Nakul Kokate

Pune, Maharashtra | kokatenakul11@gmail.com | LinkedIn | github.com/Naks-bro | github.com/chamyachinu-bit

Professional Summary

Cybersecurity undergraduate graduating in July 2027 with a 5th-place finish among 700+ Capture the Flag participants and internships in enterprise endpoint security and cybercrime investigation. Build Windows detection, read-only AWS auditing and investigation prototypes using C#/.NET, Python and TypeScript. Document technical findings, evidence, access controls and remediation.

Education

Symbiosis Skills & Professional University (SSPU) — Expected July 2027
B.Tech, Computer Science & IT (Cyber Security) · Current CGPA: 9.0/10 — *Pune, India*

Pimpri Chinchwad Polytechnic College — 2021–2024
Diploma, Computer Engineering · 84.63% — *Pune, India*

CTF, Security Recognition & Disclosure

DY Patil CTF 2024: Ranked 5th of 700+ participants; worked through OSINT, digital forensics, cryptography and steganography challenges.

Seasides Information Security Conference 2026: Received a merit scholarship with travel and accommodation support for the Goa event.

Responsible disclosure: Reported three security findings across enterprise and academic environments through responsible channels; documented impact and remediation at a public-safe level.

Bharat Innovation Challenge 2025–26: National top 50. **Smart India Hackathon 2026:** Selected in the college internal round.

Security Experience

Cybersecurity Research Intern — Konecranes — Jun–Jul 2025
Enterprise endpoint security · Pune, India

- Investigated endpoint controls with Cortex XDR and Qualys; identified and responsibly escalated an endpoint privilege-escalation finding.
- Prepared reproduction, impact and remediation documentation for security and IT teams.

Cyber Crime Branch Intern — Pune Police — Jun 2025
Investigation support · Pune, India

- Supported phishing and financial-fraud casework through preliminary evidence review, complaint documentation and pattern analysis across related reports.

Selected Security Projects

RDRS — Ransomware Detection & Response Service | *C#/.NET 8, ETW, WMI, PowerShell* | GitHub — 2025–2026

- Developed a Windows defensive agent combining seven file, process, crypto-API, shadow-copy and network signals into a per-process 0–100 risk score; used decoy files and entropy analysis to identify suspicious encryption activity.
- Implemented configurable suspension, process-tree termination, execution restriction, Defender scan requests and structured JSON alerts; documented PowerShell scenarios for normal and suspicious file activity.
- Mapped detection scenarios to MITRE ATT&CK techniques T1486, T1490 and T1071; treated false-positive control as a design constraint rather than claiming production detection rates.

CloudPosture — AWS Security Posture Scanner | *Python, Boto3, pytest/moto* | GitHub — 2026

- Built a read-only scanner with 26 CIS AWS Foundations-aligned checks for IAM, S3, EC2/EBS and CloudTrail; a Boto3 API guard blocks write calls, while findings show actual versus expected state and remediation guidance.
- Separated failed, unavailable and not-applicable results from passes; built CSV/JSON exports and a Streamlit dashboard, with 74 pytest/moto tests against simulated AWS accounts.

Crime Branch OS — Investigation Workspace | *FastAPI, PostgreSQL, NetworkX, Next.js* — 2025–2026

- Developed a prototype for case records, entity relationships, cross-case identifier search and graph-path review; intake previews let an investigator verify mappings before import.
- Recorded source-file hashes and custody events, with optional AI-extracted links held for officer review. Used synthetic demonstration records; this is not a deployed police system.

TISAP — Threat Intelligence & Security Awareness Platform | *React, Next.js, FastAPI* | GitHub | Interactive demo

- Built Admin, HR and Employee training views with phishing, browser-security and malware-response labs, quizzes and progress tracking; a separate FastAPI analytics prototype collects simulated Chrome, Windows and Outlook security events.

GhostNet-X — Adaptive Deception Prototype | *Node.js, Express, Supabase* | GitHub

- Implemented a Node/Express honeypot that scores SQL injection, XSS, command-injection, traversal and scanner probes; routes requests to normal, monitored or decoy views and logs events to Supabase for a SOC-style dashboard.

