Pentesting Automation

RAFAEL COELHO

THIS PROJECT WAS BUILT WITH THE FOLLOWING TOOLS:


QEMU

KALI LINUX


APACHE AIRFLOW

LUIGI


PYTHON


BASH

GO

NMAP


NIKTO


PROJECT DISCOVERY TOOLS

Project Discovery Tools: Nuclei | Subfinder | HTTPX | DNSX | Katana | Naabu

Python Tools: DNSReaper | Graphw00f | Arjun | SSTImap | SQLmap | SpyHunt | CORSY | XSRFProbe | XSStrike | FavFreak

Go Tools: WayBackURLs | FFuF | Goctopus | TInjA | SURF | SmuggleFuzz | Gxss | DalFox | Subzy | MX-SPF Takeover | 403jump | Favirecon | Shortscan | Trufflehog

Other Tools: Trivy

This is a complex pentesting automation developed to aiming to participate in various bug bounty programs. It scans more than 20 types of web vulnerabilities in an automated way, saving me time from manual work so that I can focus on tasks where manual and careful analysis is necessary.

I used a Kali Linux VM (virtualizer: QEMU), and several Go, Python and Bash tools.
I started using Airflow to build this automation, but for some unknown reason, despite me adjusting several parameters, Airflow was consuming a lot of CPU processing inside the VM and was making all tasks extremely slow.

To solve this problem, I replaced Airflow with Luigi, another automation framework in Python. It not only solved my problem but also gave me more flexibility to build an automation pipeline (Fun fact: Airflow was developed by Airbnb; Luigi was developed by Spotify).
Both tools are excellent; Luigi is suitable for simpler pipelines, Airflow for robust pipelines such as Data Engineering, for example.


