Juan Esteban Muñoz Díaz

Application Security Engineer | Security Automation & AppSec Testing

Bogotá, Colombia • +57 305 895 7432 • juan.munoz@naing.co • linkedin.com/in/juaesm

Open to remote (US / international) and Bogotá-based roles

PROFESSIONAL SUMMARY

Application security engineer focused on securing APIs and data paths through automated security testing and CI/CD integration. Currently own the AppSec testing strategy for a U.S. government compliance platform — authentication, authorization, token misuse, and sensitive-data leakage across 1,500+ endpoints. Background in large-scale test automation (Playwright, CI/CD) plus deep offensive-security and Linux-internals research, bringing an attacker's mindset to building security guardrails developers actually use. M.S. in Information Security; eJPT-certified; fluent English (C1).

PROFESSIONAL EXPERIENCE

Application Security / Security QA Engineer 2026 – Present

B2Gnow (via Insight Global) — Phoenix, AZ, USA *Remote*

Data-path and sensitive-data security for eComply, a U.S. government compliance platform (legacy ASP.NET MVC).

- Mapped system architecture and data flows across **1,500+ endpoints** to build the platform's first inventory of sensitive-data entry points and risk exposure — from a codebase with near-zero documentation.
- Designed an **automated authorization-sweep** approach to validate access control (IDOR, privilege escalation, broken authZ) at scale, surfacing the highest-impact OWASP risks across all endpoints rather than one at a time.
- Built automated security test suites for critical data paths and integrated them into **CI/CD pipelines**, enabling continuous validation of authentication, authorization, and session-management controls.
- Performed negative security testing to confirm no sensitive data leaks through logs, API responses, or error messages; tracked and prioritized findings by risk.
- Own the AppSec testing strategy for data-sensitive areas: token-misuse scenarios, privilege-escalation testing, and observability/logging validation.

Test Automation Engineer 2025 – 2026

Globant — Bogotá, Colombia *Hybrid*

Qiddiya program — large-scale Web / Mobile / API quality automation.

- Built cross-platform automation frameworks (Playwright, Appium, Cucumber) for Web, Mobile, and API, reaching **90% automated coverage** on critical business flows.
- Integrated automation suites into GitLab CI/CD pipelines, shortening feedback loops and improving release reliability — the foundation now applied to security automation.
- Applied a shift-left approach, analyzing system architecture early to surface failure points before release; contributed to an internal AI-powered testing agent.

SECURITY RESEARCH & LAB INFRASTRUCTURE

Self-built security lab demonstrating offensive depth and an attacker's perspective — a differentiator for AppSec work.

- **Offensive research:** Linux kernel-module development in C (syscall-table manipulation, CR0 write-protection bypass, syscall hooking, covert C2 over Netfilter); M.S. thesis on rootkit detection via kernel-level entropy analysis.
- **Hands-on practice:** Continuous offensive-security practice on Hack The Box (web exploitation, network attacks, privilege escalation) with an ongoing weekly streak.
- **Network & infrastructure:** Five-VLAN segmented architecture on RouterOS with independent IPv6 via LACNIC; Tor relays/obfs4 bridges; OpenVPN/WireGuard.
- **Defensive operations:** Honeypots (Cowrie, Dionaea, Conpot), MISP threat-intelligence pipeline, and Wazuh SIEM monitoring in an isolated sandbox.

TECHNICAL SKILLS

Application Security: API & web app security, OWASP Top 10, authentication/authorization testing, IDOR & privilege-escalation testing, negative/abuse testing, sensitive-data & PII leakage validation, vulnerability assessment (VAPT).

Security Automation & DevSecOps: Playwright, security test frameworks, CI/CD security gates (GitLab, GitHub Actions), DAST (OWASP ZAP), CI/CD integration, containerization & hardening.

Offensive Security: Penetration testing (eJPT), kernel-level exploitation, rootkit development & detection, network attack/defense.

Networking & Infrastructure: IPv6, VLAN segmentation, RouterOS/MikroTik, OpenWRT, firewalling, VPNs (OpenVPN, WireGuard), DNS/DNSSEC, traffic analysis.

Languages & Tooling: C, Python, Go, Bash; Linux internals; Burp Suite, OWASP ZAP, Wazuh, MISP.

Spoken Languages: Spanish (native), English (C1), French (B2).

EDUCATION

M.S. in Information Security Jan 2026 – Dec 2027 (in progress)

Universidad de los Andes — Bogotá, Colombia

- Offensive and defensive security: Cloud Security, Network Defense, Cryptography, Secure Programming, Digital Forensics. Thesis: Linux rootkit detection via information theory.

B.S. in Systems Engineering Jan 2022 – Jul 2025

Pontificia Universidad Javeriana — Bogotá, Colombia

- Strong foundation in networks, operating systems, and security. Teaching Assistant (OS, Data Structures, Advanced Programming); Vice-Chair of IEEE Javeriana (Best Student Branch in Colombia).

CERTIFICATIONS

eJPT — eLearnSecurity Junior Penetration Tester (2025) • ISC2 CC — Certified in Cybersecurity • INE CCA — Certified Cloud Associate • Google Cloud — Cloud Digital Leader • Hack The Box — active practice

RECOGNITION & LEADERSHIP

- 1st place in Colombia — IEEEXtreme 18 Programming Competition (2024).
- 2nd place — CyberWings cybersecurity competition, Colombian Air Force.
- Judge — VEX Robotics World Championship, Dallas, USA. Founded chapters and led technical teams of 30+ members across IEEE Javeriana and IEEE Uniandes.