오픈소스 가드닝

Open Source Gardening

OWASP Seoul Chapter 2025.08 | @hahwul

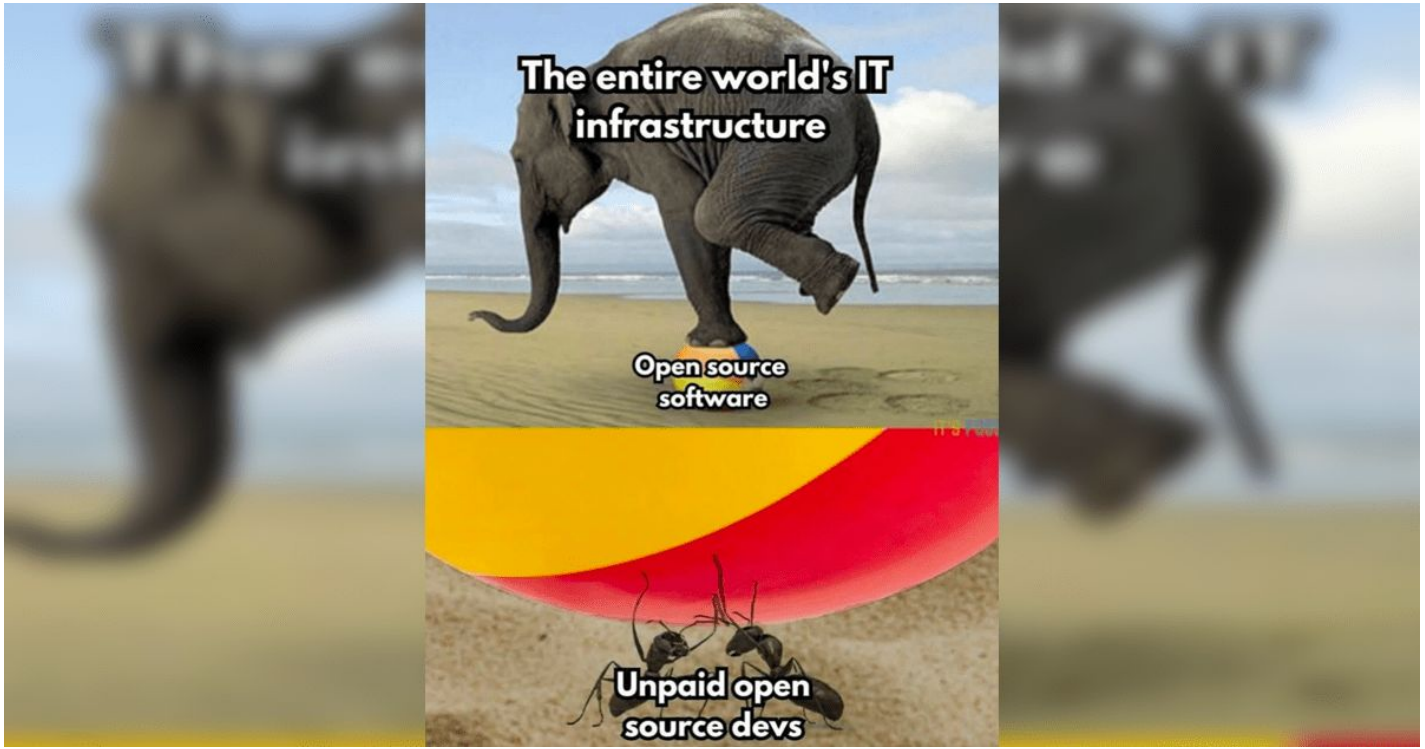
WHO AM I

- HAHWUL (@hahwul)
- Offensive Security Engineer
- Open Source Developer
  - Rust, Ruby, Go and Crystal
- OWASP Noir
  - @owasp-noir
  - h.lee@owasp.org