SUBFINDER
WAYBACKURLS
HTTPX
API_DISCOVERY
DNSREAPER
BRUTEFORCE_SUBDOMAINS
DIRECTORIES
KATANA
FINAL_DATA_VERSION
DNSX
FINGERPRINT
END_A
FINAL_DATA_VERSION
CLUSTER1
V02_HOST_HEADER_INJECTION
V02_HOST_HEADER_INJECTION_FFUF
V05_API
N01_NUCLEI_API
N01_NUCLEI_GRAPHQL
V05_API_GRAPHQL_ENDPOINTS
V05_API_GOCTOPUS
V05_API_GRAPHW00F
V05_API_ARJUN
V19_TEMPLATE_INJECTION
N13_NUCLEI_TEMPLATE_INJECTION
V19_TEMPLATE_INJECTION_TINJA
V19_TEMPLATE_INJECTION_SSTIMAP
V23_INFORMATION_DISCLOSURE
V23_INFO_DISC_DIRB_FFUF
V10_FILE_INCLUSION
N06_NUCLEI_FILE_INCLUSION
V22_SQL_INJECTION
N15_NUCLEI_SQL_INJECTION
V22_SQL_INJECTION_SQLMAP
CLUSTER2
V01_CORS
V01_CORS_MISCONFIGURATION_SPYHUNT
V01_CORS_CORSY
V03_CSRF
V03_CSRF_XSRFPROBE
V04_REQUEST_SMUGGLING
V04_REQUEST_SMUGGLING_SMUGGLEFUZZ
V20_SSRF
N14_NUCLEI_SSRF
V20_SSRF_SURF
V18_XSS
N12_NUCLEI_XSS
V18_XSS_GXSS
V18_XSS_DALFOX
V18_XSS_XSSTRIKE
CLUSTER3
V06_OPEN_REDIRECT
N02_NUCLEI_OPEN_REDIRECT
V07_IDOR
N03_NUCLEI_IDOR
V08_XXE
N04_NUCLEI_XXE
V09_RCE
N05_NUCLEI_RCE
V11_COOKIE
N07_NUCLEI_COOKIE
V12_OAUTH
N08_NUCLEI_OAUTH
V13_TAKEOVER
N09_NUCLEI_TAKEOVER
V13_TAKEOVER_SUBZY
V13_TAKEOVER_MX_SPF
V14_TRAVERSAL
N10_NUCLEI_TRAVERSAL
V15_CRLF_INJECTION
N11_NUCLEI_CRLF_INJECTION
V16_403_BYPASS
V16_403_BYPASS_403JUMP
V17_FAVICON
V17_FAVICON_FAVFREAK
V17_FAVICON_FAVIRECON
CLUSTER4
N16_NUCLEI_HTTP_CNVD
N17_NUCLEI_HTTP_CVES
N18_NUCLEI_HTTP_DEFAULT_LOGINS
N19_NUCLEI_HTTP_EXPOSED_PANELS
N20_NUCLEI_HTTP_EXPOSURES
N21_NUCLEI_HTTP_MISCONFIGURATION
N22_NUCLEI_HTTP_TECHNOLOGIES
N23_NUCLEI_HTTP_VULNERABILITIES
N24_NUCLEI_JAVASCRIPT
N25_NUCLEI_SSL
N26_NUCLEI_DAST
N27_NUCLEI_HEADLESS
N28_NUCLEI_DNS
CLUSTER5
A01_NIKTO_INTERESTING_FILE
A02_NIKTO_MISCONFIGURATION
A03_NIKTO_INFORMATION_DISCLOSURE
A04_NIKTO_INJECTION
A05_NIKTO_REMOTE_FILE_RETRIEVAL
A06_NIKTO_DENIAL_OF_SERVICE
A07_NIKTO_REMOTE_FILE_RETRIEVAL
A08_NIKTO_COMMAND_EXECUTION
A09_NIKTO_SQL_INJECTION
A10_NIKTO_FILE_UPLOAD
A11_NIKTO_AUTHENTICATION_BYPASS
A12_NIKTO_SOFTWARE_IDENTIFICATION
A13_NIKTO_REMOTE_SOURCE_INCLUSION
A14_NIKTO_WEBSERVICE
A15_NIKTO_ADMINISTRATIVE_CONSOLE
END
FINGERPRINT
END_A
NAABU
NMAP
B01_FINGERPRINT
B02_SHORTSCAN
B03_TRUFFLEHOG
B04_TRIVY

Luigi Task Status

Task List | Dependency Graph | Workers | Resources

Running

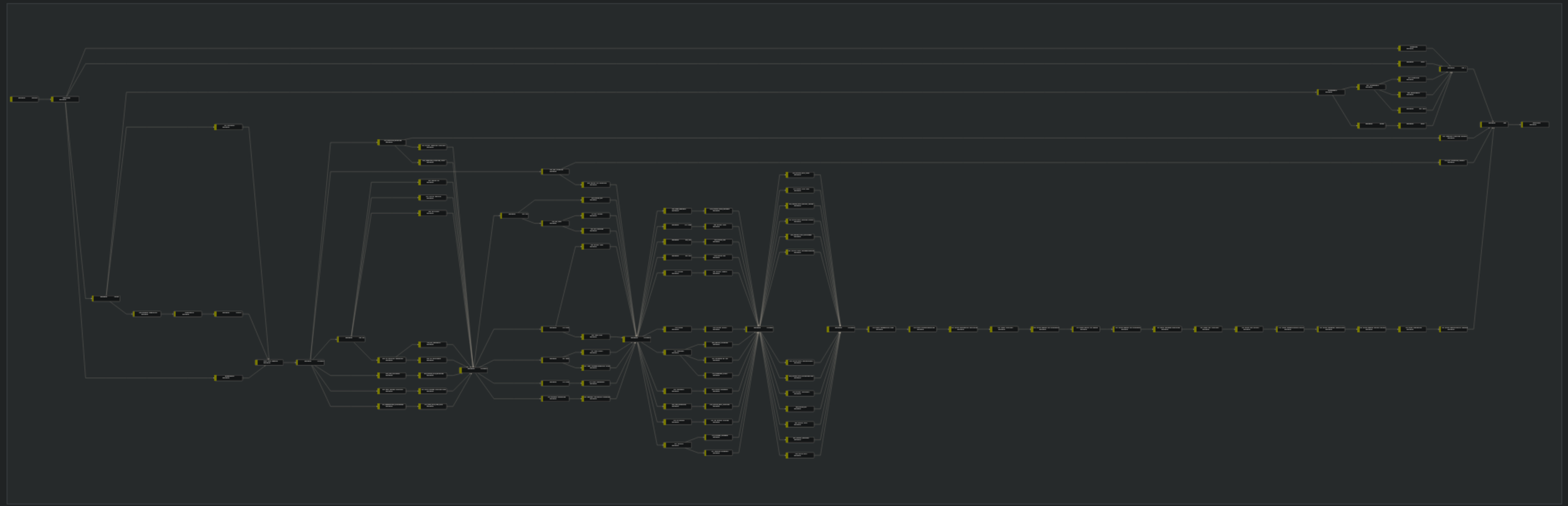
RunAllTasks__home_rafael_PRO__home_ra | Show task details

