JEAA Infosec LLC

Offensive Security | Vulnerability Management | Security Automation | Servicio en Español

antonio@jeaainfosec.com
https://www.jeaainfosec.com
https://linkedin.com/company/jeaa-infosec

UEI: WYQGFA6R4U46 | **DUNS:** 135084538 | **CAGE:** 14C54 | **EST:** Dec 13, 2024

JEAA Infosec LLC is a veteran-owned cybersecurity firm specializing in offensive and defensive information security services. Founded and operated by industry-certified professionals, JEAA Infosec delivers advanced penetration testing, red team operations, and application security consulting designed to strengthen organizations' resilience against modern threats. Beyond traditional offensive and defensive operations, JEAA Infosec specializes in securing AI and Large Language Model (LLM) ecosystems, hardening them against data exfiltration, prompt manipulation, and model-level exploitation. The firm further strengthens client environments through localized, fault-tolerant security frameworks that eliminate single points of failure and preserve operational resilience.

500+	100+	72 hours	15%
VULNERABILITIES FOUND	ASSESSMENTS	AVG TURNAROUND	ATTACK REDUCTION

Web Application Penetration Testing

Comprehensive web security assessments combining a mix of automated and manual techniques to identify, exploit, and validate vulnerabilities across modern application stacks. Engagements focus on real-world exploitability and business risk.

- OWASP Top 10
- API Security Testing
- Authentication Bypass
- Logic Flaws
- Custom Exploit Chains
- Advanced Payload Engineering
- XSS
- SQL Injection
- RCE

Security Automation & Tool Development

Custom Python-based automation frameworks that streamline vulnerability discovery, exploitation validation, and reporting workflows. Tools integrate AI-powered analysis for faster triage and adaptive scanning.

- Automated Scanning Pipelines
- Flask Security Applications
- AI-Assisted Analysis
- Real-Time Alerting
- Workflow Integration APIs
- Continuous Testing Modules

Vulnerability Management Platform

Development of tailored vulnerability management systems with markdown-ready reporting, visual analytics, and remediation lifecycle tracking. Designed for developer collaboration and long-term visibility.

- Executive Dashboards
- Developer-Friendly Reports
- Risk Prioritization
- Remediation Roadmaps
- API Integrations
- Secure Data Storage

AI & LLM Security Integration

Assessment and hardening of AI and Large Language Model (LLM) environments to mitigate data leakage, prompt injection, and model exploitation risks. Includes design of localized, redundant architectures to minimize single points of failure.

- AI/LLM Threat Modeling
- Prompt Injection Testing
- Data Isolation
- Localized AI Infrastructure
- Model Exploitation Defense
- Security Automation for AI Pipelines

WHY CHOOSE JEAA INFOSEC LLC

- ✓ AI & LLM Security – Securing next-generation AI systems against data and model exploitation.
- ✓ Developer-Focused Fixes – Actionable remediation with code examples and validation testing.
- ✓ Research-Driven – Constantly evolving methodologies built on active security research.
- ✓ Workflow Integration – Findings integrated seamlessly into existing CI/CD and ticketing systems.
- ✓ Localized Resilience – Fault-tolerant solutions that eliminate single points of failure.
- ✓ Adversary Simulation – Real-world attack emulation beyond standard vulnerability scans.
- ✓ Agile Delivery – Rapid, adaptive engagement model tailored to each client's environment.
- ✓ Bilingual Operations – Servicio en Español for international and cross-border collaboration.

PAST PERFORMANCE

Application Security Assessment – Financial Services Sector

Identified multiple high-impact vulnerabilities, including a critical XML External Entity (XXE) injection that allowed unauthorized server file access. Delivered proof-of-concept exploitation, root-cause analysis, and mitigations aligned with OWASP and NIST standards.

Web Application Penetration Test – SaaS Platform Provider

Discovered and demonstrated persistent XSS through SVG file uploads, leading to cross-tenant data exposure risks. Provided secure file-handling remediation guidance and validation testing post-fix deployment.

Adversary Simulation – Government Contracting Environment

Executed a red team operation leveraging API chaining, privilege escalation, and authentication bypasses to simulate insider threat scenarios. Provided executive debriefs and actionable mitigation roadmaps for long-term resilience.

TOOLS & TECHNOLOGIES

Burp Suite Pro | Metasploit | Custom Python Arsenal | Nmap | SQLMap | Docker | Proxmox | VMWare | Cisco | .Net | PHP | Node.js | Next.js | Java | Javascript | LLM

CERTIFICATIONS

Security+ | A+ | Linux+ | Pentest+ | GIAC Penetration Tester (GPEN) | GIAC Certified Forensic Analyst (GCFA) | GIAC Web Application Tester (GWAPT)