Threat-Intel IAM Attack-Path Verifier | *Python, FastAPI, graph search* | GitHub

- Created a fixture-only FastAPI slice that matches approved rules to synthetic IAM graphs; bounded breadth-first search prevents cycles and caps hops, expansions and time. Six synthetic cases exercise evidence-grounded findings; no live AWS policy simulation.

Applied Security Engineering

Technology Intern — Syrma SGS Technology Ltd. Jun–Oct 2026

- **Purchase Requisition Workflow:** Built a Next.js/TypeScript and MS SQL Server approval application supporting an SAP S/4HANA procurement process, scoped for 20+ users, with role-based routing and audit history; worked on Entra ID/OIDC sign-in requirements and documented DNS, TLS and firewall configuration.

Full-Stack Developer (Freelance) — Arkoun Farms Feb 2025–Present

- **Arkoun Operations Portal:** Built a Next.js/Supabase platform for ordering, dispatch, inventory and billing across nine roles; implemented PostgreSQL Row-Level Security, server-side authorization and transaction-safe inventory and payment workflows.

Technical Lead, Platform & Automation (Volunteer) — YGPT Jul 2025–Present

- **Event Management System:** Built an eight-role Next.js/Supabase platform with approvals, budgets and reporting; applied PostgreSQL RLS and Google Apps Script automation for Drive folders and email notifications.

Additional Computer Science Projects

JeevanSetu Wearable Safety Lab | *ESP32, Wokwi, Python/Flask, SQLite*

- Contributed to a five-device simulated SOS and fall-alert lab linking ESP32 events to Flask/SQLite incident timelines, deduplication, notification retries and caregiver acknowledgement; no physical or medical validation.

Arkoun Order & Delivery Automation | *Google Apps Script, JavaScript, ORS API*

- Converted order exports into vendor orders and dispatch sheets; used road-duration matrices, Clarke–Wright savings and 2-opt route refinement to prepare delivery plans within the Arkoun engagement.

Arkoun Hydroponics Explorer | *Blender, GLB, JavaScript* | Demo

- Built a browser-based inspection experience for five 3D system layouts and 32 viewpoints, with assembled/exploded views and controlled animation playback; engineering dimensions are illustrative.

YGPT Public Website | *HTML, CSS, JavaScript, Vercel, Supabase* | Site

- Developed responsive organization pages and an events view backed by a serverless API that filters approved public records.

VACS Organization Website | *HTML, CSS, JavaScript* | GitHub | Live site

- Delivered a dependency-free responsive site with accessible navigation, reduced-motion behavior and a content-gated launch structure.

Parivaar Parivartan Bilingual Report Tool | *HTML, JavaScript, JSON*

- Built an English/Hindi report editor with stable content IDs, autosave, fallback rendering and checks for missing or duplicate translations; packaged local and server-based editing paths.

Desktop File Manager | *Python, Tkinter* | GitHub

- Built file navigation, sorting, search, tagging and file-operation modules in a desktop interface.

Nakul Focus System | *Python, SQLite, Flask* | GitHub

- Built a local CLI and browser dashboard for focus sessions, habits and reminders; added reversible hosts-file website blocking with an administrator check.

Shopat E-Commerce Front End | *HTML, CSS, JavaScript* | GitHub

- Implemented a storefront front end as an earlier web-development internship project.

Nakul Kokate Portfolio & Resume Site | *JavaScript, Three.js, Blender, Vercel* | Site

- Built a project-case directory and downloadable role-specific resumes around an accessible reading route and optional interactive 3D visual experiments.

Technical Skills

Security challenges: OSINT, digital forensics, cryptography and steganography (CTF); web authorization, endpoint telemetry, threat detection, evidence review, responsible reporting.

Tools and systems: Cortex XDR, Qualys, ETW, WMI, PowerShell, Wireshark, Burp Suite, Autopsy, FTK Imager, Ghidra, Linux, Git, Docker.

Programming and cloud: Python, C#/.NET 8, TypeScript, SQL, FastAPI, PostgreSQL/Supabase, AWS IAM/S3/EC2/CloudTrail, Boto3, REST APIs, OAuth/OIDC, RBAC/RLS.