OBIOMA FELICITY UZOH

Cybersecurity Analyst | Blue Team & GRC

Gmail: [*obiomafelicityuzoh@gmail.com*](mailto:obiomafelicityuzoh@gmail.com) *| LinkedIn:* [*https://www.linkedin.com/in/felicityuzoh*](https://www.linkedin.com/in/felicityuzoh) *|*
Portfolio: [*https://techounik.github.io/techounik/*](https://techounik.github.io/techounik/)

PROFESSIONAL SUMMARY

Final-year Cybersecurity student and Hackviser Ambassador with a strong focus on **Security Operations (SOC)** and **Incident Response**. Experienced in building custom **Python automation tools** for log analysis and executing vulnerability assessments. Certified in Google Cybersecurity and Web Security, seeking to leverage skills in **threat detection** and **SIEM analysis**.

TECHNICAL SKILLS

- SIEM (Splunk), Log Analysis (Windows Event Logs), Digital Forensics, Python Automation, Incident Response.
- **Security Assessment:** Penetration Testing, Vulnerability Scanning, Threat Analysis, OWASP Top 10, Risk Assessment.
- **Network Security:** TCP/IP, Wireshark (Packet Analysis), Intrusion Detection, Cryptography, Identity & Access Management (IAM).
- **Tools & OS:** Kali Linux, Metasploit, Nmap, Burp Suite, VMware, Command-Line Interfaces (CLI).
- **Programming & Scripting:** Python (Intermediate), Bash Scripting.

TECHNICAL PROJECTS

BlueTeam_Kit | Forensic Triage Framework *(Python, Linux)*

- Developed a custom CLI tool to automate forensic analysis of Windows Event Logs (`.evtx`).
- Programmed detection logic to identify **Persistence (Event 4720)** and **Anti-Forensics (Event 1102)**.
- Implemented image metadata scanning to detect hidden malware payloads (Steganography).
- **Code:** github.com/TechOunik/BlueTeam_Kit

PROFESSIONAL EXPERIENCE

Student Ambassador | *Hackviser Oct, 2025 - Present*

- Actively engaged with the cybersecurity community to promote ethical hacking best practices and Hackviser training modules.
- Facilitated peer learning by simplifying complex cybersecurity concepts (such as Privilege Escalation and Cryptography) for fellow students.
- Demonstrated leadership by organizing study groups and providing feedback on platform usability.

Cybersecurity Job Simulations | Forage (Mastercard & Commonwealth Bank) | *Dec - 2025*

- **SOC & Incident Response:** Engineered Splunk dashboards for fraud detection and analyzed phishing data to identify high-risk social engineering targets.
- **Security Assessment:** Performed penetration tests on web applications, identified vulnerabilities, and authored remediation reports aligned with industry standards.
- **Governance:** Evaluated security training gaps and designed awareness infographics based on Australian Cybersecurity Centre standards.

Application Security Trainee (Certified) | Talk2Luke Academy | *Feb - 2026*

- **Vulnerability Scanning:** Configured and executed automated scans using OWASP ZAP on a Dockerized web application, identifying 14+ vulnerabilities.
- **Exploitation:** Demonstrated successful SQL Injection (SQLi) attacks to bypass authentication and execute administrative privilege escalation.
- **Scripting & XSS:** Developed custom Python scripts to detect Reflected XSS vulnerabilities and demonstrated impact via browser-based payloads.

EDUCATION

Bachelor of Science in Cybersecurity *[Miva Open University], [Abuja, Nigeria] Expected Graduation: [May, 2026]*

CERTIFICATIONS

- **Certified Associate Penetration Tester (CAPT)** - Hackviser | *November, 2025*
- **Google Cybersecurity Professional Certificate** - Coursera | *November, 2025*
- **Certified Web Security Expert (CWSE) -** Hackviser | December, 2025
- **Introduction to Cybersecurity -** Cisco | January, 2026
- **Talk2Luke Academy - Cybersecurity Training Program** | February, 2026