OBIOMA FELICITY UZOH

Entry-Level Cybersecurity Professional

Gmail: obiomafelicityuzoh@gmail.com | *LinkedIn: https://www.linkedin.com/in/felicityuzoh* | *Portfolio: Https://techounik.github.io/techounik*

PROFESSIONAL SUMMARY

Results-oriented Final-year Cybersecurity student and Hackviser Student Ambassador with a hybrid focus on **Offensive Security** and **Blue Team Defense**. Proven experience executing vulnerability assessments (OWASP Top 10, SQLi, XSS) and engineering **Splunk** dashboards for threat detection. Skilled in **Python scripting** for security automation and translating technical findings into executive reports. Committed to continuous learning and ready to apply a 'Purple Team' mindset to professional security challenges.

TECHNICAL SKILLS

- **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.

PROJECTS AND PRACTICAL EXPERIENCE

Integrated Security Portfolio (Red & Blue Team Operations) | *Self-Directed*

- **Red Team Ops:** Executed full-lifecycle penetration tests on virtual environments using **Kali Linux** and **Metasploit**, successfully identifying privilege escalation paths, SQLi, and XSS vulnerabilities.
- **Blue Team & Defense:** Analyzed 500+ packet captures in **Wireshark** to trace brute-force attacks and configured **VMware** labs to audit Identity & Access Management (IAM) controls.
- **Reporting:** Authored technical reports detailing 12 critical vulnerabilities with remediation steps aligned to **OWASP Top 10** standards.

PROFESSIONAL EXPERIENCE

Student Ambassador | *Hackviser October, 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 Analyst Job Simulation | Commonwealth Bank (Forage) *December 2025*

- **SOC & Incident Response:** Engineered data visualization dashboards using **Splunk** to detect fraud patterns and anomalies in historical customer data.
- **Penetration Testing:** Conducted security assessments on web applications to identify vulnerabilities and authored remediation reports to bolster defensive posture.
- **Security Awareness:** Designed infographics on password management best practices aligned with Australian Cybersecurity Centre standards.

Security Awareness Analyst Job Simulation | Mastercard (Forage) *December 2025*

- **Threat Analysis:** Analyzed phishing simulation data to identify high-risk business units susceptible to social engineering attacks.
- **Security Governance:** Evaluated gaps in organizational security training and implemented targeted educational procedures to improve the human firewall.
- **Reporting:** Authored executive summaries detailing threat landscapes and recommended training interventions.

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
- **CompTIA Security+ (SY0-701)** | *In Progress (Target Completion: June 2026)*