Michal Bazyli

AI Red Team Security Researcher

bazyli.michal@gmail.com · · Remote

EXECUTIVE SUMMARY

Offensive Security Engineer and Security Researcher with ~8+ years of experience in **penetration testing, red teaming, blockchain security, and AI security**. Proven track record of discovering critical vulnerabilities (CVE-listed), leading security teams, and building advanced tooling using LLMs and automation.

EXPERIENCE

Cyber Security Researcher – AI
07/2025 – Present

Cracken.ai · Remote

- Adversarial testing of LLM applications — developing custom jailbreaks, prompt injection payloads, and bypass chains against guardrails.
- Design and implement defenses against prompt injections, jailbreaks, and indirect prompt injection vectors.
- Build generative AI solutions (Python, Go): prompt engineering, RAG pipeline tooling, and LLM-driven autonomous agents.
- Architect automated evaluation systems measuring agent accuracy, safety, and reliability across adversarial scenarios.
- Rapid prototyping of security automation tools for offensive/defensive AI workflows.

Lead Security Engineer
03/2023 – 06/2025

Resonance.Security · Remote

- Led a team delivering adversarial simulations across DeFi, L1/L2 infrastructure, and AI-integrated systems.
- Designed internal security tooling leveraging LLMs and generative AI to automate recon, triage, and report generation.
- Conducted smart contract audits (Rust, Solidity) — identified critical vulnerabilities and advised secure architecture.
- Scoped engagements and authored Statements of Work for complex red team assessments.

Lead Offensive Security Engineer
12/2021 – 11/2022

Halborn · Miami, FL

- Led CosmWasm security team — smart contract audits across Solidity, CosmosSDK, and Substrate.
- Conducted adversary simulations from conception through reporting; developed custom exploits and tooling in Rust and JS.
- Audited Layer 1 blockchain node implementations (Rust).

Senior Information Security Specialist
01/2021 – 12/2021

Shorebreak Security · Cocoa Beach, FL

- Full-scope penetration testing: web, infrastructure, thick client, Android, and iOS applications.
- End-to-end client engagement — scoping, execution, reporting, and remediation guidance.

Security Researcher / Senior Penetration Tester
07/2019 – 01/2021

Afine · Warsaw

Senior Penetration Tester
02/2018 – 08/2019

ING TECH · Katowice

Python Developer
12/2016 – 02/2018

Nokia · Wrocław

SKILLS

PyTorch · LangChain · LlamaIndex · RAG Pipelines · HuggingFace · Giskard · OpenAI API

Prompt Injection · Jailbreak Development · Data Poisoning · Adversary Simulation · Guardrail Bypass · LLM Eval Frameworks

Custom Exploit Dev · Rust · Python · Go · Solidity · CosmWasm

CERTIFICATIONS

- AIRTP+
- Certified Red Teaming Expert
- OSCP – Offensive Security
- eWPTX – eLearnSecurity

CVES

- CVE-2019-1082 – Microsoft Windows Elevation of Privilege
- CVE-2019-4103 – IBM Tivoli Netcool Remote Code Execution
- CVE-2019-2414 – Oracle HTTP Server Local Privilege Escalation
- CVE-2018-10835 – Meinberg Arbitrary File Upload / Privilege Escalation
- CVE-2018-10834 – Meinberg Arbitrary File Read / Privilege Escalation
- CVE-2018-11093 – CKEditor Cross-Site Scripting

EDUCATION

Engineer — Telecom & Electronics

Opole University of Technology, 2017