deti universidade de aveiro
departamento de eletrónica, telecomunicações e informática

Individual **Portfolio**

Security in Software Engineering

Luana Carolina Reis | nº 131193

Six tasks,
One playbook

One throughline: shift-left where you can, detect at runtime where you must, and never trust by default.

SAST + DAST

build-time and run-time scanning

API Security

a working honeypot, probed live

Pentest

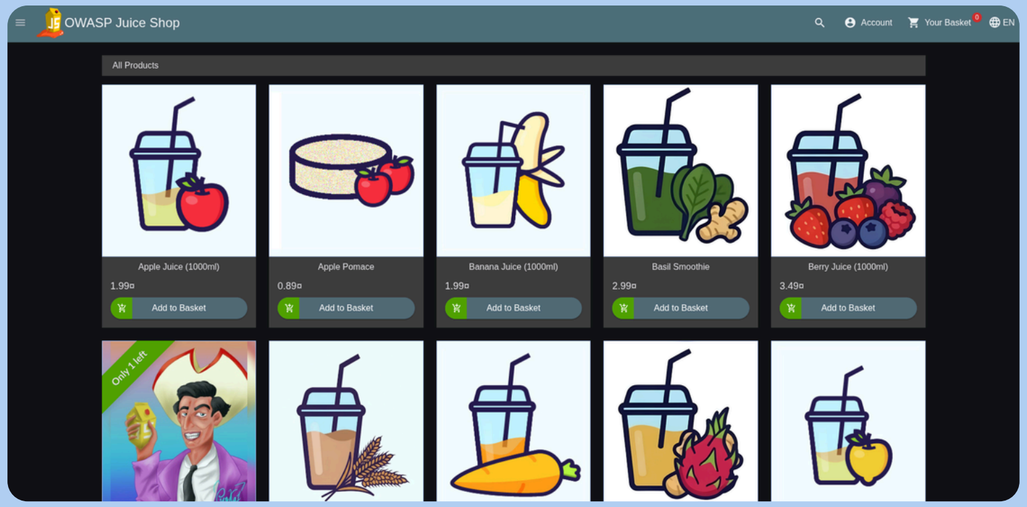
automated recon before manual testing

Seminar

AI-driven threats meet course concepts

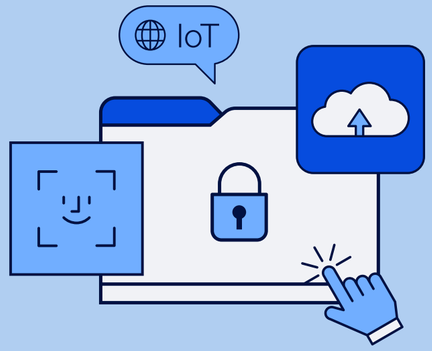
Zero Trust

how GenAI reshapes ZTA



Validated on **OWASP Juice Shop** + a custom Shadow API.

