Rayane Boucheraine

AI SECURITY RESEARCHER

CONTACT

Phone: +213 540 03 21 24

Location: Béjaïa, Algeria

Email: r_boucheraine@estin.dz

Portfolio: https://r4y4n3.tech/

X: https://x.com/R4Y4N3___

GitHub: https://github.com/R4Y4N3

LinkedIn: https://www.linkedin.com/in/rayane-boucheraine

PROFILE

AI Security Researcher focused on the security and safety of AI models, LLM applications, and autonomous agents. My work combines vulnerability research and adversarial testing, covering prompt injection, RAG and MCP security, agent skills, tool-use vulnerabilities, and authorization boundaries. I conduct independent research and AI bug bounty hunting, developing reproducible proofs of concept to assess security risks and their impact. My goal is to turn research findings into practical defenses for safer, more secure AI systems.

EXPERIENCE

Independent AI Security Researcher | 2026 – Present

Offensive AI Security & Agentic Systems

- Conduct independent vulnerability research and bug bounty hunting across LLM applications and agentic systems, investigating prompt injection, RAG, MCP, and authorization security.
- Developed working exploit chains demonstrating how attacker-controlled content can compromise agent behavior, modify persistent configurations, and trigger unauthorized tool execution.
- Develop and evaluate adversarial attacks to identify exploitable weaknesses, assess security risks, and improve the security and safety of AI systems.

CTF Competitor | 2023 – Present

CascRooT Team

- Compete in AI security, web exploitation, and other cybersecurity challenges, applying offensive security techniques.
- Apply vulnerability analysis, scripting, and exploit development to solve complex security problems collaboratively.

EDUCATION

ESTIN — National School of Computer Science and Technologies | 2023–2028

Engineering Degree in Computer Science — Expected 2028

- Specialization: Cybersecurity. Fourth-year student in a five-year integrated engineering program.
- Relevant coursework: Artificial Intelligence, Algorithms and Data Structures, Software Engineering, Operating Systems, Computer Networks, and Mathematics.

ACTIVITIES & LEADERSHIP

Nexus Security Club | 2025–2026

President

- Led a cybersecurity student community of over 400 members, coordinating technical workshops, CTF competitions, and hands-on security activities.
- Mentored students in vulnerability analysis, technical projects, and collaborative problem-solving while supporting event organization and technical teams.

SKILLS

AI & Agent Security:

- LLM and agent red teaming, indirect prompt injection, RAG/MCP security, tool-use vulnerabilities, memory poisoning, and authorization boundaries.

Security Research:

- Vulnerability research, threat modeling, attack-surface analysis, adversarial evaluations, exploit development, reproducible experimentation, and security impact assessment.

Programming:

- Python, Rust, C, JavaScript.

Research Interests:

- Secure agentic AI, AI identity and authorization, trustworthy tool ecosystems, multi-agent security, and AI robustness.

LANGUAGES

- **English — Fluent**
- **Arabic — Native**
- **French — Intermediate**