MAIMO HARRIS SHAALANYUY

Penetration Tester | VAPT Engineer | BEng Computer Engineering

Bamenda, Cameroon | +237 680 226 898 | maimoharris111@gmail.com | linkedin.com/in/maimoharris | github.com/Maimoharris

Open to remote work and relocation

PROFESSIONAL SUMMARY

Penetration Tester with 5+ years of experience across web application, API, mobile, network, and Active Directory environments, delivering black-box, gray-box, and white-box assessments for international clients. Completed 350+ paid engagements and disclosed critical vulnerabilities across 100+ bug bounty programs, scoring findings under CVSS v3.1 and mapping remediation to OWASP, PTES, MITRE ATT&CK, PCI-DSS, and ISO 27001.

CORE SKILLS

- **Testing Scope:** Web Application, API (OWASP API Top 10), Mobile (iOS/Android), Network, Active Directory, Cloud (Azure), IoT, Red Team & Adversary Emulation, Social Engineering / Phishing Simulation
- **Frameworks & Compliance:** OWASP Top 10, OWASP ASVS, PTES, NIST SP 800-115, MITRE ATT&CK, PCI-DSS, ISO 27001, CVSS v3.1
- **Tools & Scripting:** Burp Suite, OWASP ZAP, Metasploit, Nmap, SQLMap, Wireshark, Nessus, Havoc C2, Sliver C2, Evilginx2, Impacket, BloodHound, Hydra, John the Ripper, FFUF, Gobuster, Python, C/C++, Rust, Bash, PowerShell

CERTIFICATIONS

- Certified Red Team Analyst (CRTA) — CyberWarfare, August 2025
- Certified Associate Penetration Tester (CAPT) — Hackviser, December 2025
- Certified API Security Analyst (CASA) — APISEC University, April 2026

PROFESSIONAL EXPERIENCE

Cyenetic Solutions LTD — Lead VAPT Engineer April 2026 – Present

Dhaka, Bangladesh

- Lead VAPT delivery for enterprise clients, owning engagement scoping, testing execution, and client reporting; completed 20+ engagements to date.
- Mentor a team of 5 penetration testers, standardizing testing checklists and peer-review processes to cut reporting turnaround time across engagements.
- Conduct black-box and gray-box tests against web, API, and network infrastructure using Burp Suite, Nmap, and Metasploit, aligned with the OWASP Testing Guide and PTES.
- Discovered a critical Broken Access Control flaw where privileged endpoints lacked server-side authorization; fixed within a week, prompting a client-wide review that caught more issues and added mandatory authorization testing to their secure development checklist.
- Manage overlapping client testing schedules through Agile-based sprint planning to keep concurrent engagements on schedule.

Skye8 — Penetration Tester **August 2024 – February 2026**

Bamenda, Cameroon

- Executed 200+ black-box, gray-box, and white-box tests across API, web, and mobile targets using Burp Suite, OWASP ZAP, SQLMap, and Postman, following OWASP ASVS and OWASP API Security Top 10.
- Led red team operations and full-scope offensive engagements — including malware development under authorized, contracted engagements — to simulate APT tactics mapped to MITRE ATT&CK.
- Used BloodHound to uncover a chained privilege-escalation path to Domain Admin (600-employee org) via accumulated delegated permissions invisible to manual review; remediation (tiered admin model, Protected Users, LAPS) closed the path, confirmed in a month-later retest.
- Authored technical write-ups and executive-level reports, scoring findings with CVSS v3.1 and aligning recommendations with NIST SP 800-115 and PCI-DSS.

IZZY Tech — Penetration Tester **March 2022 – July 2024**

Bambui, Cameroon

- Conducted 150+ vulnerability assessments and penetration tests; found a Critical IDOR in a client's invoicing API exposing other customers' financial data and PII, fixed within 5 days, with expanded checks catching two more authorization issues before release.

Bug Bounty Researcher — HackerOne, Bugcrowd, Hackprove **February 2020 – Present (Part-Time)**

Remote

- Identified and responsibly disclosed critical vulnerabilities across 100+ bug bounty programs; notably a Critical BOLA on a private fintech program exposing other users' financial data, fixed within days and awarded a $1,000 bounty.

EDUCATION

University of Bamenda — B.Eng, Computer Engineering **Oct 2023 – Present (Final Year)**
Bamenda, Cameroon | GPA: 3.74

- Coursework: Computer Security, Networking, Operating Systems, C/C++, Rust, Python 3, Software Engineering

KEY PROJECTS

- **Reac2Shell — CVE-2025-55182 Scanner (May 2025):** Proof-of-concept exploit and vulnerability scanner for the React2Shell RCE vulnerability. Stack: Python 3, Node.js, React.js. GitHub: github.com/Maimoharris/React2ShellScanner
- **Automated Recon Tool for Bug Bounty (Feb 2025):** Modular subdomain enumeration, port scanning, and live-host detection tool. Stack: Python, Bash, Nmap, Subfinder, httpx, Amass. GitHub: github.com/Maimoharris/portscanner
- **Azure Red Team Lab & C2 Infrastructure (July 2026):** Self-hosted red team lab running Sliver C2 and Evilginx2 for adversary emulation, with CDN-fronted redirectors reducing signature-based detection during authorized engagements. Stack: Azure, Sliver C2, Evilginx2, Nginx, CDN.
- **DocConvert & DevSecKit (HR-Tech, 2025 – Present):** Founded HR-Tech and independently built DocConvert (AI document conversion SaaS) and DevSecKit (privacy-first developer/security toolkit). Live: docconvert.me, devseckit.lovable.app

AWARDS & ACHIEVEMENTS

- Ranked 1st out of 300+ Participant — HackSprint 2025, University of Bamenda
- Winner, RSA CTF — Red Shielders Africa (2025)
- PACE7 Ranked 20th Position out of 600+ Project — Cameroon Digital Innovation Weak (2026)

LANGUAGES

English — Native
French — B1