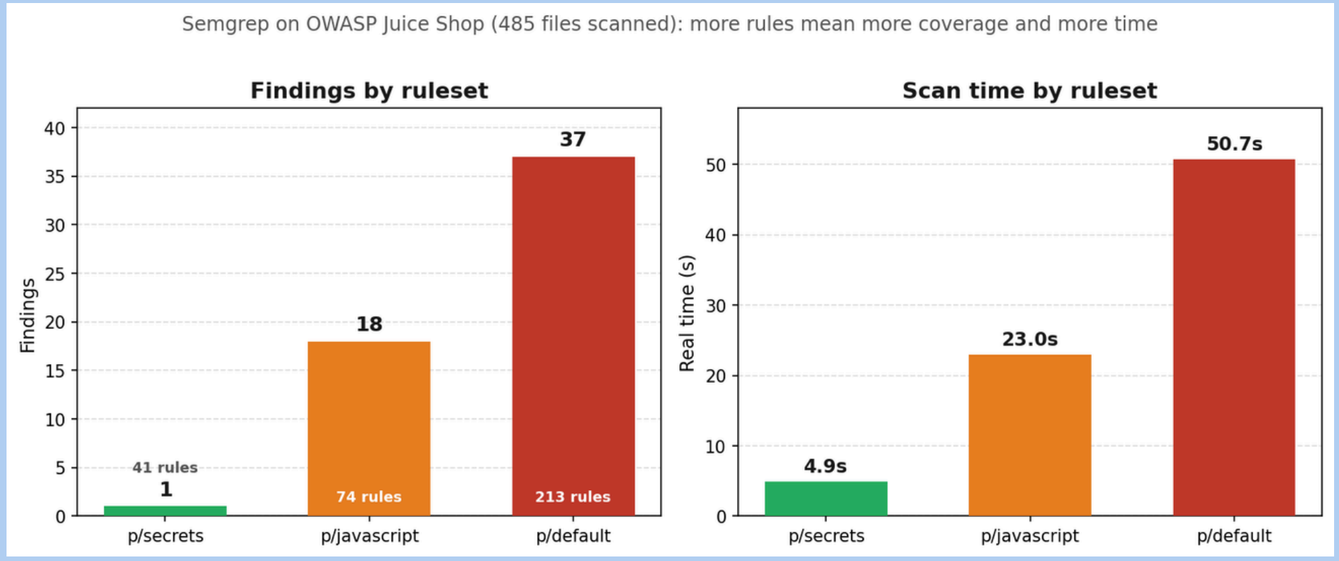
01 · SAST
shift-left scanning



5 stages, fast to deep:

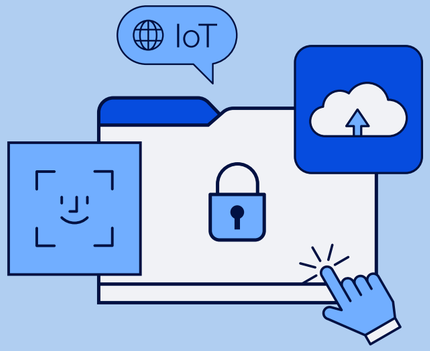
> IDE **SonarLint** live
> commit **Semgrep** blocks critical
> PR **Semgrep + SonarCloud**
> nightly **Bandit** deep

Key idea
No single scanner wins. Match the tool to when it runs and how deep it must go.

