Maimo Harris Shaalanyuy Ndze

Red Team | 3+ Years Offensive Security Experience | Web, Network, IoT & Mobile Pentesting | Bug Bounty Hunter

Cameroon, Bamenda,Bamili ☎ +237680226898 @ maimoharris111@gmail.com https://maimoharris.onrender.com
LinkedIn GitHub

◦ Skills ◦

Penetration Testing & Red Team Skills
Web, Mobile, IoT, and Network Pentesting Active Directory Attacks Vulnerability Assessment & Exploitation Red Team Simulation & Post-Exploitation Malware Development & Reverse Engineering Social Engineering & Physical Security (basic)

Tools & Frameworks
Burp Suite, OWASP ZAP, Nmap, Metasploit, SQLMap Wireshark, Hydra, John the Ripper, Nessus Amass, FFUF, Sublist3r, Gobuster MITRE ATT&CK Framework OWASP Top 10 Custom payload scripting, IDA Pro ,Ghidra, olydbgx64

Programming & Scripting
Python (Advanced) C, C++ Bash & PowerShell scripting Django (Backend Web Development)

Programming

Machine Learning in Security
Automated recon & anomaly detection ML models for malware behavior analysis Python (Scikit-learn, Pandas, NumPy)

Operating Systems & Environments
Kali Linux, Parrot OS Ubuntu, Windows, Windows Server VirtualBox, VMware, Docker (basic)

Miscellaneous Technical Skills
Git & GitHub Secure API testing Report writing & vulnerability documentation Task automation and recon tool building

◦ Interests ◦

Offensive Security & Red Teaming
Cybersecurity, Hacking, Pentesting

Malware Analysis
IDA Pro, Ghidra, Assembly Language, Architectures

Bug Bounty Hunting

Capture the Flag (CTF) Competitions

Open Source Projects

Machine Learning and AI

Physics and Maths

◦ Certifications ◦

Certified Red Team Analyst (CRTA)
cyberwarfare
August 2025

Demonstrates foundational skills in red teaming including adversary simulation, network exploitation, and attack techniques.

https://portal.cyberwarfare.live/

Ethical Hacker
Cisco
December 2023

Validates expertise in ethical hacking methodologies, penetration testing, and vulnerability assessment.

https://www.credly.com/badges/09233391-f467-4c13-beff-2df1ddcbc653/public_url

Penetration Tester
IT-Master
February 2025

- **Level**: Beginner–Intermediate—ideal for those entering penetration testing
- **Skills covered**: Scoping engagements, environment reconnaissance, Active Directory assessment, privilege escalation, and reporting findings
- **Why it's valued**: Hands-on labs and structured methodology give practical readiness for entry-level roles.

https://learn.itmasters.edu.au/course/view.php?id=3873

Certified Associate Penetration Tester (CAPT)
hackviser
September 2025

https://hackviser.com

◦ Awards ◦

Winner, HackSprint
Center of Cybersecurity and mathematical Cryptology UBa
May 2025

Demonstrated advanced offensive security skills by successfully identifying and exploiting multiple vulnerabilities in a controlled environment, showcasing expertise in penetration testing, vulnerability assessment, and ethical hacking.

https://ubacybercryptocenter.cm/en

Winner, RSA CTF
Red Shielders Africa (RSA)
July 2025

Demonstrated advanced offensive security skills by successfully identifying and exploiting multiple vulnerabilities in a controlled environment, showcasing expertise in penetration testing, vulnerability assessment, and ethical hacking.

https://rsafrica.org/

Winner, COME OverFlow 2.0
NAHPI
May 2025

Developed a full-stack e-commerce mobile application using Django for the backend and React Native for the frontend. Delivered a seamless user experience with secure authentication, product listings, and real-time updates, demonstrating strong skills in cross-platform development and rapid prototyping.

https://nahpi.cm/

◦ Languages ◦

English
Native

Pidgin English
Native

Spanish
Beginner

Arabic
Beginner

Profiles

- maimoharris
- Maimoharris

Summary

Passionate and hands-on offensive security professional with 5+ years of experience in red teaming, penetration testing, malware analysis, and bug bounty hunting. Skilled in assessing Web, Mobile, IoT, and Network security using both manual techniques and industry-standard tools. Expertise in integrating Machine Learning for vulnerability discovery and anomaly detection. Also a Backend Developer proficient in Django and Python, with a strong focus on secure application development. Currently a 3rd-year Computer Engineering student seeking a 6-month internship in Red Team Operations.

