

PROFILE

Senior penetration tester and offensive-security engineer with 4+ years across web, Active Directory, embedded / IoT and OT/ICS, wireless and AI systems. Leads assessments end-to-end, white-box to black-box, reporting directly to engineering and compliance stakeholders. Product-security specialist in regulated environments: EN 18031 (RED delegated act) and CRA readiness, ETSI EN 303 645 IoT security, IEC 62443 IACS/OT, ANSSI CSPN and FDA medical audits. Wireless testing on connected products (WiFi WPA2/WPA3-EAP, BLE, RF). OSCP and CRTP certified, author of CVE-2025-52970 PoC. Every finding demonstrated with a working proof-of-concept.

EXPERIENCE

Security Expert / Penetration Tester

Mar 2025 - Present

BYCYB (ex CRYPTON.IT, filiale LNE) · cyber audit, certification & training · Paris



- Multi-domain assessments (white-box, grey-box and black-box):** web and API, Active Directory, Android/iOS, IoT/OT/ICS/SCADA and medical devices; UART/I2C/JTAG/USB, firmware and update reverse engineering.
- Wireless & RF security:** WiFi (WPA2/WPA3-EAP), Bluetooth Low Energy, RF spectrum analysis, packet injection and wireless protocol testing on connected products.
- Product & industrial compliance:** EN 18031 (RED delegated act) and CRA readiness evaluations, ETSI EN 303 645 IoT security, IEC 62443 IACS/OT assessments, ANSSI CSPN and LNE cash-register audit.
- Offensive security research & LLM:** local inference engines, model optimization, fine-tuning and evaluation; OWASP GenAI attack testing across prompt injection, guardrails, system-prompt leakage and agent/MCP workflows.
- Senior delivery:** scopes and leads assessments end-to-end, from kick-off to retest, with direct reporting to engineering and compliance stakeholders; custom Python tooling and 79 findings across five 2026 engagements (14 critical).
- Knowledge transfer:** internal and external training on Android malware reverse engineering, LLM/MCP pentesting, EN 18031 to CRA, and IACS/OT/SCADA security.

Security Expert / Penetration Tester

Mar 2025 - Jul 2025

CRYPTON.IT · cybersecurity consulting · Paris · team rebranded to BYCYB in Aug 2025



- Cybersecurity consulting across web, Active Directory and embedded/IoT systems:** white-box and grey-box testing, custom Python exploits and reporting.
- IoT and compliance foundation:** EN 18031 readiness, IoT device assessment and first WiFi/BLE wireless tests on connected products.

Apprentice Penetration Tester

Sep 2021 - Jul 2024

Département des Hautes-Alpes - Gap

- Web and grey-box Active Directory pentesting,** custom Python/HTML/JavaScript exploits and reporting.
- 22 zero-days** on internal applications; malware development (Python/C#/ASM), EPP/EDR evasion, BOF and MDE detection testing.
- Authorized red-team exercise:** physical intrusion, 70+ USB devices deployed and 30% callback; Cyberwatch vulnerability management and ISO 27002 governance.

SELECTED FINDINGS

- Mobile secrets to Firebase,** HR backend exposure and account takeover chain (critical, sanitized client finding).
- Cross-domain IDOR/BOLA at scale:** user, employee and document records exposed (critical, sanitized client finding).
- Unsigned charging-station firmware,** open debug access and unauthenticated privileged control commands.
- Medical workstation kiosk escape** and pre-authentication token parsing weakness.
- SAML assertion replay** bypassing WordPress authentication; **U-Boot / HAB bypass** leading to unauthenticated RCE.
- Public disclosures** incl. unauthenticated WordPress REST endpoint (ElementsKit Lite) and reflected XSS chain on Dorksearch.
- 2025 assessments:** unauthenticated DICOM parser DoS, AdminSDHolder persistence, stored XSS through upload validation and broken access control in enterprise workflows.

OPEN-SOURCE TOOLS & CONTRIBUTIONS

Tools: [GitHarvest3r](#) · [Nerv0usR4bbit](#) · [Ping-Of-Death](#) · [Soft-Script-V.2](#). Metasploit Ruby exploit (2021): [Microsoft Office Word MSHTML RCE](#). Contributions: [CrackEverything6 \(2023\)](#) · [malicious-wordpress-plugin \(2024\)](#).

AI SECURITY, LOCAL LLM & RESEARCH

Built and maintained a large local-LLM lab for model deployment, inference-engine evaluation and security research: quantization and performance optimization, fine-tuning, benchmarking, reproducible evaluation harnesses and agent/tool workflows. Studied and tested AI vulnerabilities including prompt injection, indirect injection, system-prompt leakage, guardrail bypass, unsafe tool use, data exfiltration and MCP/agent security. Developed offensive tooling and repeatable experiments for local models, applied to vulnerability research and defensive analysis. Fine-tuned Kairos, a 0.3B Apache-2.0 decision model for zero-generation decision scoring and semantic routing in cascade deployments, [on Hugging Face](#). Public technical study: integer-overflow analysis in Apple CoreGraphics (iOS / macOS), [CVE-2026-86950](#).

SKILLS

Web & API	Burp Suite Pro, SQLMap, ffuf, Nuclei, OWASP WSTG
Active Directory	BloodHound, Mimikatz, Rubeus, Impacket, PingCastle, PurpleKnight
Embedded / IoT / OT	UART, I2C, JTAG, RS232, binwalk, Ghidra, U-Boot, IEC 62443
Wireless / RF	WiFi, RF, spectrum analysis, wireless protocols, packet injection
Red Team	Metasploit, Havoc, BOF, SysWhispers, Hell's Gate, EPP/EDR evasion
AI / LLM	Local inference engines, optimization, quantization, fine-tuning, evaluation, OWASP Top 10 GenAI, MCP, Kairos (own fine-tuned 0.3B decision model, huggingface.co/34zY/Kairos)
Recon / threat intel	Subfinder, httpx, Shodan, MITRE ATT&CK, CVE and zero-day research
Compliance / standards	EN 18031 (RED), ETSI EN 303 645, IEC 62443, ANSSI CSPN, CRA readiness, ISO 14971 / IEC 62304
Languages	Python, PowerShell, Bash, C, C#, JavaScript, x86-64 ASM

CERTIFICATIONS



OSCP · Offensive Security, 2024



CRTP · Certified Red Team Professional, 2025



Red Hat · System Administration II & III, 2022



PentesterLab · HTTP, Essential, White, Blue, Serialize, 2023

EDUCATION

ESEE-IT - engineering school (Paris) - Engineering Manager in Cybersecurity, 2021-2024

Lycée Philippe de Girard - BTS Digital Systems, Electronics & Communications, 2019-2021

LANGUAGES

French (native) · English (professional) · Spanish and German (basic)