Show Upstream Dependencies ☐ | Hide Done ☐

Visualisation Type D3 | SVG

[redacted]

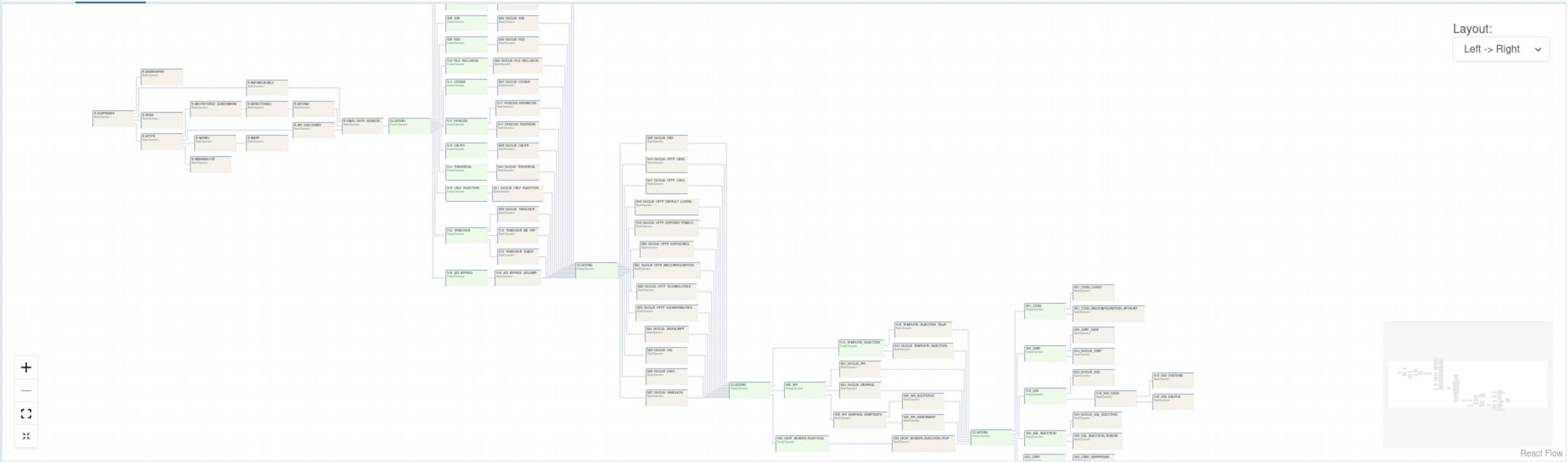
Dependency Graph



DAG
pentesting_dag / Run ▸2024-06-28, 04:13:49 UTC

Clear Mark state as...

Details Graph Gantt Code Audit Log



Let’s work together!

E-MAIL

coelhorafael@proton.me
rafaelcoelho1409@hotmail.com