Experience

Skye8
Red Team Lead & Penetration Tester
Bemenda, Cameroon
August 2024 - Present

- Coordinated internal red team operations and full-scope offensive engagements
- Conducted web, network, IoT, and mobile application penetration testing using tools like **Burp Suite**, **Nmap**, **Metasploit**, and custom scripts
- Developed and analyzed custom **malware and payloads** for internal simulation exercises
- Created detailed vulnerability assessment reports with **risk ratings, exploit evidence, and remediation guidance**
- Integrated **machine learning models** to automate log analysis and anomaly detection in red team simulations

https://skye8.tech/

CVA-Tech Ventures
Web Application Penetration Tester
Molyko, Buea
May 2024 - May 2025

- Performed manual and automated vulnerability assessments on client-facing web applications
- Identified OWASP Top 10 vulnerabilities and provided developers with actionable remediation steps
- Used tools such as **Burp Suite**, **OWASP ZAP**, **SQLMap**, and **Dirb** for scanning and testing
- Delivered security reports in professional formats with clear reproduction steps, screenshots, and impact statements

https://network.axial.net/company/cva-tech-ventures

IZZY Tech
Penetration Tester
Bambui, Cameroon
March 2023 - Present

- Conducted **penetration testing and vulnerability assessments** on internal systems, APIs, and mobile applications

https://izzytechteam.org/

Remote | Global Platforms (HackerOne, Bugcrowd, Hackprove)
Bug Bounty Researcher (Freelance / Independent)
Remote
Feb 2021 - Present

- Identified and responsibly disclosed critical vulnerabilities in **web applications, APIs, and cloud-hosted platforms**, including issues like **IDOR, XSS, SQLi, SSRF**, and authentication bypasses
- Utilized tools and custom scripts for reconnaissance and fuzzing, including **Burp Suite**, **FFUF**, **Amass**, and **custom Python payloads**
- Documented technical writeups and reproduced PoCs for platform triage teams
- Leveraged **machine learning-based recon automation tools** for large-scope targets (e.g., subdomain takeover, asset discovery)

https://www.hackprove.com

NEXURA
CTO
Bamenda,Cameroon
February 2025

https://nexura.com

Education

Uiversity of Bamenda
Bachelors of Engineering in Computer Engineering
3.8 GPA
Full-Time on Campus
October 2023 - Present

- Currently in **3rd Year**
- Relevant coursework: Computer Security, Networking, Operating Systems, Programming in C/C++, Software Engineering
- Academic focus on systems programming, low-level memory management, and secure application design
- Engaged in extracurricular **cybersecurity research, red teaming labs**, and independent offensive security projects

https://uniba.cm/

Projects

Internal Recon Automation Tool
Built a Python tool for internal recon in red team ops, gathering Active Directory data, scanning shares, and detecting exposed services, while employing stealth tactics to bypass endpoint security.
March 2023

Technologies: Python, Impacket, LDAP, SMB, Nmap
Role: Developer & Security Analyst

Phishing Simulation Framework
Designed and deployed a custom phishing simulation platform to assess organizational resilience. Includes email template management, credential harvesting simulation (no data stored), and reporting dashboard. Used in internal security awareness assessments.
August 2024

Technologies: Django, Bootstrap, SMTP, SQLite
Role: Full-stack Developer & Red Team Operator

Phishing & Credential Harvesting Platform (Skye8 / UN Tech Initiative Clone)
Created a phishing simulation website mimicking an official UN-sponsored tech initiative for Cameroon, designed to collect test credentials and simulate real-world attacks for user phishing awareness training.

- **Technologies:** Django, Django REST Framework, Bootstrap, Email Spoofing Techniques
- **Role:** Backend Developer, Red Team Operator

Pseudo Character Device Driver (Linux Kernel)
Developed a custom Linux kernel module under drivers/misc to simulate a pseudo character device supporting read, write, and seek operations — useful in low-level OS exploitation labs.
May 2025

- **Technologies:** C, Linux Kernel 5.x, GCC, insmod/rmmod
- **Role:** Kernel Developer

XSS & Web Exploit Testing Framework
Built test harnesses for simulating XSS payload injections on forms and DOM elements. Used for validating custom sanitization defenses and training junior analysts.
January 2025

- **Technologies:** JavaScript, Python (requests), Burp Suite, HTML payloads
- **Role:** Web App Security Engineer

KASH – Peer-to-Peer E-Commerce Platform
Built a web platform facilitating direct interaction between buyers and sellers, with a unique feature for reselling listings by customizing pricing and product photos. Implemented user authentication, product management, and admin controls, optimized for mobile and privacy-focused workflows.
April 2025

Technologies: Full-Stack Web Application | Django, Bootstrap, PostgreSQL, jQuery

https://www.digetech.org

Custom Python Keylogger (Red Team Lab Tool)
Developed a lightweight keylogger for educational and Red Team lab use, capturing keystrokes, timestamps, and window context with optional stealth mode. Used in isolated environments to study endpoint detection and behavioral analysis techniques in controlled, ethical hacking labs.
July 2025

Technologies:Offensive Security Tool | Python, Windows API, Logging

https://github.com/Maimoharris/keylogger

Automated Recon Tool for Bug Bounty Hunters
Security Automation | Python, Bash, Nmap, Subfinder, httpx, Amass
Febuary 2025

Developed a modular recon automation tool to streamline initial reconnaissance in bug bounty programs. Automates subdomain enumeration, port scanning, HTTP probing, live host detection, and screenshot capture, producing structured reports for efficient triage and vulnerability discovery. Optimized for scope filtering and tool chaining.

https://github.com/Maimoharris/portscanner