DALFOX

Linux, Kubernetes,
OpenSSL, Vault,
Git

Open Source Software

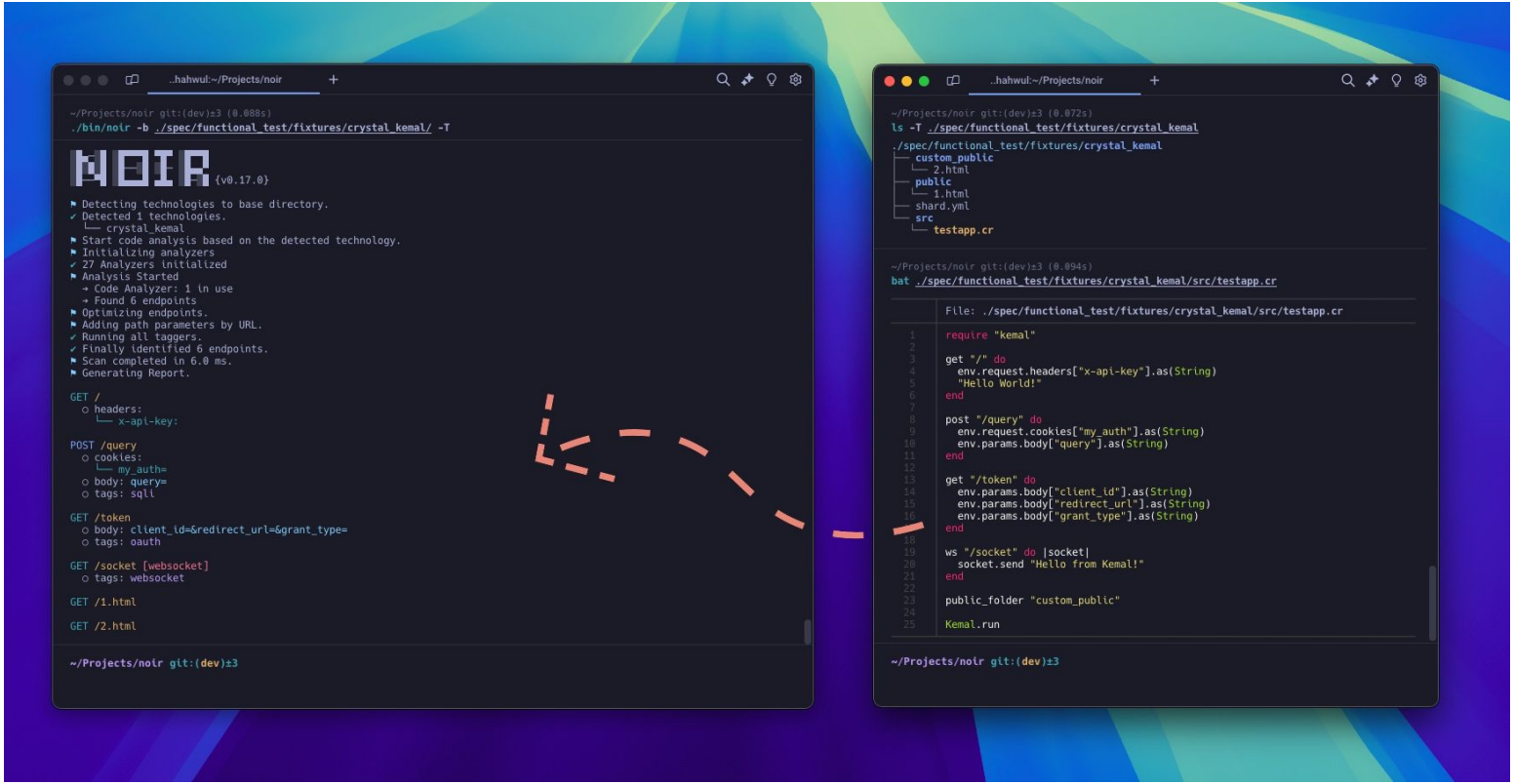


Open Source in Security

오픈소스 기여해보신 적이 있나요?


OWASP NOIR

OWASP Noir


..hahwul:~/Projects/noir
~/Projects/noir git:(dev)±3 (0.088s)
./bin/noir -b ./spec/functional_test/fixtures/crystal_kemal/ -T
NOIR {v0.17.0}
Detecting technologies to base directory.
Detected 1 technologies.
crystal_kemal
Start code analysis based on the detected technology.
Initializing analyzers
27 Analyzers initialized
Analysis Started
Code Analyzer: 1 in use
Found 6 endpoints
Optimizing endpoints.
Adding path parameters by URL.
Running all taggers.
Finally identified 6 endpoints.
Scan completed in 6.0 ms.
Generating Report.
GET /
headers:
x-api-key:
POST /query
cookies:
my_auth=
body: query=
tags: sqli
GET /token
body: client_id=&redirect_url=&grant_type=
tags: oauth
GET /socket [websocket]
tags: websocket
GET /1.html
GET /2.html
~/Projects/noir git:(dev)±3
..hahwul:~/Projects/noir
~/Projects/noir git:(dev)±3 (0.072s)
ls -T ./spec/functional_test/fixtures/crystal_kemal
./spec/functional_test/fixtures/crystal_kemal
custom_public
2.html
public
1.html
shard.yml
src
testapp.cr
~/Projects/noir git:(dev)±3 (0.094s)
bat ./spec/functional_test/fixtures/crystal_kemal/src/testapp.cr
File: ./spec/functional_test/fixtures/crystal_kemal/src/testapp.cr
require "kemal"
get "/" do
env.request.headers["x-api-key"].as(String)
"Hello World!"
end
post "/query" do
env.request.cookies["my_auth"].as(String)
env.params.body["query"].as(String)
end
get "/token" do
env.params.body["client_id"].as(String)
env.params.body["redirect_url"].as(String)
env.params.body["grant_type"].as(String)
end
ws "/socket" do |socket|
socket.send "Hello from Kemal!"
end
public_folder "custom_public"
Kemal.run
~/Projects/noir git:(dev)±3