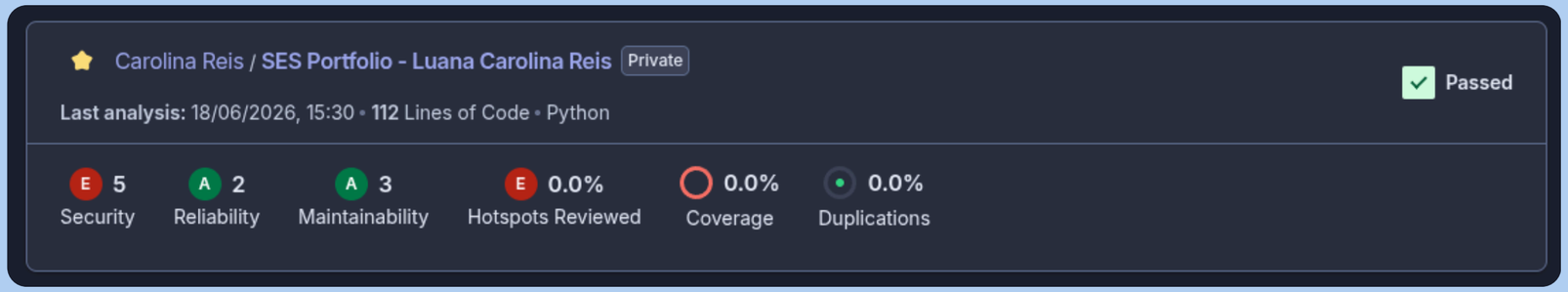


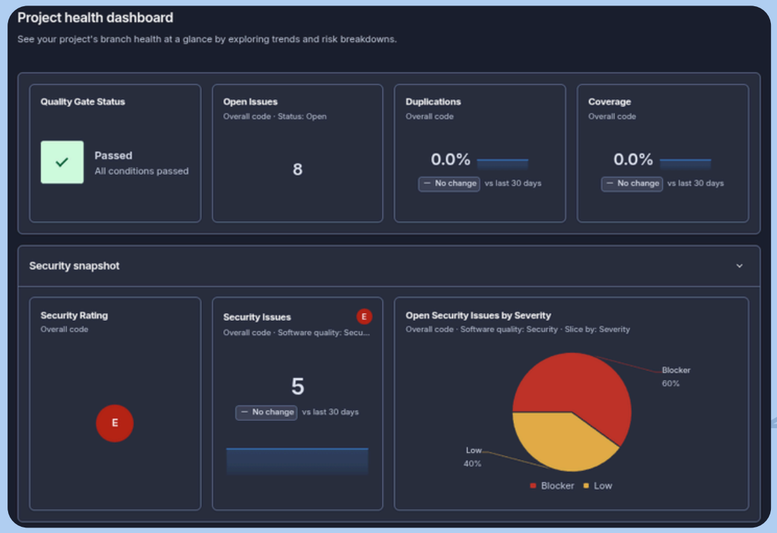
Measured & reproduced on Juice Shop (485 files)

01 · SAST
the Quality Gate passes



Every push and pull request sends results to **SonarCloud**, a live dashboard tracking security, reliability and maintainability. The project **passes its Quality Gate**.

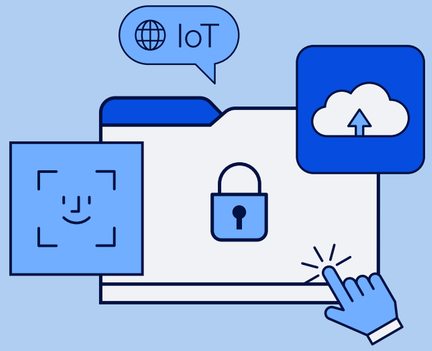




Honest reading

Reliability and Maintainability are A. The Security E is a single hotspot, disabled CSRF, which is a documented false positive: CSRF does not apply to a Bearer-token API with no auth cookies.

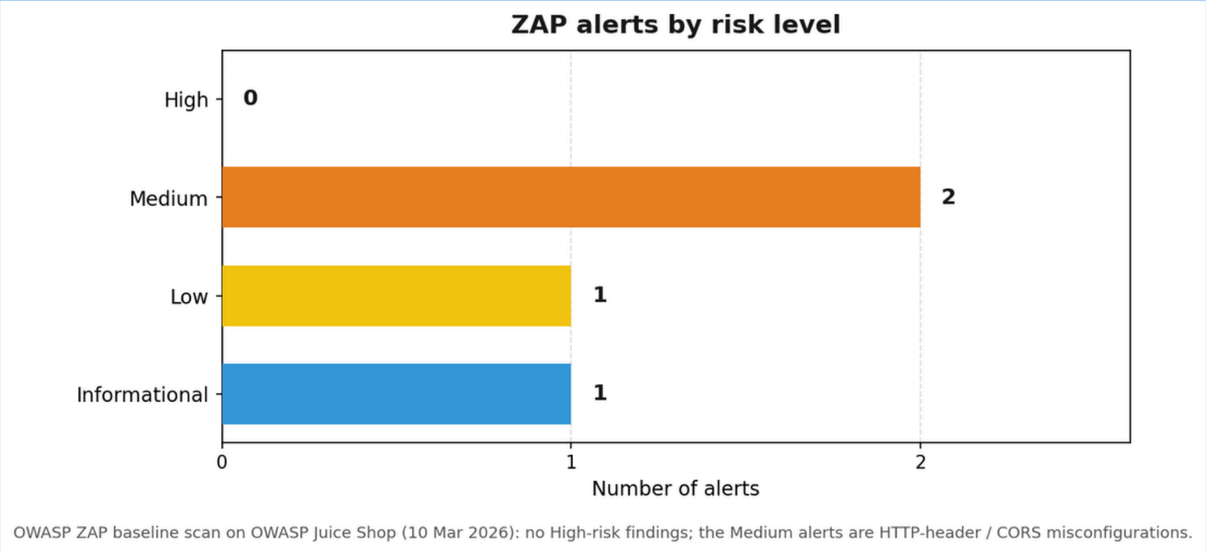
02 · DAST
run-time scanning with ZAP



3 execution moments:

