

Gabo Rodriguez

role Application Security · DevSecOps · Pentesting · AI Security
location Buenos Aires, AR
github  GitHub (<https://github.com/y3rb1t4>)
linkedin  LinkedIn (<https://www.linkedin.com/in/grodriguezsec/>)

Application security and DevSecOps engineer with a pentester's background. I build security into the delivery pipeline — threat modeling, SAST and DAST, secure SDLC — and I have spent years on the offensive side, testing web, mobile and cloud targets. On the cloud side I work with IAM across AWS and Azure, leaning on short-lived credentials instead of static secrets so access stays auditable.

Most recently I have been working on the security of AI agent systems: colmena, my open-source trust firewall, applies deterministic per-agent policy to every tool call a coding agent makes, with no model in the hot path.

EXPERIENCE

Senior Application Security Engineer @ Cashea 2026-02 — present

AppSec Research Engineer @ Baufest 2025-05 — 2026-02

- Drove application security initiatives across multiple product teams.
- Ran security assessments covering SAST, DAST, and mobile and cloud evaluations.
- Designed secure SDLC practices, integrating security tooling into CI/CD pipelines.

Senior Application Security Analyst @ ITTI Digital 2023-10 — 2025-04

HTB Ambassador, Argentina @ Hack The Box 2024-02 — 2025-04

Community role: ran and supported the Argentine Hack The Box community.

Security Consultant — Application Security @ IBM 2022-06 — 2023-12

Cloud security advocate at the Cybersecurity CoE, on the Banco Supervielle account.

Pentester @ Just Mobile Security 2022-05 — 2023-10

Red Team @ Xelere 2022-03 — 2022-06

ETL Developer @ Charles Taylor 2021-08 — 2022-06

Virtual Learning Tutor @ Argentina Programa 2021-09 — 2023-01

Design engineer and site supervisor @ Electrical engineering

2010-06 — 2021-09

Eleven years in electrical and thermomechanical engineering before moving into security — UTN Buenos Aires (scholarship holder and electrical designer), Galileo Technologies, Planeta Frío and Brignone. Design, budgeting and on-site supervision.

SKILLS

application security	Threat modeling · SAST · DAST · Secure SDLC · Web application security · Mobile security · Secure code review
devsecops	CI/CD pipeline security · Automated security gates · Policy as code · Infrastructure as Code · Secrets management · GitLab
offensive security	Penetration testing · Red team · Web and API pentesting · Mobile pentesting · Cloud pentesting
ai security	AI agent governance · LLM tool-call policy enforcement · Prompt injection defense · Multi-agent trust boundaries · MCP · Threat modeling for AI systems
cloud & iam	AWS IAM · Azure · STS / short-lived credentials · Least privilege · IAM maturity models
languages	Rust · Python · Bash · TypeScript

CERTIFICATIONS

GitLab DevSecOps Sales Specialty — GitLab
DevSecOps Essentials
Blockchain Essentials

EDUCATION

Engineering degree — Electrical Engineering — Universidad Tecnológica Nacional
2011-01 — 2020-07

LANGUAGES

spanish	Native
english	Professional working proficiency (B2)
german	Elementary