any help, I am pretty active there:

@GhimireVeshraj