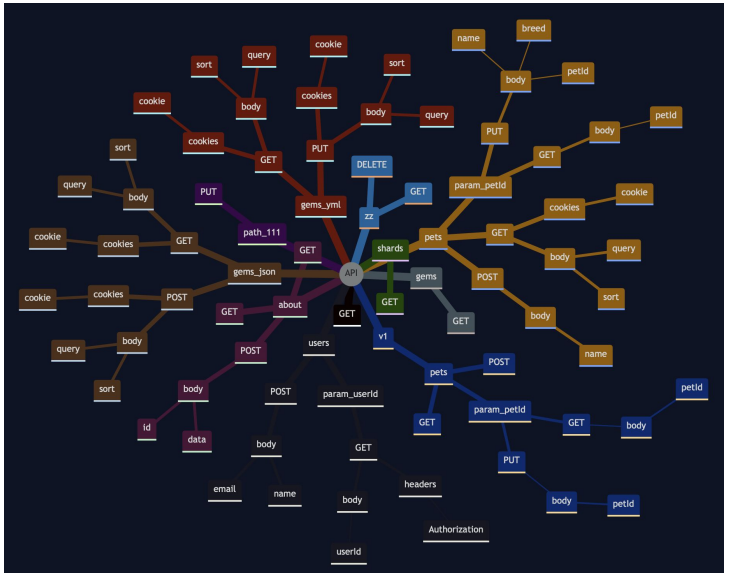
OWASP Noir

- ❏ 소스코드에서 Endpoint (API, Path, Param 등)을 추출
- ❏ For White-box Testing, DevSecOps Pipeline (DAST+)
- ❏ CLI Application
- ❏ Co-lead: @hahwul @ksg97031
- ❏ Crystal, Regex, Tokenizer/Lexer/Parser, LLM

OWASP Noir

- [OWASP Project]
- [GitHub: owasp-noir/noir]

```
GET /favicon.ico

GET /422.html

GET /apple-touch-icon.png

GET /500.html

GET /404.html

GET /apple-touch-icon-precomposed.png

GET /robots.txt

GET /up

★ Passive Results:
[critical][private-key][secret] Detect PRIVATE_KEY
  ├── extract: -----BEGIN PRIVATE KEY-----
  └── file: ./testapp/private_key.pem:1
```

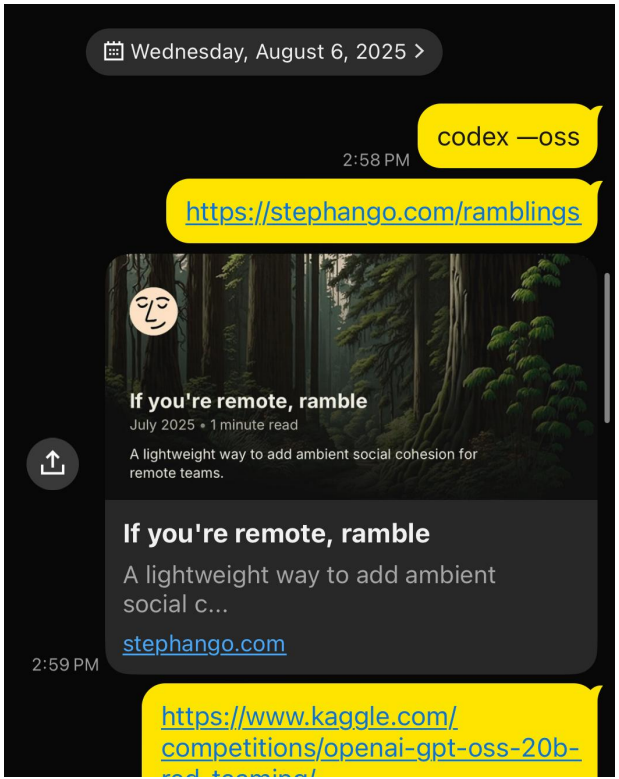


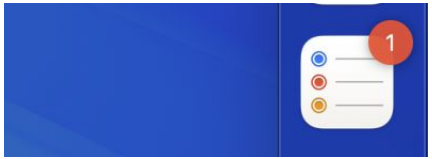
오픈소스 프로젝트를 만들어 보고 싶어!

씨앗 뿌리기

모든 것은 작은 불편함에서 시작되었다.

