STEEVY TONGOUE BAGOFA

OFFENSIVE SECURITY STUDENT

CONTACT

steevyvalery7@gmail.com

Paris, France
(Open to Remote)

19 years old

linkedin.com/in/steevy-valery-tongoue-bagofa

github.com/Steevy-prog

Hack The Box – @Farstyle

TECHNICAL SKILLS

OFFENSIVE SECURITY

- Penetration Testing (in training)
- Web Application Security
- Network Enumeration
- Vulnerability Assessment
- Privilege Escalation
- Active Directory / Windows Security
- Authentication Attacks
- Exploitation & Post-Exploitation

TOOLS

Nmap, Burp Suite, Wireshark, Gobuster, ffuf, Netcat, Metasploit, Impacket, NetExec / CrackMapExec, BloodHound, Responder, Hashcat, John the Ripper

PROGRAMMING

Python, Bash, Rust, SQL, C++, Java, JavaScript, PHP

SYSTEMS & NETWORKING

Linux, Windows, Active Directory, TCP/IP, DNS, HTTP, SMB, LDAP, Kerberos, pfSense, VLANs/DMZ, Snort, Wazuh, Virtualization

LANGUAGES

French (Native)
English (Professional)

AVAILABILITY

Remote · Part-time
Up to 10 hrs/week alongside studies

INTERESTS

Tennis · Table tennis · Basketball
Video games

PROFESSIONAL SUMMARY

Third-year computer engineering student at ESIEA, Paris, specializing in cybersecurity. I focus on offensive security and enjoy building my own tools to understand and replicate real-world attack techniques. Looking for an internship where I can contribute to security assessments and continue growing as part of a technical team.

PRACTICAL SECURITY TRAINING

HACK THE BOX – LABS & ACADEMY — Ongoing

Level 33 – "Skilled" rank

- Work through Linux and Windows machines covering enumeration, exploitation, and privilege escalation.
- Practice Active Directory attacks using Kerberos, LDAP, SMB, BloodHound, Impacket, and NetExec.

SELF-PACED PLATFORMS & CTFs — Ongoing

- PortSwigger Web Security Academy — completed the Authentication learning path.
- CyLab Security Academy — 24 CTF challenges solved (20 easy, 4 medium).
- TryHackMe — Apprentice, 7 rooms covering pentesting fundamentals and content discovery.

RED TEAM EXPERIENCE – CTF COMPETITION — 2026

Team of four – Regional cybersecurity meetup

- Solved web, network, and forensics challenges under time pressure to take first place overall.
- Split workload across the team and coordinated findings during the competition.

SECURITY PROJECTS

VULNERABLE WEB APPLICATION LAB — Personal Lab

- Built a self-hosted, segmented environment to practice full OWASP-style attack chains rather than only pre-built targets.
- Stack: Nginx reverse proxy, ModSecurity WAF, Next.js / PostgreSQL / Prisma.
- Practiced enumeration, exploitation, and WAF-evasion in a controlled setup.

FARSTYLE – SECURITY AUDITING PLATFORM — Personal Project

- Native Rust desktop app (egui/eframe) bundling a proxy, repeater, intruder, and module engine in one interface.
- Built an HTTP/HTTPS intercepting proxy (rustls, rcgen) with a Python module system and JSON-over-stdin/stdout IPC for pluggable scanners.
- Added an AI workspace mapping tool modules to the right scanner based on knowledge base; ships built-in recon, fuzzing, and SQLi modules.

SEGMENTED NETWORK & MONITORING LAB — Personal Lab

- Built a functional multi-zone network with pfSense (firewall/router), DMZ and internal VLANs, and enforced inter-zone routing and firewall rules.
- Deployed Snort (IDS) and a Wazuh SIEM for intrusion detection, log collection, and alerting.
- Provides a blue-team view of the same attacks I practice offensively.

EDUCATION

ENGINEERING DEGREE – COMPUTER ENGINEERING — 2026 – 2029

ESIEA – Paris, France – Entering 3rd year – Specialization in Cybersecurity (from year 4)

PREPARATORY CYCLE – ENGINEERING — Sept 2024 – July 2026

UCAC-ICAM – Douala

VOLUNTEER EXPERIENCE — 2025

Volunteer – Hospital (Janitorial & Facilities Support)