Hitesh Chandak

Software Engineer (Backend) | Python, FastAPI, AWS
Nagpur, Maharashtra, India (open to relocation) | +91-9503201370 | chandakhitesh77@gmail.com
github.com/itachi2112-Tsukuyomi | linkedin.com/in/hitesh-chandak-750a18258 | Portfolio | LeetCode | Codolio

Professional Summary

Final-year Computer Engineering student building backend services with **Python and FastAPI**: **REST APIs**, **JWT/OAuth2 authentication**, and **AWS automation** with boto3 and Terraform. Brings a security-first approach to API and cloud design (CTF All India Rank 37). Seeking **SDE / Backend Engineer** roles.

Education

Shri Ramdeobaba College of Engineering and Management, Nagpur Aug 2023 – 2027 (Expected)
B.Tech in Computer Engineering (Cyber Security) | CGPA: 7.58/10 | Latest SGPA: 8.5
Relevant Coursework: Data Structures & Algorithms, OOP, DBMS, Operating Systems, Computer Networks

Technical Skills

- **Languages:** Python, SQL, Bash
- **Backend:** FastAPI, RESTful APIs, JWT / OAuth2 Authentication, Pydantic, OpenAPI / Swagger
- **Databases:** PostgreSQL, SQLite
- **Cloud & DevOps:** AWS (S3, IAM, CloudTrail, boto3), Terraform (IaC), Docker, Git, GitHub, Linux
- **ML & Data:** PyTorch, Streamlit

Projects

CloudSnare – AWS Honeypot & Attack Detection Platform View on GitHub
Tech Stack: Python, FastAPI, AWS (boto3, CloudTrail, IAM), Terraform, SQLite
- Final-year team project: a platform that detects exposed AWS resources, deploys realistic decoys beside them, and alerts on attacker interaction.
- Built a **boto3** scanner covering 6 AWS services with snapshot-and-diff change detection.
- Automated decoy deployment (including deny-all honeytoken IAM keys) with **Terraform (Infrastructure as Code)** and correlated **AWS CloudTrail** logs to capture attacker activity.
- Generated **MITRE ATT&CK**-mapped incident reports via the **Claude API**, served through a **FastAPI** REST backend; validated end-to-end with a scripted attack simulation on live AWS.

Phishing Link Analyzer View on GitHub
Tech Stack: Python, PyTorch, Streamlit, Pyshark
- Trained a **PyTorch 1D-CNN** to classify phishing URLs with **88% accuracy** on 2,100+ URLs from PhishTank and OpenPhish, served through an interactive **Streamlit** dashboard.
- Implemented live packet capture with **Pyshark** to inspect DNS/HTTP traffic, score domain risk in real time, and trigger automated alerts.

S3 Bucket Security Scanner View on GitHub
Tech Stack: Python, boto3, AWS S3
- Built a **boto3**-based scanner that detects public and misconfigured S3 buckets by checking anonymous access, ACLs, and bucket policies, and generates severity-ranked reports.

SecureAuth API – User Authentication & Management Service
Tech Stack: Python, FastAPI, Pydantic, JWT, OAuth2
- Developed RESTful CRUD endpoints in **FastAPI** with Pydantic request/response validation and auto-generated **Swagger** docs.
- Secured routes with the **OAuth2 password flow and JWT access tokens** (creation, verification, expiry); managed secrets via environment-based configuration.

Experience

Crypto Forensic and Technology (CFT) | Digital Forensics Intern June 2025 – July 2025
Nagpur, India
- Performed forensic acquisition and analysis of compromised storage media using **Autopsy** and **FTK Imager**, recovering deleted artifacts under chain-of-custody procedures.
- Documented findings in structured case reports identifying indicators of malicious activity.

Achievements & Certifications

- **Problem Solving:** Solved **275+ problems** on LeetCode, HackerRank, and GeeksforGeeks across arrays, hashing, two pointers, trees, graphs (DFS/BFS), backtracking, and dynamic programming.
- **REDFOX CTF:** Secured **All India Rank 37** among 400+ teams; also competed in **CyberStorm 2025**, Mumbai.
- **Leadership:** Coordinated **ByteBreak CTF** and trained **50+ peers** through College Cyber Security Club workshops.
- **Certifications:** Zscaler Zero Trust Certified Associate (ZTCA), Certified Cyber Forensic Examiner (CCFE), Google Cloud Computing Foundations