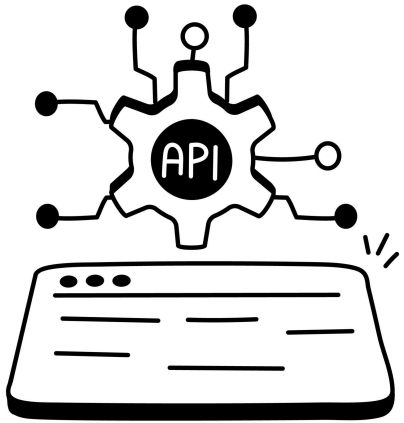
아이디어는 갑자기 찾아온다





Roadmap

- ❑ 아이디어의 구체화
- ❑ 소스코드 수명
- ❑ Simple is Best

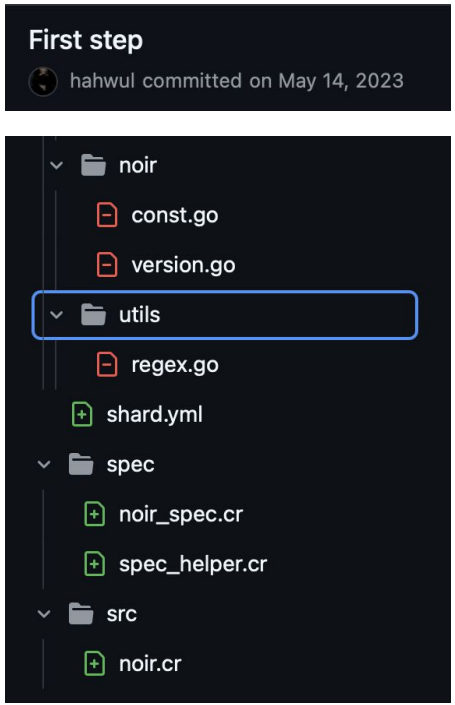


White-box testing

Shadow API

Prototyping model

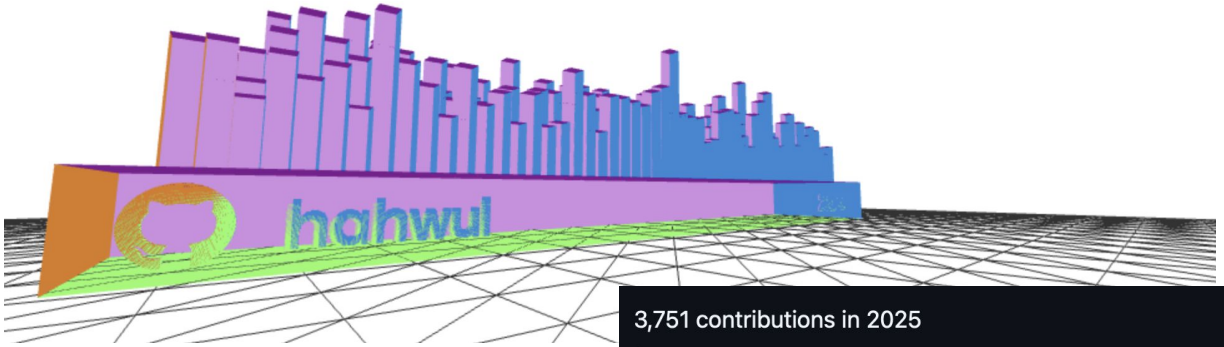
- ❏ 피드백 중심 모델
- ❏ 가능성 시험의 구간
- ❏ Noir에선 Golang으로 프로토타입, Crystal로 실제 개발

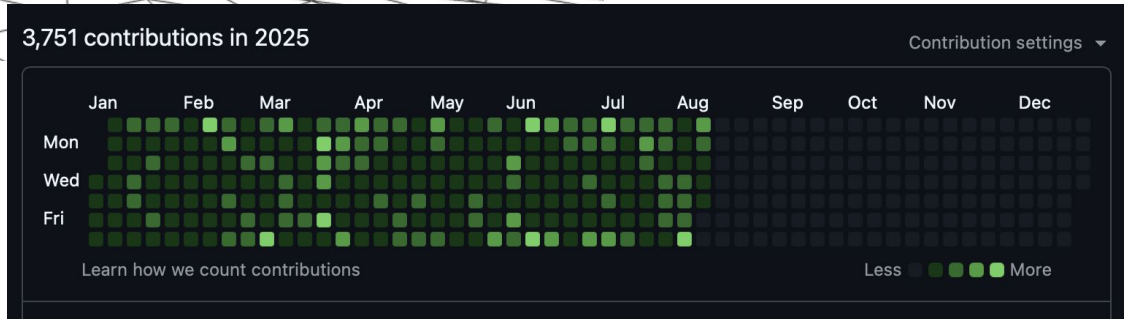


싹 틔우기

지속적인 관심과 개발, 글작성이 필요합니다.

