

FRANK ONYEIGWE

APPLICATION SECURITY | PENETRATION TESTING

Lagos, Nigeria • frankchidiebere96@gmail.com • +234 810 313 6388 • [GitHub](#) • [LinkedIn](#)

PROFILE

Application Security professional focused on manual penetration testing of web applications and APIs, with hands-on experience identifying authentication, authorization, business logic, and OWASP Top 10 vulnerabilities across Vulnerability Disclosure Programs and lab environments. Skilled in leveraging industry-standard tools such as Burp Suite, Metasploit, and Nmap. Committed to identifying critical vulnerabilities and delivering clear, actionable remediation strategies.

SKILLS

- Threat Modeling and Risk Assessment.
- Web Application Penetration Testing.
- Manual Vulnerability Validation.
- OWASP API Security and Web Application Top 10 Vulnerabilities Testing.
- Vulnerability Report Writing.
- Remediation Guidance.
- Clear Communication, Team Collaboration, and Adaptive learning.
- Operating Systems: Windows, Kali Linux, Parrot OS.
- Web Proxies: Burp Suite, Caido.
- Scripting and Automation: Python, JavaScript, Metasploit.
- Open Source Intelligence (OSINT): Shodan, Google Dorks.
- Network Analysis: Nmap, Wireshark, Netdiscover.

PROFESSIONAL EXPERIENCE

Bugcrowd

July 2026 - Present

Position: Security Researcher

- Identified business logic vulnerabilities in financial, healthcare, and e-commerce workflows, including price manipulation and authentication bypass scenarios, and documented real-world business impact for triage and remediation.
- Performed manual security testing on enterprise web applications and APIs within authorized Vulnerability Disclosure Program (VDP) scopes, identifying and reporting high-priority issues including Broken Object Level Authorization, broken authentication, insecure API endpoints, and authorization bypass conditions.
- Validated the effectiveness of organizational security controls by testing against the OWASP Top 10 framework, identifying and reporting security weaknesses within authorized program scope.

Position: Web Security Apprentice

- Executed technical assessments on web application architecture to verify the effectiveness of security controls against unauthorized access and data leakage.
- Analyzed 20+ web vulnerability categories, including SQL injection, IDOR, OTP bypass, XSS, access control flaws, and business logic vulnerabilities, assessing exploitability, impact, and risk across lab environments.

PROJECTS

ShadowScout – Automated Recon and Risk Scoring Engine | [View on Github](#)

- Engineered an asynchronous Python-based reconnaissance engine designed to automate the discovery of sensitive endpoints and file leakage detection.
- Implemented a custom Risk Scoring Algorithm that weighs findings based on severity (Critical to Informational) of exposures like .env files and AWS credentials, enabling analysts to prioritize remediation efforts.
- Developed a Deep Intelligence Mode that parses client-side JavaScript to extract API endpoints and referenced hostnames, expanding application attack-surface visibility.
- Standardized audit workflows by generating structured JSON reports.

Security Assessment and Account Takeover Prevention | [View on LinkedIn](#)

- Assessed an intentionally vulnerable web application and REST API, investigating access-control and authentication weaknesses across account-management and password-reset workflows.
- Reproduced a Broken Object Level Authorization (BOLA/IDOR) vulnerability in a controlled lab to demonstrate unauthorized access to resources belonging to other users.
- Evaluated password-reset security controls, including OTP validation, token expiration, replay resistance, and server-side authorization enforcement.
- Implemented remediation measures, including resource-level authorization checks and single-use reset tokens.

EDUCATION

University of Nigeria, Nsukka

Sept 2016 - Nov 2022

Bachelor of Agriculture (B.AGRIC)

- Second Class Honours (Upper Division)

CERTIFICATIONS AND TRAINING

OffSec Certified Professional (OSCP)

(In Progress)

Certified Cybersecurity Educator Professional (CCEP)

Junior Penetration Tester (TryHackMe)

Cybersecurity Professional (Google)