

Lucas Valbuena

León, Spain | lucasvalbuena@pm.me | linkedin.com/in/lucknite | github.com/x1xhlol | +34 648 139 101

Experience

Orchid AI (Y Combinator P25) | Remote

Jul 2026 - Present

AI Agent & Product Intern

- Contribute to the Orchid platform and agent, fixing product issues and improving capabilities, features, and behavior
- Improve onboarding and product workflows to make the agent easier and more reliable to use

Projects

ZeroLeaks

Mar 2025 - Present

Founder & Lead Developer — Open-Source AI Security Scanner

github.com/ZeroLeaks/zeroleaks

- Built an open-source AI security scanner that tests LLM systems for prompt injection and extraction vulnerabilities using multi-agent architecture and research-backed attack techniques
- Engineered vulnerability assessment pipelines, prompt extraction prevention modules, and IP protection features
- Selected for Y Combinator Summer Fellows (Summer 2026)

System Prompts & Models of AI Tools

Mar 2025 - Present

Creator & Maintainer — Open-Source Research Repository

github.com/x1xhlol/system-prompts-and-models-of-ai-tools

- Extracted and documented system prompts from 30+ AI platforms through security research, building a public repository with 30,000+ lines of annotated documentation
- Achieved 140k+ GitHub stars and 35k+ forks (as of Jun 2026)
- Widely referenced by security researchers and cited in academic literature for exposing prompt injection failure modes and driving industry improvements

Recognition & Awards

- Awarded \$6,000 by OpenAI for contributions to AI safety via the GPT-5 Bio Bounty program (Jan 2026)
- Featured in La Nueva Crónica and other national media for pioneering AI security research

Skills

- Security & AI: LLM red-teaming, prompt injection analysis, agent security, automated vulnerability scanning, multi-agent orchestration
- Development: Python, TypeScript, React, Next.js, Convex, Vercel, CI/CD
- Languages: Spanish (native), English (advanced proficiency)

Education

Colegio Marista San José — León, Spain

Sep 2022 - Present

High School Diploma (expected Jun 2027). Focus: mathematics, computer science, and technology.