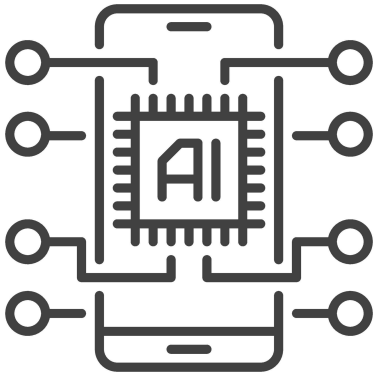
Dev


hahwul


3,751 contributions in 2025
Contribution settings
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Mon
Wed
Fri
Learn how we count contributions
Less
More

Dev with AI

AGENTS.md



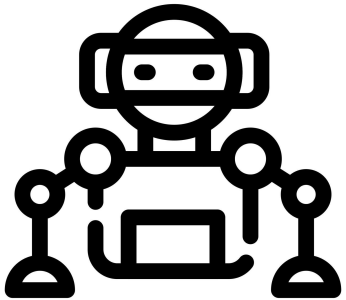
Tools

Goal

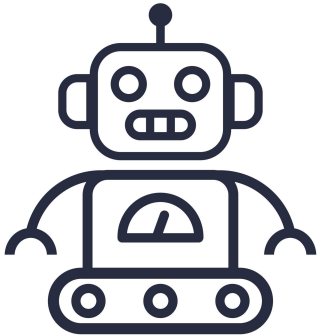
Task

Prompt < Context

AI Team



Research



Coding Agent

IDE

이정도면 괜찮을까?

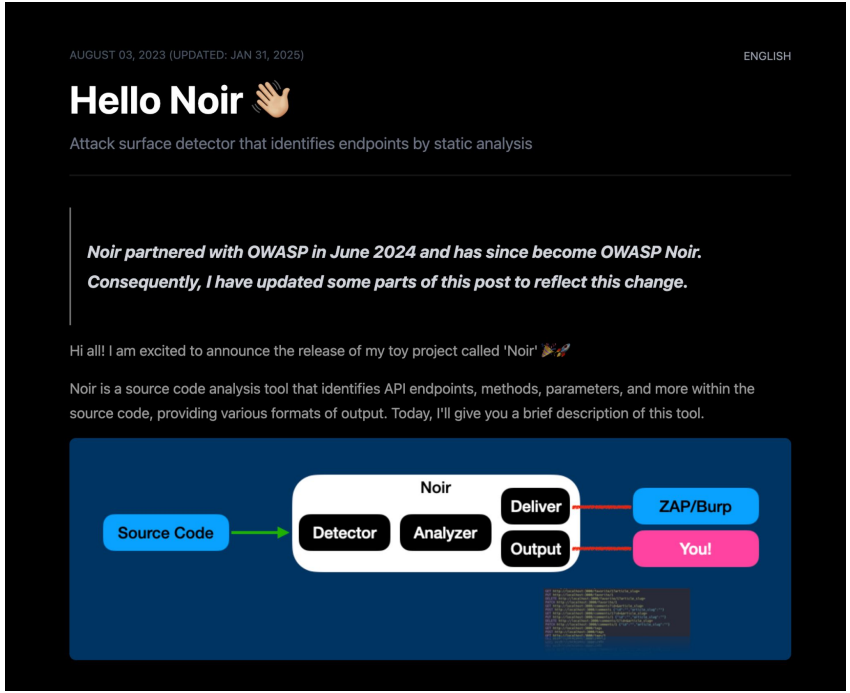
First Release

```
grep "RequestMapping" *
rg "GetMapping"
```

Dogfooding은 필수

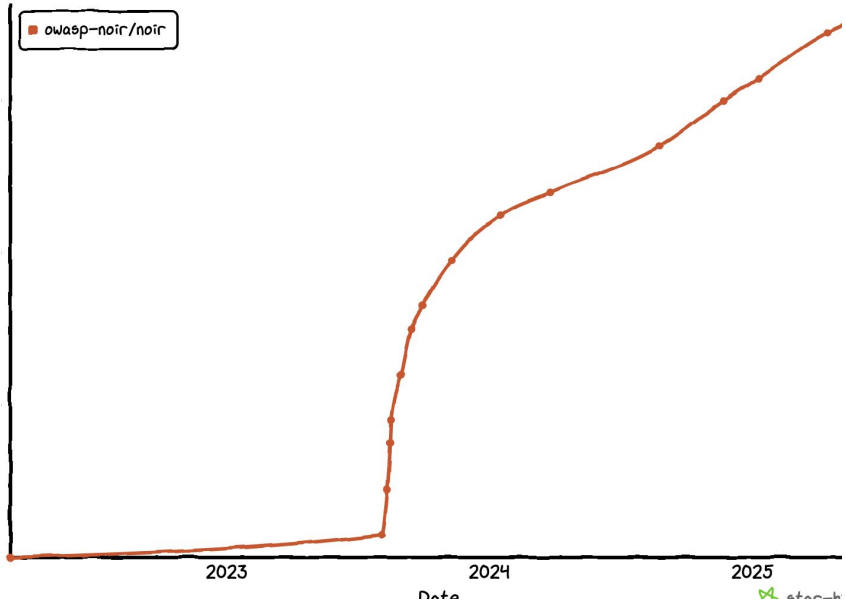
Community Building

- ❑ Social network (e.g. 𝕏, Thread, ETC)
- ❑ Github Discussions, Discord
- ❑ Kitploit
- ❑ Awesome Series
- ❑ Blog Post

