MUYIDEEN ABDULSAMAD

Penetration Tester · Security Engineer · Bug Bounty Hunter · Blue Team

PROFESSIONAL SUMMARY

Security engineer with 6+ years of offensive and defensive security experience across web applications, APIs, mobile apps, network infrastructure, and Active Directory environments. Active bug bounty hunter on HackerOne and Bugcrowd. Experienced in cloud server hardening (Suricata, Wazuh, Splunk, OSSEC), red team penetration testing, and secure software development. Brings an additional edge in Rust systems programming and ML-driven anomaly detection for security applications.

TECHNICAL SKILLS

Offensive (Red Team): Burp Suite, Nessus, Metasploit, SQLmap, API hacking, Active Directory attacks (Kerberoasting, Pass-the-Hash, BloodHound), mobile app pentesting (Android/iOS), network pentesting

Defensive (Blue Team): Suricata, Wazuh, Splunk, OSSEC, Snort, SIEM, log analysis, threat hunting, server hardening, firewall configuration

Languages & Scripting: Python, Rust, Bash, JavaScript, Java, PHP, SQL injection payloads

Web Security: OWASP Top 10, XSS, CSRF, IDOR, JWT attacks, OAuth flaws, API security, custom encryption algorithms

Cloud & Infra: Linux server administration, Docker, SSH hardening, VPN, network segmentation

Certifications: Practical Ethical Hacking (TCM), Certified Network & Web Pentesting Professional (XSS-RAT), Network Security Assessment (StationX)

PROFESSIONAL EXPERIENCE

Penetration Tester / Bug Bounty Hunter | HackerOne · Bugcrowd · STEM Coders *2019 – Present*

- Built SamaritanX — an agentic bug-bounty framework (Python, asyncio) from scratch: autonomous agents for recon, crawl, 12-category vulnerability scanning, logic abuse, and exploit-chain synthesis, with HTTP-boundary scope enforcement, interactsh OOB validation, and automated MD/PDF reporting. (github.com/Th3Samaritan/SamaritanX)
- Conducted full-scope web application penetration tests covering OWASP Top 10 vulnerabilities, business logic flaws, authentication bypasses, and API security weaknesses using Burp Suite, custom scripts, and manual analysis.
- Performed network and Active Directory penetration tests including Kerberoasting, Pass-the-Hash, lateral movement, and privilege escalation; delivered detailed remediation reports to clients.
- Executed mobile application security assessments on both Android and iOS platforms; identified insecure data storage, improper session handling, and API endpoint vulnerabilities.
- Identified and responsibly disclosed critical vulnerabilities across production web apps and APIs through HackerOne and Bugcrowd bug bounty programmes.
- Blue Team: hardened cloud servers for multiple production environments using Suricata (IDS/IPS), Wazuh (SIEM/EDR), Splunk (log analytics), OSSEC (host-based IDS), and Snort; reduced attack surface and achieved 100% clean audits post-hardening.
- Developed custom Python and Bash scripts for automated vulnerability scanning, log parsing, and threat detection workflows.
- Leveraged Rust for writing high-performance, memory-safe security tooling — custom network scanners and packet parsers with zero undefined behaviour.

Secure Software Developer | STEM Coders Club / Freelance *2017 – Present*

- Designed and implemented custom AES-based database encryption algorithms for client web applications; ensured data-at-rest protection meeting industry security standards.

- Applied secure coding practices across all software projects: input validation, parameterised queries, CSRF protection, secure session management, and Content Security Policy headers.
- Architected and deployed production systems (FastAPI + React.js on Kubernetes) with security-first design: RBAC, secrets management, and network policy enforcement.
- Built FajrGuard — on-device AI app with local inference, deliberately avoiding cloud data transmission to preserve user privacy by design.

Content Creator & Tutor — Cybersecurity | Hackerats.com / STEM Coders / Campus *2019 – Present*

- Published cybersecurity content on Hackerats.com covering bug bounty methodology, ethical hacking techniques, and InfoSec career guidance.
- Delivered cybersecurity workshops and tutorials to campus students covering bug bounty hunting, ethical hacking, and web application security — trained 30+ students.

EDUCATION

B.Eng. Metallurgical & Materials Engineering *Oct 2024*

Ahmadu Bello University, Zaria · Second Class Upper (Hons)

Thesis: ML simulation and prediction of steel mechanical properties via iron-carbon phase diagram (Materials Informatics) — 90%+ prediction accuracy.

CERTIFICATIONS

- Practical Ethical Hacking — TCM Academy
- Certified Network & Web Pentesting Professional — XSS-RAT
- Network Security & Network Security Assessment — StationX
- Google Project Management Certificate
- Tech Oracle Award — NUESA Online Quiz Competition, 2024