

Ibrahim Abdulqadir

Cybersecurity Engineer · Offensive Security · AI Security Automation

your@email.com · github.com/IbrahimAbdulqadir · hackerone.com/himdir · linkedin.com/in/ibrahim · Abuja, Nigeria

PROFESSIONAL SUMMARY

Cybersecurity engineer with a B.Sc. in Cyber Security from Bayero University Kano and hands-on experience across offensive security, defensive tooling, and AI-driven attack automation. Proven ability to design and ship production-grade security tools — from autonomous penetration-testing agents to network vulnerability scanners and smart-contract auditors — that reduce manual effort and surface actionable findings. Active on HackerOne and experienced in real-world security engagements including a paid university portal assessment. Equally capable in red-team and blue-team contexts, with growing expertise in SIEM development and AI agent pipelines for security automation.

CORE COMPETENCIES

- | | | |
|---|--|--|
| ■ Penetration Testing (Web / Network / API) | ■ AI Agent Development & LLM Orchestration | ■ Intrusion Detection Systems (Snort / NIDS) |
| ■ Smart Contract Auditing (Web3 / Solidity) | ■ SIEM Development & Log Analysis | ■ Bug Bounty Hunting (HackerOne) |
| ■ Vulnerability Research & CVE Analysis | ■ Phishing Detection & ML Classifiers | ■ Security Report Writing & Client Delivery |

PROJECTS & ENGINEERING WORK

RedMind — Autonomous AI Pentesting Agent

2024 – Present

Independent Project · Python, GPT-4o, Flask

- Architected a 14-module offensive security agent orchestrated by GPT-4o, covering recon, injection, auth bypass, IDOR, XSS, CSRF, and more.
- Engineered a canary-based false-positive detection engine that cut noise from 12+ false flags to near-zero on modern SPA targets.
- Validated against OWASP Juice Shop and live engagement targets; auto-generates structured PDF findings reports.
- Modular tool-registry design allows new attack modules to be added without touching the core agent loop.

IDOR Hunter — Authenticated Access-Control Scanner

2024

Independent Project · Python, Session Auth, BurpSuite

- Built a purpose-built authenticated IDOR hunting tool that logs in with real session credentials and maps all object-ID-bearing endpoints.
- Systematically swaps IDs across privilege levels to surface broken access control — optimised for bug bounty engagements where authenticated scanners outperform broad ones.
- Successfully surfaced confirmed IDOR findings across multiple HackerOne program scopes.

Web3Shield — Smart Contract Pentesting Framework

2024

Independent Project · Python, Solidity, Slither, web3.py

- Developed an Etherscan-based crawler with transparent proxy detection and external dependency mapping.
- Integrated Slither static analysis with a normalised output layer for access-control and re-entrancy auditing.
- Produces structured vulnerability reports consumable by both technical and non-technical stakeholders.

AI PhishDec — Phishing Detection Classifier

2023 – 2024

Independent Project · Python, scikit-learn, Flask

- Trained a Random Forest classifier on ~391,000 real phishing domain records, achieving high-confidence classification.
- Deployed a Flask dashboard for live URL classification with PDF report export for client delivery.

NetRecon Pro — Network Vulnerability Scanner

2023

Independent Project · Python, Nmap, NIST NVD API

- Automated network sweep and CVE correlation pipeline integrating Nmap with the NIST NVD REST API.
- Matched discovered open services against known CVEs and generated client-ready PDF reports per scan.
- Implemented a dynamic IP-restriction security layer to prevent unauthorised scanner use.

SIEM Tool Development

2023 – 2024

Independent Project · Python, Log Analysis, Alerting

- Designed and implemented a custom SIEM solution for aggregating, correlating, and alerting on security events across network infrastructure.
- Built real-time alerting pipelines and dashboards for threat visibility in resource-constrained environments.

BUG BOUNTY & SECURITY RESEARCH

HackerOne — Bug Bounty Hunter

2023 – Present

Handle: himdir · hackerone.com/himdir

- Active participant across multiple HackerOne programs with a focus on authentication vulnerabilities, IDOR, and access-control flaws.
- Conducted structured recon phases using custom tooling; built prioritised attack-surface maps before testing.
- Engaged Coupang TW program scope of 44 web subdomains with phased recon plan and authentication vulnerability checklist.
- Performed a paid security assessment of a university web portal, delivering a structured findings report.

EDUCATION

B.Sc. Cyber Security

2020 – 2024

Bayero University Kano · Kano, Nigeria

Final Year Project: Network Intrusion Detection System (NIDS) using Snort — designed, configured, and validated a real-time intrusion detection pipeline capable of identifying common network-layer attacks including SYN floods, port scans, and signature-based threats.

TECHNICAL SKILLS

Languages	Python, JavaScript, Bash / Shell, Solidity, SQL
Frameworks & Tools	Flask, Next.js, Nmap, Slither, BurpSuite, Snort, Metasploit
AI / ML	LLM Orchestration (GPT-4o), scikit-learn, Random Forest, Agent Design
Security	Web App Pentesting, Network Security, Smart Contract Auditing, SIEM, IDS/IPS
Platforms	Linux (Kali), Git, GitHub, NIST NVD API, Etherscan API, HackerOne
Reporting	PDF Report Generation (ReportLab), Structured Finding Templates, Client Delivery