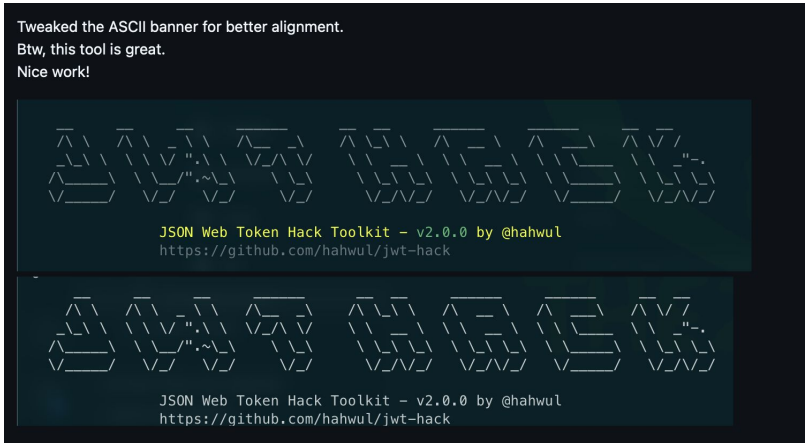


생각보다 큰 효과

- ❏ 𝕏 & Blog 공개 이후 빠르게 향상
- ❏ 비례하여 커뮤니티 관심도도 높아짐
- ❏ 버그/이슈 제보 수도 같이 상승



기억에 남는 Pull Request

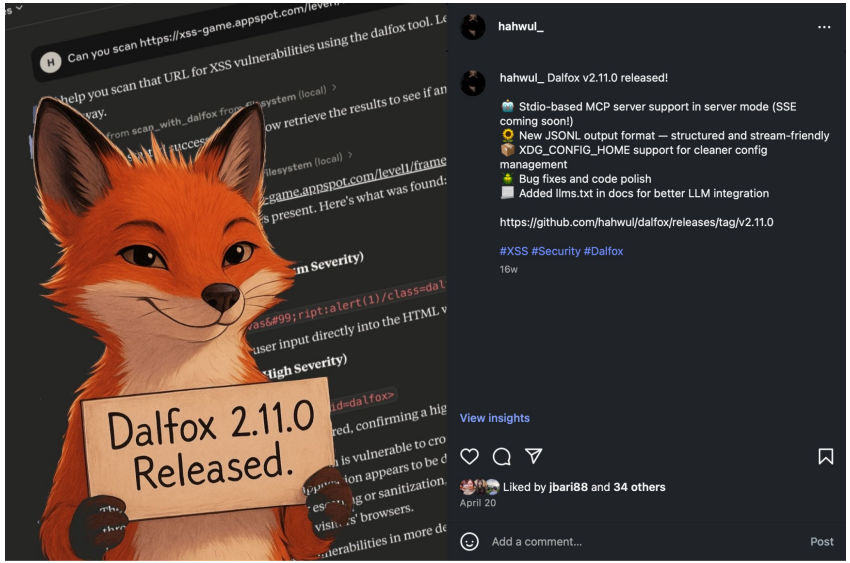


TIP: Github Issue to Pull Request

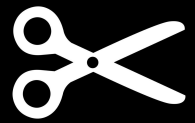
- ❏ 이슈를 제보 받기만 보단 PR로 바꿀 수 있는 것도 중요
- ❏ 점차 Contributor를 늘려나갈 수 있는 방법

TIP: Only Text? Image & Video!

- ❏ 릴리즈를 알리는 행위는 중요
- ❏ 텍스트 보단 이미지, 영상이 흥미를 유발
- ❏ GenAI 이후 쉬워진 작업



힘들다



가지치기

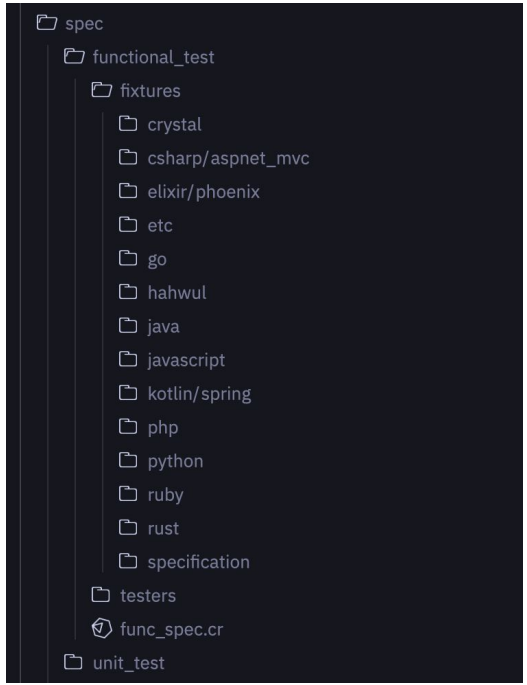
건강한 성장을 위해선 가지를 쳐야합니다.

