

SEYI ISREAL ADEBOYE

Penetration Tester

✉ adeboyeisrael839@gmail.com ☎ 08149286915 📍 Oyo State, Nigeria
🌐 linkedin.com/in/seyi-adeboye 🐙 github.com/Adeboye839

Professional Summary

First-Class graduate in Cybersecurity and practicing penetration tester specializing in application security, API testing, and network/Active Directory penetration testing. Hands-on experience across 10+ authorized black-box and grey-box engagements on fintech and payments platforms, uncovering critical vulnerabilities including BOLA/IDOR, authentication bypass, hardcoded secrets, and cloud misconfigurations. Skilled with Burp Suite, OWASP ZAP, Nessus, and Metasploit. Maintain a custom offensive-security toolchain, including an AI-orchestrated pentesting pipeline (HexStrike AI MCP + Claude), and has taught ethical hacking and penetration testing fundamentals to students and professionals.

Professional Experience

Penetration Tester & Security Researcher , <i>Smartcomply Technology Solution</i>	Present
• Conducted end-to-end authorized black-box penetration tests on fintech and payments platforms, combining manual testing in Burp Suite Professional with an AI-orchestrated recon and exploitation pipeline (HexStrike AI MCP). • Identified and reported critical/high-severity vulnerabilities including unauthenticated PII exposure, BOLA on OTP verification endpoints, missing rate limiting, hardcoded API keys, unauthenticated S3 file upload, and CORS misconfigurations reflecting arbitrary origins with credentials. • Flagged and escalated a client-controlled privilege-escalation vector (role-manipulation via request cookie) for priority remediation follow-up. • Performed static and dynamic analysis of Android banking applications (Flutter and native), uncovering debug certificates in production builds, hardcoded backend environment configs, and missing SSL pinning. • Delivered formal, CVSS/CWE-mapped pentest reports (DOCX) with prioritized remediation guidance, and conducted revalidation engagements to confirm client fixes. • Tuned vulnerability scanning strategy (Nuclei, Nmap, ffuf) to operate reliably against WAF/CDN-protected targets while minimizing detection and false positives.	
Cybersecurity Instructor , <i>POOLOT Academy</i>	Present
• Teach cybersecurity fundamentals to students and early-career professionals, covering offensive security concepts, tooling, and safe/legal testing practice. • Delivered a technical talk on breaking into offensive security, covering personal recon methodology and real-world findings from professional engagements.	
Cybersecurity Instructor , <i>Deejoft Technologies</i>	04/2025
• Delivered instruction on ethical hacking, penetration testing, and network defense to students ranging from beginners to professionals. • Designed and facilitated hands-on labs covering password attacks, web application security, network scanning, OSINT, and social engineering. • Guided students in using Kali Linux tools such as Metasploit, Wireshark, Nmap, Burp Suite, and John the Ripper in realistic attack and defense scenarios.	

Cybersecurity Hackathon, NITDA (SECDOJO Platform)

07/2025 – 07/2025

Participated in a national-level cybersecurity challenge organized by the National Information Technology Development Agency; ranked among the top 6 professionals.

Cybersecurity Intern, Securesphere Foundation

09/2024 – 12/2024

Researched and reported emerging cybersecurity threats, contributing to the foundation's threat intelligence framework.

Remote

Education

B.Tech Cybersecurity, Ladoke Akintola University of Technology (LAUTECH)

2021 – 2026

- First-Class Honours (CGPA: 4.69)
- Relevant coursework: Cybersecurity Fundamentals, Introduction to Digital Forensics, Network Security, Web Application Security, Secure Software Development, Risk Management and Incident Response.

Ogbomoso, Oyo State,
Nigeria

Core Skills

Web & API Security

OWASP Top 10 & API Top 10, BOLA/IDOR, authentication & session flaws, OTP/rate-limit bypass, CORS misconfiguration, JWT attacks, race conditions, broken access control, input validation flaws

Mobile Security

Android/iOS static & dynamic analysis, Flutter/Dart AOT reversing, SSL pinning bypass, MobSF, Frida, Objection, drozer

Tooling

Burp Suite Professional, OWASP ZAP, Nessus, Metasploit, Nuclei, Nmap, ffuf, subfinder, dnsx, httpx, katana, jsluice, HexStrike AI MCP, custom recon.sh automation pipeline

Programming

Python and Bash scripting for PoCs and automation

Network & Active Directory

Domain enumeration, privilege escalation, lateral movement, GPO assessment, Kerberos attacks, network scanning

Cloud & Infrastructure

S3 misconfiguration, hardcoded credentials/API key discovery, Terraform state exposure, container/DevOps misconfig review

Reporting

CVSS/CWE-mapped formal reporting, executive summaries, remediation tracking & revalidation, Python/Node.js report tooling (python-docx, docx.js)

Selected Engagements

Fintech Platform (Business Banking)

Full black-box assessment; 9 findings including BOLA, unauthenticated PII exposure, and OTP brute-force vectors.

Payments Infrastructure Platform

14 findings including hardcoded API key, unauthenticated S3 file upload, and CORS misconfiguration.

Consumer Fintech Platform (Clerk-based auth)

Identified CORS infrastructure misconfiguration, weak password policy settings, and potential IDOR on sign-up objects.

Cross-Border Payments Platforms

Identified and later revalidated findings spanning CORS misconfiguration, token failures, exposed TOTP secrets, and account-destruction race conditions.

Food-Delivery & Mobile Banking Apps

Hardcoded API keys, IDOR chains, admin route exposure, and mobile SSL pinning gaps.

E-Commerce Platform (ShopyDash, freelance client)

Authorized security assessment identifying and validating input validation flaws and broken access controls; delivered a structured report with executive summary, PoC evidence, and prioritized remediation guidance, followed by post-remediation validation testing.

Bug Bounty & CTF

Bug Bounty Testing

Participated in bug bounty testing on a major digital wallet/payments platform via the YesWeHack and Hackerone platform.

WebverseLabs CTF

Active CTF competitor; completed WebverseLabs challenges spanning SQL injection, GraphQL BFLA, and git history secret exposure.

MetaCTF Cybersecurity Competition, *Remote*

Tackled challenges in web application security, API testing, cryptography, and reverse engineering; identified and exploited vulnerabilities in simulated environments using OWASP ZAP, Burp Suite, and custom scripts.

Cloud-focused Pentest Labs (HackSmarter)

Completed cloud-focused pentest labs (HackSmarter), including Terraform state file exposure, AWS S3 credential leakage, and a Rocket.Chat RCE chain (CVE-2021-22911).

Projects

LAUTECH Cyber Risk Sentinel

Degree thesis: a Python/Flask hybrid cyber-risk scoring system combining a Random Forest classifier with rules-based scoring and Isolation Forest anomaly detection, including a phishing simulation module and multi-tab analyst dashboard.

Vulnerability Assessment and Exploitation Lab (Metasploitable Home Lab)

Designed and implemented a home lab using Metasploitable 2 to practice ethical hacking and vulnerability assessment; performed vulnerability scans with Nessus and OWASP ZAP, simulated real-world attacks (SQL injection, remote code execution, weak password policies), used the Metasploit Framework to craft exploitation payloads, and documented findings with remediation plans.

Certifications

- | | | |
|--|---|--|
| • Certified Application Security Practitioner (CAP) — The SecOps Group | • Certified Network Security Practitioner (CNSP) — The SecOps Group | • Certified in Cybersecurity (CC) — ISC2 |
| • Practical Web Application Security — TCM Security | • Web Application Penetration Tester — TryHackMe | • Junior Penetration Tester — TryHackMe |