> smoke scan post-deploy
> **PR gate** blocks merge
> scheduled deep scan

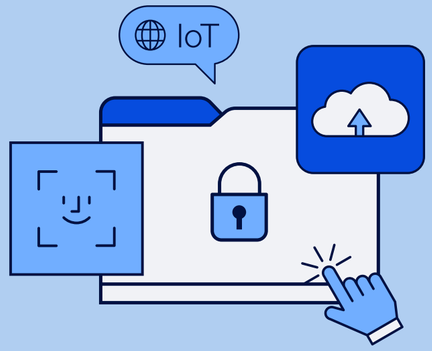
Authenticated by design
OIDC login to token to authenticated context; logout excluded to keep the session alive.



OWASP ZAP on Juice Shop (10 Mar 2026)

Real ZAP scan: **0 High**, 2 Medium, 1 Low.

03 · Pentest
automated reconnaissance

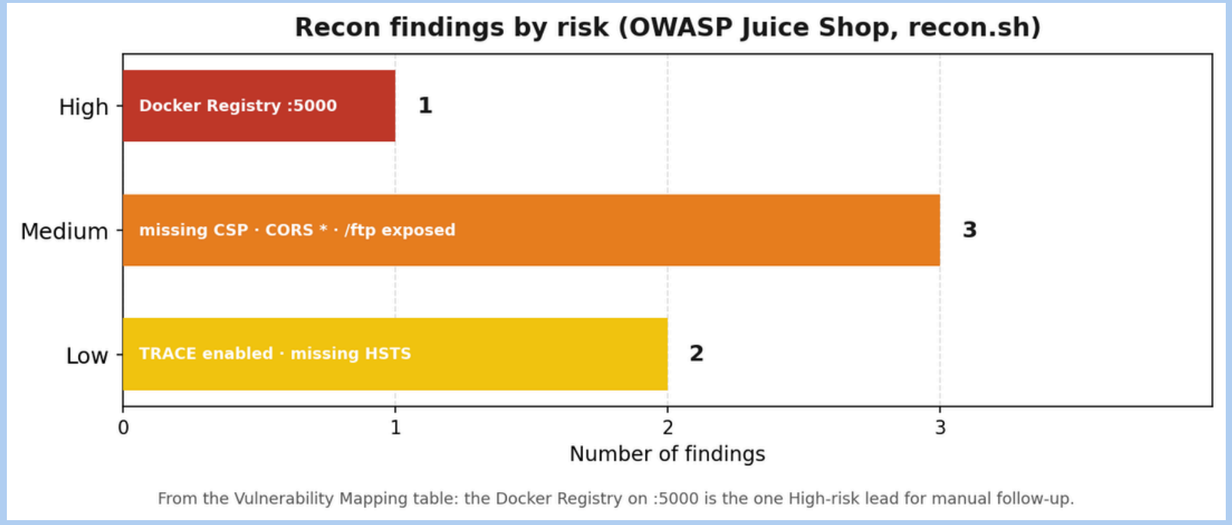


recon.sh automates the repetitive PTES phases:

> dig, nmap, curl, gobuster
> one report folder per run

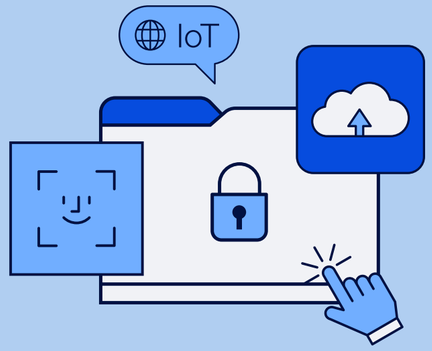
From signal to attack path
port 5000 to Docker Registry: a High-risk lead. robots.txt to /ftp: directory exposed.

Report generated & verified on Juice Shop.

