Anshik Singh

Bengaluru, Karnataka, India
+91-8278187062 | anshikthind@gmail.com | linkedin.com/in/anshik-singh | github.com/anshiq | anshik.in

Education

Chitkara University — Chandigarh, India
Bachelor of Technology in Computer Science & Engineering — *2022 – 2026*
- **CGPA**: 9.1 / 10.0

Experience

Devops Intern — June 2026 – Present
Leadrat: AI Real-Estate CRM – Spring Boot, PostgreSQL, Docker, Linux, Java, AWS — *Onsite (HSR, Bengaluru)*
- Hardened Docker images and container configs for develop/staging/production environments, reducing attack surface by removing unnecessary packages and enforcing non-root container execution.
- Reviewed IAM roles and AWS resource policies for least-privilege access across environments, flagging and remediating over-permissioned service roles.
- Audited CI/CD pipelines (GitHub Actions) and environment configs for exposed secrets and credentials, integrating secret-scanning checks into the deployment workflow.

Software Engineer Intern — May 2025 – April 2026
Silverpush: AdTech Platform - Nodejs, React, Reactflow, Langchain, Langgraph, Microservices, AWS — *On-site (Gurugram)*
- Built **Zimmer**'s **campaign journey architecture** with **WebSocket event-driven architecture** to support dynamic, real-time campaign execution logic and **error validations** for nodes throughout the campaign journey creation on frontend.
- Engineered **RESTful analytics APIs** to process real-time data, building **PostgreSQL-backed pipelines** for reach metrics and **LLM token cost tracking**, enhancing cost visibility and decision-making during campaign execution.
- Developed a **LangGraph**-based stateful **agent orchestration** layer to power AI-driven decision nodes (categorization, evaluation, summarization) inside the campaign journey engine, enabling **conditional branching**, sub-flow composition, and automatic retry/fallback recovery across multi-step agent workflows.
- Implemented a **Retrieval-Augmented Generation (RAG)** pipeline that chunks, embeds, and indexes multi-source knowledge bases (PDFs, web pages, Q&A pairs) into a **vector store**, enabling grounded **semantic search** and reducing hallucinated output in AI-generated campaign content.

Security Projects & CTF

FAM CTF – FamPay Security Challenge | *Android Reverse Engineering, Web, Cloud/AWS* — 950+ pts
- Reverse-engineered an Android APK's native ARM/x86_64 libraries with `apktool`, `strings`, and `objdump`, manually decoding an XOR-obfuscated runtime algorithm from disassembly to recover a hidden Firebase App Check debug token.
- Exploited a Firebase Realtime Database misconfiguration by using the Identity Toolkit REST API to obtain an anonymous auth JWT, bypassing an `auth != null` security rule to read protected data.
- Bypassed Firebase App Check attestation end-to-end by exchanging a reverse-engineered debug token for a signed App Check JWT and using it to query Firestore directly via REST.
- Forged a JWT with an `alg:none` header to escalate privileges on a web portal, bypassing signature verification to gain unauthorized admin access to a protected admin panel.
- Chained an SSRF vulnerability in an internal webhook proxy with the EC2 IMDSv2 metadata service (bypassing an IP allow-list via the `instance-data` hostname alias) to steal temporary IAM credentials, then used `boto3` to generate presigned SigV4 URLs and exfiltrate a flag from a VPC-restricted S3 bucket.

Open Source Contributions

Metasploit Framework (Rapid7) | *Documentation Contribution*
- Submitted a documentation fix for the Android Meterpreter `reverse_tcp` payload module, adding setup guidance and resolving `msftidy` validation errors – PR #16342.

Technical Skills

Languages: Python, Java, JavaScript, Bash
Security Tools: Burp Suite, apktool, apkleaks, objdump, readelf, Nmap, Postman
Cloud & DevOps: AWS (IAM, EC2, S3), Docker, GitHub Actions, Linux, Firebase
Concepts: OWASP Top 10, Mobile App Security (APK/native reversing), JWT/Auth vulnerabilities, SSRF, IMDS/Cloud misconfigurations, CI/CD security