OWASP, Co-lead

- OWASP Project
- Co-lead

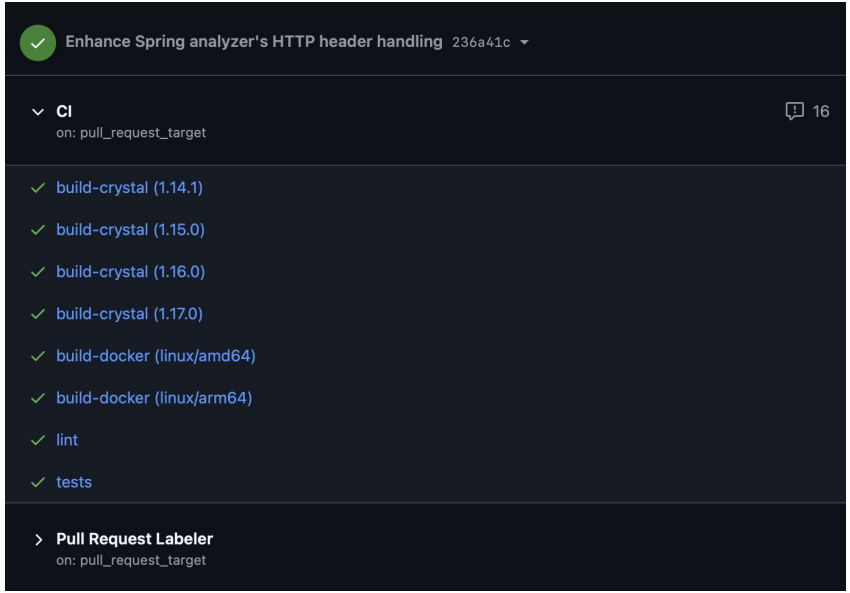
TDD(Test-Driven Development)

- ❏ 소스코드 품질을 위해서 중요
- ❏ 버그를 줄이고 성능을 개선하는데 긍정적 효과
- ❏ AI IDE/Agent 협업 시 필수
- ❏ Noir에선 Unit Test와 Functional Test 모두 수행



Automation (CI/CD)

- ❑ Build & Test
- ❑ Coding Convention
- ❑ Release
  - ❑ Homebrew
  - ❑ Docker Hub
  - ❑ GHCR
  - ❑ Snapcraft
  - ❑ Etc
- ❑ Contributions
  - ❑ 안내서
  - ❑ 체크리스트



개발자도 사람입니다. 휴식과 관리가 필요해요.

TIP: Spammer는 무시

- ❏ 생각보다 오픈소스에 대한 Spam은 많아요.
- ❏ Mail, Github Issue, Discussions
- ❏ 무시하는게 좋아요.

열매 맺기

Collaboration

Homebrew/homebrew-core

noir 0.11.0

bump-formula-pr · CI-published-bottle-commits

hahwul · 5 · Opened on Dec 7, 2023 · #156590

Homebrew/homebrew-core

noir 0.10.0 (new formula)

!-- Use [x] to mark item done, or just click the checkboxes with device pointer -- - [x] Have you followed the guidelines for contributing? - [x] Have you ensured that your commits follow the commit ...

CI-published-bottle-commits · new formula · outdated

p-linnane · 1 · Opened on Nov 8, 2023 · #153592

19

Hacker tools

Dalfox - XSS Scanning Made Easy

TOOL AUTHOR hahwul

CURATED BY INTIGRITI

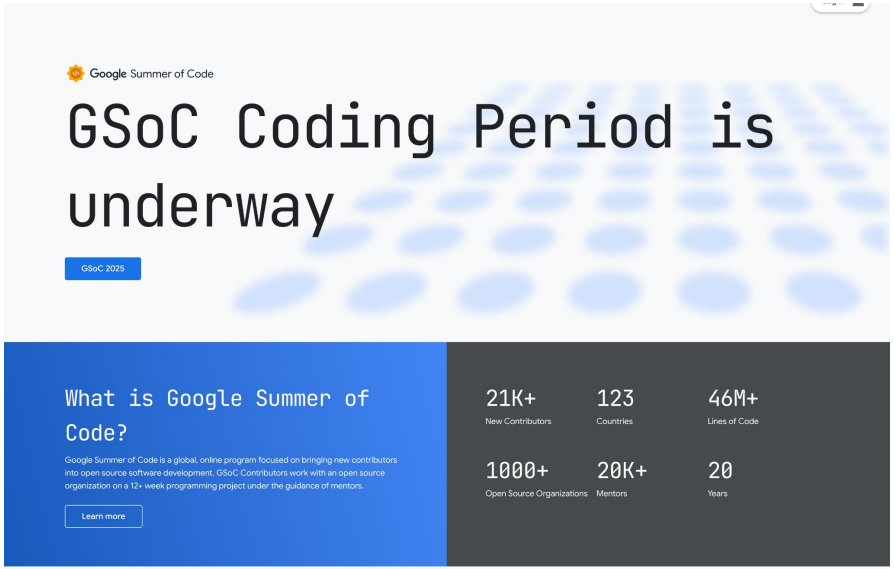
Dalfox – Hacker Tools: XSS Scanning Made Easy

