

Charity Mulei

Software Developer, Penetration Tester

kochcharity3@gmail.com | <https://www.linkedin.com/in/charitymuleinakhchaz/>

<https://github.com/charity553>

Nairobi, Kenya, Kenya | +254706208553

Work Experience

Penetration Tester

Jan 2025 - May 2025

KIEP-SKIES Program, Jomo Kenyatta University of Agriculture and Technology

- Key Responsibilities :
- Conducted security assessments on operating systems, endpoints, and networks to identify vulnerabilities.
- Implemented endpoint security measures to protect against malware, unauthorized access, and insider threats.
- Applied network security protocols, including firewalls, IDS/IPS, VPN configurations, and secure tunneling.
- Assisted in compliance auditing for security standards such as ISO 27001, NIST, GDPR, HIPAA, and SOX.
- Evaluated cybersecurity risks, threat landscapes, and governance models.
- Conducted case studies on risk mitigation, cybercrime classification, and penetration testing standards (OWASP, SANS25, PTES).
- Performed threat hunting using MITRE ATT&CK, Cyber Kill Chain, and IOCs (Indicators of Compromise).
- Conducted network monitoring using Wireshark to detect malicious activity and network anomalies.
- Assisted in incident response planning, detecting, analyzing, and mitigating security incidents.
- Penetration Testing & Vulnerability Assessment
- Deployed and configured Vulnerability Assessment tools to scan and analyze security weaknesses.
- Conducted penetration testing using Metasploitable 2, Kali Linux, and OSINT tools to simulate real-world attacks.
- Performed privilege escalation (Windows & Linux), password cracking, post-exploitation, and risk reporting.
- Interpreted CVSS scores to prioritize vulnerabilities and recommended patches/updates.
- Gained hands-on experience with cryptography principles, encryption standards, and secure coding techniques.
- Conducted computer forensics investigations, including disk imaging, OS forensics, network forensics, and dark web analysis.
- Investigated web attacks, malware forensics, email and social media crimes.
- Applied anti-forensics techniques and forensic acquisition methodologies.
- Researched and analyzed cloud security, IoT security, and AI threats.
- Explored cybersecurity risks in Industrial Control Systems (ICS) and Cyber-Physical Systems (CPS).
- Implemented SIEM solutions for security monitoring and threat detection.
- Used PowerShell for security automation and Security Orchestration, Automation, and Response (SOAR) tools.
- Configured and maintained honeypots for deception technology and attack analysis.
- Tools & Technologies :
- Shodan (Cyber Threat Intelligence)
- Metasploitable 2, Kali Linux (Penetration Testing & Ethical Hacking)
- Wireshark (Network Traffic Analysis)
- SIEM & SOAR Tools (Security Event Management & Incident Response)
- Disk Imaging & Forensic Tools (Data Acquisition & Analysis)
- Firewalls, IDS/IPS, VPNs, Honeypots

Backend Developer

May 2023 - Apr 2025

THE HOT PLATFORM | Remote

- Developed robust and scalable APIs using Django, ensuring efficient communication between front-end and back-end systems.
- Implemented RESTful API endpoints, adhering to industry best practices and standards.
- Successfully integrated third-party applications, such as Zoom, into the existing system, enhancing functionality and user experience.
- Collaborated with cross-functional teams to understand integration requirements and implemented seamless solutions.
- Implemented security measures to protect APIs against common vulnerabilities, such as SQL injection and Cross-Site Scripting (XSS). Utilized version control systems (e.g., Git) to manage and track changes in the codebase.
- Conducted unit testing and participated in code reviews to maintain high code quality.

Software Developer Intern

Jan 2023 - Jan 2025

UNIVERSITY OF NAIROBI ENTERPRISES USAID | KAKAMEGA

- Key Responsibilities :
- Contributed to the development and improvement of the KenyaEMR system by participating in multiple workshops. Fixed bugs reported through user feedback and implemented UI enhancements to improve user experience. For example by adding a count feature to the procedure and radiology tabs, I made it easier for users to track data, which significantly enhanced the way users manage their workload in the radiology and procedure departments.
- Supported the remote and on-site installation and maintenance of the KenyaEMR system across Kakamega, Bungoma, Trans Nzoia, West Pokot, and Turkana counties. This involved capacity building, networking infrastructure setup, and software installations.
- Volunteered as a judge for a 4-day hackathon at Chuka University, evaluating projects centered around the Electronic Health Information System (eCHIS), developing middle-ware solutions for automated reporting to the Kenya Health Information System (KHIS), focusing on system logs for data analysis.
- Tools & Technologies :
- Shodan (Cyber Threat Intelligence)
- Metasploitable 2, Kali Linux (Penetration Testing & Ethical Hacking)
- Wireshark (Network Traffic Analysis)
- SIEM & SOAR Tools (Security Event Management & Incident Response)
- Disk Imaging & Forensic Tools (Data Acquisition & Analysis)
- Firewalls, IDS/IPS, VPNs, Honeypots

Core Skills

Python, Django, Flask, Java(Spring Boot), React, Nodejs, Nextjs, Microfrontends

Education

Masinde Muliro University of Science and Technology

Sep 2018 - Dec 2022

Bachelor's Computer Science

GPA: Second Class Upper

Certificates

Zero Trust Certified Associate (ZTCA)

Mar 2025

Z-scaler

Data Protection Basics

Mar 2025

Atingi

AWS for DevOps: Continuous Delivery and Process Automation

LinkedIn

KHMFL

MOH VIRTUAL ACADEMY

May 2022

KHIS-DHIS2

MOH VIRTUAL ACADEMY

Mar 2022