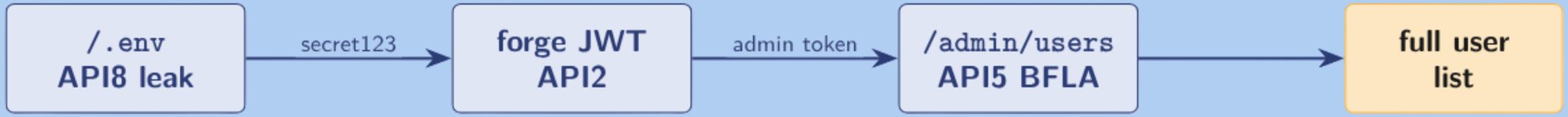


Recon findings by risk

04 · API Security
the Shadow API honeypot



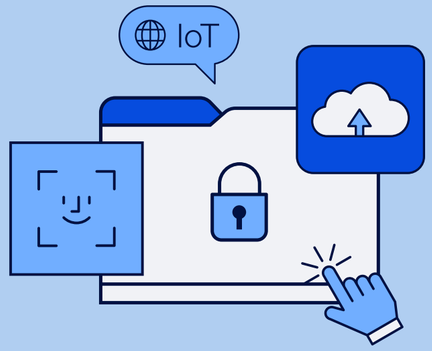
A deliberately vulnerable API that looks irresistible and logs every probe. Five OWASP API Top 10 flaws, probed live.



The chained attack

No login needed: one leaked secret signs every token, so a config leak collapses the whole auth model. Every request becomes a high-confidence detection event.

05 · IDN Youth Seminar **critical reflection**



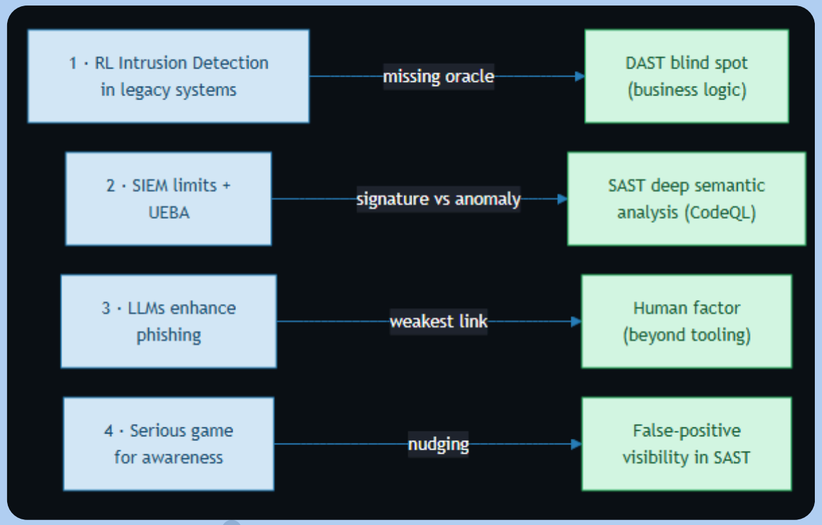
Panel 1 thread: **static, rule-based tools fail against AI-accelerated threats**. The answer is not to replace them, but to add an adaptive layer.

Shift-left
SAST

Runtime
DAST ▪ UEBA

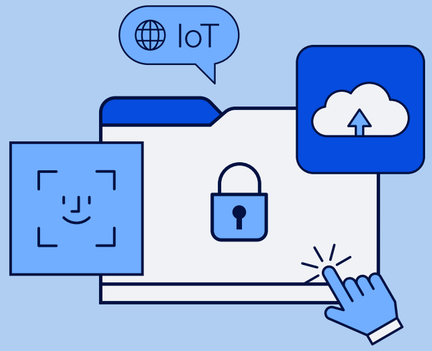
Human factor
training ▪ nudging

Defence in depth: the three layers are complementary, not alternatives.



Takeaway
No single tool is enough. The course gives the vocabulary to layer static analysis, runtime detection and human awareness.

06 · Zero Trust & GenAI



Question: what new attack surfaces does GenAI add, and how does ZTA respond?

