

AKANDE BLESSING EBENEZER

APPLICATION SECURITY ENGINEER · WEB, API & DEVSECOPS

Lagos, Nigeria · +234 816 168 4809 · BlessingAKande1001@gmail.com
github.com/BlessingAKande · linkedin.com/in/blessing-akande-9829b0320

PROFESSIONAL SUMMARY

Application Security Engineer with hands-on ownership of web application and REST API security across the Secure Software Development Lifecycle (SSDLC). Delivers secure source-code review, source-to-sink analysis, threat modelling, SAST/SCA/DAST, API security testing, and manual penetration testing with full vulnerability validation and remediation verification.

Currently securing a multi-repository e-commerce platform end-to-end — integrating automated security controls into CI/CD, performing dependency and secret scanning, and driving findings from detection through developer remediation. Strong practical depth in authentication and authorization testing (BOLA/IDOR), injection classes, XSS, session management, business-logic flaws, and DevSecOps automation. Combines AI-assisted analysis with rigorous independent validation.

CORE TECHNICAL SKILLS

Application Security: SSDLC · Secure Code Review · Source-to-Sink Analysis · Threat Modelling (STRIDE) · Data Flow Diagrams · SAST · SCA · DAST · API Security · Vulnerability Assessment · OWASP Top 10 · OWASP ASVS · CVSS v3.1

Web & API Security: Authentication & Authorization · BOLA/IDOR · Access Control · Input Validation · SQL/NoSQL Injection · XSS · Session Management · Business Logic Testing

Security Tooling: Burp Suite · OWASP ZAP · Semgrep · Snyk · CodeQL · Gitleaks · SonarQube · SQLMap · Caido · FFUF · Gobuster · Nmap

DevSecOps & CI/CD: Git · GitHub · GitHub Actions · SAST/SCA Pipeline Integration · Automated Security Testing · Dependency Scanning · Secret Detection · Finding Triage · Repository Security Scanning

Technologies: JavaScript/Node.js · REST APIs · Postman · Linux · Kali Linux · Docker

AI-Assisted Security: Code comprehension · Security research · Vulnerability analysis · Test-case generation · Remediation research · Technical documentation (always independently validated)

PROFESSIONAL EXPERIENCE

APPLICATION SECURITY ENGINEER

PhyhanAgro Marketplace Limited · Nigeria · 2024 – Present

- Own application security for a multi-repository e-commerce platform (backend, frontend, and corporate site), with primary focus on backend services and actively assessed repositories.
- Perform secure source-code reviews and source-to-sink analysis to identify insecure data flows and high-risk application behaviour before release.
- Design and execute security assessments across authentication, authorization, access control, input validation, API endpoints, session management, third-party dependencies, and business logic.
- Integrated four core security controls into the backend workflow — Semgrep, CodeQL, Snyk, and Gitleaks — enabling continuous automated analysis of code, dependencies, and secrets.
- Embedded Semgrep into GitHub Actions CI/CD so that source-code security findings surface during development rather than at the end of the cycle.
- Operate a multi-channel analysis workflow (CI/CD pipelines, local repository scans, and platform dashboards) to investigate findings from both automated and manual perspectives.
- Connected Snyk, Semgrep, and SonarQube dashboards to provide centralized visibility into findings, affected code locations, and remediation requirements for engineering teams.
- Conduct Software Composition Analysis (SCA) to identify vulnerable and outdated third-party packages and assess real-world security impact on the application.
- Run Gitleaks against repositories and full Git history to detect and eliminate accidentally exposed secrets and hardcoded credentials.
- Lead threat modelling exercises using Threat Dragon, Data Flow Diagrams, and STRIDE — mapping trust boundaries, abuse cases, and required security controls across application components.
- Execute targeted API and application testing for BOLA/IDOR, broken access control, injection, authentication weaknesses, and business-logic flaws.
- Manually validate automated findings, accurately separate true positives from false positives, and deliver clear, actionable remediation guidance to developers.
- Produce technical security reports that pinpoint affected code locations, explain security implications, and support developers through fix implementation.
- Perform structured remediation verification and retesting to confirm that security fixes fully address identified issues.
- Leverage AI-assisted workflows for rapid code comprehension, research, test-case development, and documentation while independently verifying every technical conclusion.

SELECTED SECURITY PROJECTS

ENTERPRISE MEDICAL RECORDS (EMR) — AUTHORIZED PENETRATION TEST

LimaviCTech Company · Nigeria

- Led an authorized penetration test of an Enterprise Medical Records application, evaluating runtime behaviour and the effectiveness of existing security controls.
- Performed comprehensive manual web application testing with Burp Suite, OWASP ZAP, SQLMap, and supporting reconnaissance tooling.
- Systematically assessed authentication, authorization, access control, session management, input handling, and core application functionality.
- Identified and validated multiple vulnerability classes including SQL Injection, Cross-Site Scripting (XSS), authorization weaknesses, sensitive-data exposure, and session-security flaws.
- Delivered proof-of-concept demonstrations and a formal security assessment report covering technical impact, business risk, evidence, and prioritized remediation recommendations.
- Supported the development team through remediation and conducted retesting to verify that all reported issues were properly resolved.

OWASP JUICE SHOP — FULL-STACK APPLICATION SECURITY ASSESSMENT

- Executed a complete security assessment combining SAST, SCA, DAST, manual penetration testing, and source-code review against a deliberately vulnerable application.
- Identified and validated SQL Injection, XSS, IDOR, and authentication weaknesses; mapped findings to OWASP Top 10 categories.
- Performed structured threat modelling with STRIDE and produced root-cause analysis with practical remediation guidance for each finding.
- Demonstrated end-to-end DevSecOps integration by embedding Semgrep and Snyk into GitHub Actions CI/CD for automated security analysis.

OFFENSIVE SECURITY ASSESSMENT — HACKSECURE

[Cybersecurity Intern – Offensive Security · Remote · 2023 – 2024](#)

- Conducted web application penetration tests aligned with the OWASP Web Security Testing Guide (WSTG), covering reconnaissance, attack-surface discovery, and manual vulnerability validation.
- Tested authentication, authorization, access control, input validation, and business logic; produced findings with proof-of-concept evidence, risk ratings, and remediation recommendations.
- Utilized Burp Suite, OWASP ZAP, Nmap, SQLMap, and related tools; performed remediation verification after security fixes were applied.

PROFESSIONAL TRAINING

Web Application Penetration Testing · Application Security Testing & Debugging · OWASP Top 10 · Ethical Hacking Fundamentals · Offensive Hacking

EDUCATION

Certificate in Medical Laboratory Technology — College of Health Sciences and Technology, Ijero-Ekiti · 2017

ADDITIONAL INFORMATION

Languages: English, Yoruba, Nigerian Pidgin · **Focus:** Application Security · Web & API Security · Secure Code Review · Penetration Testing · DevSecOps · Vulnerability Research