Cristian Vargas

Offensive Application Security Engineer · Fluid Attacks · Remote, Colombia

Finding vulnerabilities in software people depend on, like NestJS, Fastify, DOMPurify and Ghost.

cvargas.com · https://www.linkedin.com/in/cvmiracle

DISCLOSED VULNERABILITIES · 11 ENTRIES

ID	PRODUCT	DEFECT	SEVERITY	DISCLOSED
CVE-2025-10655	Frappe Helpdesk 1.14.0	SQL injection (get_dashboard_data filters.team)	High 8.6	2025-12-09
CVE-2026-2293	NestJS 11.1.13 (fixed 11.1.14)	Auth/authz bypass via path normalization (lack of data validation)	High 8.2	2026-02-27
CVE-2026-2880	@fastify/middie 9.1.0 (fixed 9.2.0)	Improper path normalization (middleware bypass)	High 8.2	2026-02-27
CVE-2025-11461	Frappe CRM 1.53.1 (fixed 1.54.0)	SQL injection (multiple, dashboard controller)	High 7.1	2025-11-26
CVE-2025-10692	OpenSupports 4.11.0	SQL injection (staff get-new-tickets)	High 7.1	2025-10-03
CVE-2025-10696	OpenSupports 4.11.0	IDOR (supervised list, cross-user ticket disclosure)	High 7.1	2025-10-03
CVE-2025-10695	OpenSupports 4.11.0	Unauthenticated SSRF (test-imap/test-smtp)	Medium 6.9	2025-10-03
CVE-2025-9960	is-localhost-ip 2.0.0	SSRF via restrictions bypass	Medium 6.9	2025-09-22
CVE-2025-9862	Ghost 6.0.6 (5.99.0–5.130.3, 6.0.0–6.0.8; fixed 5.130.4/6.0.9)	SSRF via oEmbed bookmark	Medium 6.1	2025-09-17
CVE-2026-0540 co-found	DOMPurify 3.1.3–3.3.1 (fixed 3.3.2)	DOM-based XSS (mXSS via re-contextualization)	Medium 5.3	2026-03-24
CVE-2025-15056	Quill 2.0.3	XSS in HTML export (formula/video formats)	Medium 5.1	2026-01-13

COMPETITION RECORD

- **1st · OAS Cyber Americas Cup** — 2026 · with Fluid Attacks
- **1st · Kaspersky CTF — NA/SA/Caribbean** — 2026 · qualified SAS CTF final, Bali · Fluid Attacks
- **1st · Ekoparty CTF ×2** — 2025–2026 · consecutive · Fluid Attacks
- **1st · DragonJAR CTF** — 2025
- **2nd · DragonJAR CTF** — 2026
- **Fluid Attacks CTF: Hall of Fame #1 · 1st Ed.1 · 2nd Ed.2** — LATAM Challenge · individual · cvargas

CERTIFICATIONS

- **OSWE** — OffSec Web Expert (2024)
- **CWEE** — HTB Certified Web Exploitation Expert (2025)
- **BSCP** — Burp Suite Certified Practitioner (2023)
- **C-AI/MLPen** — Certified AI/ML Pentester (2025)
- **PWPE** — Practical Web Pentest Expert (2025)
- **ACP** — ACP Exam Passed (2025)
- **CRB** — Code Review Badge (2024)
- **CSWAE** — C)SWAE: Certified Secure Web Application Engineer (2024)
- **CAPenX** — Certified AppSec Pentesting eXpert (2024)
- **CCSP-AWS** — Certified Cloud Security Practitioner–AWS (2023)
- **CASA** — Certified API Security Analyst (2023)
- **CAP** — Certified AppSec Practitioner (2023)
- **eMAPT** — eLearnSecurity Mobile Application Penetration Tester (2023)
- **C-AgAIPen** — Certified Agentic AI Pentester ()
- **C-APIPEN** — Certified API Pentester ()

TALKS

- Codex aplicado al AppSec — Fluid Attacks · Meetup LATAM (2026) https://www.youtube.com/watch?v=qyf-AlgEy20
- Cómo obtener CAPenX — Fluid Attacks · Meetup LATAM (ES) https://www.youtube.com/watch?v=qYCFkj0RoNQ
- Cómo obtener la certificación HTB CWEE — Fluid Attacks · Meetup Agosto (ES) https://www.youtube.com/watch?v=pTnKeSemuGE

WRITING

- HTTP Verb Tampering in NestJS: Bypassing Middleware with HEAD Requests (2026) cvargas.com/blog/http-verb-tampering-nestjs/
- How Windsurf and Cursor help with secure code review (2025) cvargas.com/blog/windsurf-cursor-secure-code-review/
- CWEE or OSWE — which one to choose? (2025) cvargas.com/blog/cwee-or-oswe/

SKILLS · SELF-ASSESSED, 1–10

Web 8/10 (11 CVEs · OSWE · CWEE · BSCP) · Mobile 8/10 (eMAPT) · Research 7/10 (Fluid Attacks advisories) · AI 9/10 (C-AI/MLPen · C-AgAIPen · Talk: Codex aplicado al AppSec) · Cloud 7/10 (CCSP-AWS) · Binary Exploitation 3/10 · Crypto 2/10