New surfaces (OWASP LLM Top 10)

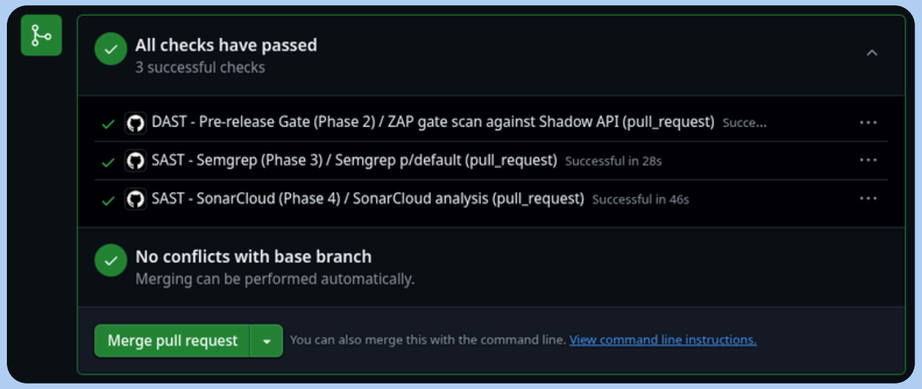
> Prompt injection (LLM01)
> Data / model exfiltration (LLM02)
> RAG leakage (LLM08)

ZTA response:

> model & tools = new PEPs
> retrieval filtered by user identity
> I/O guardrails + least privilege

Zero Trust Access in AI & LLM Systems

Bottom line
GenAI does not invalidate Zero Trust, it validates it: assume breach was always the point. NIST SP 800-207 + OWASP LLM Top 10.



On a pull request: DAST gate + SAST checks, all green

The portfolio is active **CI/CD workflows**

Five GitHub Actions workflows run on every push and pull request. They are not just documented, they run.

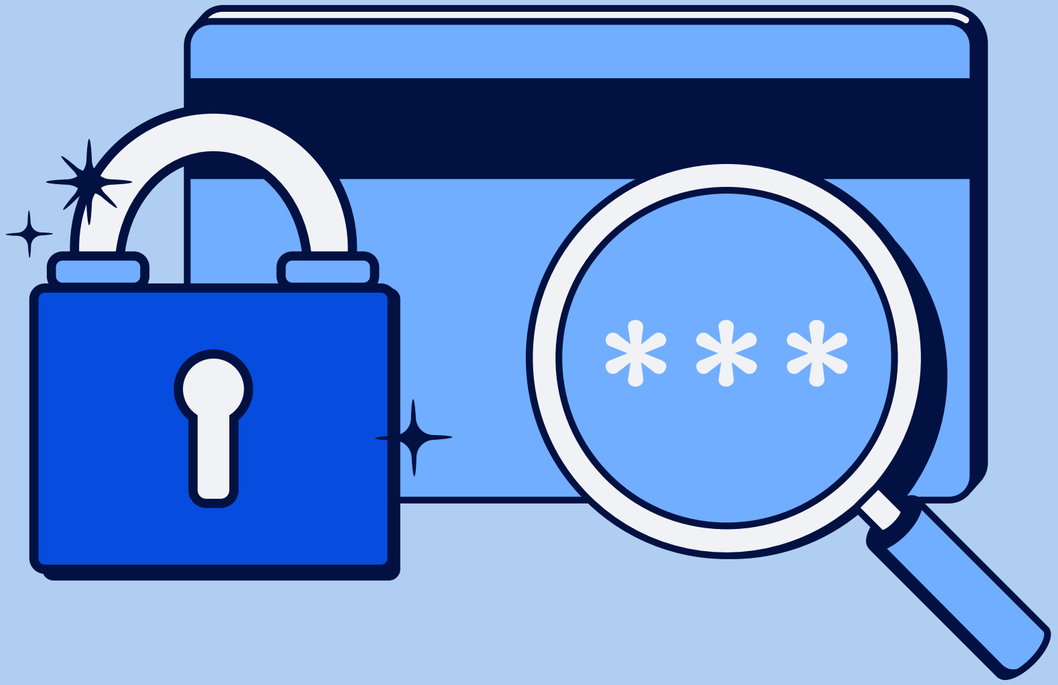
On a push to master: SAST suite + scheduled ZAP scan

deti universidade de aveiro
departamento de eletrónica, telecomunicações e informática

Thank You

Shift-left. Detect at runtime. Assume breach.

Six tasks, one defence-in-depth mindset.



University of Aveiro

Security in Software Engineering

2025/2026 | 18 June 2026