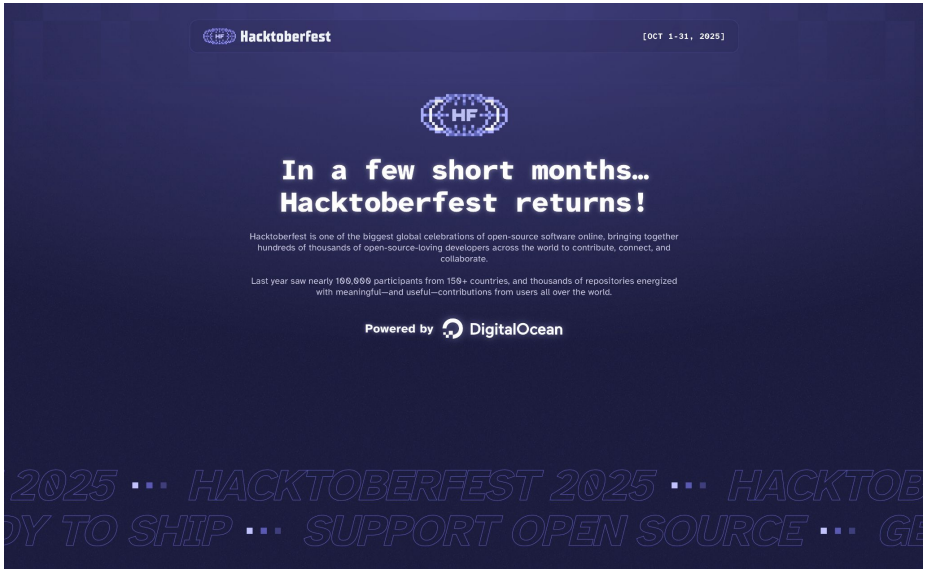
HACKING TOOLS · SEPTEMBER 14, 2021

Finding XSS can sometimes be a repetitive and laborious task. Many attempts at automating the process have been made, yet very little actually come close to gettin...

Continue reading →

개발자 이벤트


Google Summer of Code
GSoC Coding Period is underway
GSoC 2025
What is Google Summer of Code?
Google Summer of Code is a global, online program focused on bringing new contributors into open source software development. GSoC Contributors work with an open source organization on a 12+ week programming project under the guidance of mentors.
Learn more
21K+
New Contributors
123
Countries
46M+
Lines of Code
1000+
Open Source Organizations
20K+
Mentors
20
Years


Hacktoberfest
[OCT 1-31, 2025]
In a few short months…
Hacktoberfest returns!
Hacktoberfest is one of the biggest global celebrations of open-source software online, bringing together hundreds of thousands of open-source-loving developers across the world to contribute, connect, and collaborate.
Last year saw nearly 169,999 participants from 159+ countries, and thousands of repositories energized with meaningful—and useful—contributions from users all over the world.
Powered by DigitalOcean
2025 HACKTOBERFEST 2025 HACKTOB
SUPPORT OPEN SOURCE

Open Source Developer

재정지원

I'll treat you to a coffee.

open collective

정원 가꾸기

오픈소스는 마라톤

Contributors

Fixed Typo

Code

Documentation

Idea

Bug Report

AI는 좋은 협업자

Echo System

Bug Bounty

Offensive Security

Programming

Documentation

CLI Application

Web Application

DevSecOps

A Fellow Farmer's Message

As an individual it's hard to make a significant contribution to security, even if you work at a security vendor. The one exception is Open Source.

Anyone can get involved in Open Source, and Open Source is used everywhere!

ZAP is the world's most popular web scanner, and as a community project we encourage people to get involved.

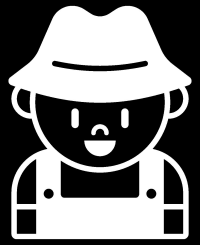
Everyone on the ZAP Core Team has had (and accepted) job offers thanks to their ZAP contributions, so not only can you make the online world a slightly safer place, you can also boost your career! If you'd like to get involved in ZAP then see https://zaproxy.org/docs/contribute/

Simon Bennetts의 메시지 (ZAP Project Leader)

Just do it!

초보자를 위한 첫걸음

- ❏ 자주 사용하는 도구, 문서의 Repository 살펴보기
- ❏ 'Good First Issue' 로 찾아보기
- ❏ 간단한 오탈자 수정 > PR 보내기



씨앗 뿌릴 준비 되셨나요?