Nikunj Miglani

+91 9519517579 | niikkunjmiglani@gmail.com | LinkedIn | GitHub | Portfolio

Summary

Cybersecurity-focused CS undergraduate who builds **security automation tools, web vulnerability scanners, and production-grade full-stack systems**. Engineered a scanner covering 7+ attack classes with CVE mapping and automated risk scoring, and shipped platforms for paying freelance clients. Seeking **SOC analyst, security engineering, and infrastructure/IT** roles.

Education

- **SRM Institute of Science and Technology** — Uttar Pradesh, India
  B.Tech in Computer Science (Cyber Security Specialization) — Aug 2024 – Jul 2028
  CGPA: 8.3/10

Experience

Freelance Full-Stack Developer — 2025 – Present

- Shipped a full-stack **placement consultancy platform** for a paying client – multi-step onboarding, candidate dashboard, admin panel – using **Next.js, NeonDB, Prisma, NextAuth**; taken from requirements to production.
- Delivered a **business website for an interior design firm** on Sanity CMS, Next.js 14, and TailwindCSS, giving the client self-service control over portfolio and content.

Projects

VulneraScan – Automated Web Vulnerability Scanner — 2025
GitHub

- Built a Python scanner that crawls target applications and injects payloads across discovered parameters to detect **7+ vulnerability classes**: SQLi, XSS, command injection, SSL/TLS misconfigurations, insecure headers, and exposed ports.
- Integrated **Nmap port scanning, CVE mapping, automated risk scoring, and PDF report generation**, replicating a real-world vulnerability assessment workflow end-to-end.

Quizzkr – Secure Quiz Platform — 2026
Live

- Architected a full-stack exam platform (Next.js, PostgreSQL, Prisma, NextAuth) with **role-based access control, secure session management, and bcrypt password hashing** for authenticated exam sessions.
- Engineered **behavioral anti-cheat monitoring** – tab-switch detection, fullscreen enforcement, timer controls, real-time suspicious-activity logging – to preserve exam integrity.

Home SOC Lab – SIEM Detection & Threat Enrichment — 2026
GitHub

- Deployed a **Wazuh SIEM** home lab with custom detection rules for SSH brute-force and sudo privilege-escalation attempts, validated against live, self-simulated attacks mapped to **MITRE ATT&CK**.
- Built a Python **threat intelligence enrichment** pipeline to automatically annotate raw alerts with IOC context, cutting manual triage effort.

Certifications & Training

- **CCNA (Cisco Certified Network Associate)** – In Progress
- **TryHackMe** – SOC Analyst Learning Path
- Hands-on practice with **Metasploitable, Kali Linux, Burp Suite, Nmap, Metasploit, and Wireshark**

Achievements

- Cleared **Smart India Hackathon (SIH) 2025** Internal Round with a blockchain supply-chain traceability solution.
- Responsibly disclosed a **privilege escalation vulnerability** on a Govt. of Kerala website via **CERT-In**.

Technical Skills

Languages: Python, C/C++, JavaScript, SQL, Solidity

Cybersecurity: Vulnerability Assessment, SIEM, Incident Response, MITRE ATT&CK, Intrusion Detection, Web Security, Network Security, Applied Cryptography

Security Tools: Nmap, Wireshark, Burp Suite, Metasploit, Hydra, Scapy

Dev Stack: Next.js, Node.js, FastAPI, LangChain, Prisma, PostgreSQL, MongoDB, TailwindCSS

Platforms & Concepts: Linux, Kali Linux, Git, TCP/IP, OSI Model, OOP, DBMS, Operating Systems, Computer Networks