HIMANSHU SONI

+91 94100 04994 | h30s.soni@gmail.com | github.com/h30s | linkedin.com/in/h30s | himanshusoni.vercel.app | leetcode.com/u/h30s

Education

KIET Group of Institutions (AKTU), Ghaziabad **Aug 2024 – May 2028 (Expected)**
B.Tech in Computer Science, CGPA 8.17/10

Experience

ResoluteX Technology Labs (Oxlo.ai) **Jul 2026 – Present**
AI Intern, OxCode AI coding agent (TypeScript, Python, FastAPI, PostgreSQL) *Remote, Dubai, UAE*

- Replaced prefix-based command auto-approval with a quote-aware shell parser, closing 6 bypass classes (chained commands, subshells, inline interpreters, package runners) in an agent that executes commands on user machines.
- Fixed task verification so blocked file writes and unverified test claims can no longer be reported as success, and stopped user-stated claims from being stored as durable agent facts.
- Scaled context handling for large monorepos with bounded context budgets, and built a tool for analyzing large build and runtime logs.
- Added secret redaction for tool output, and closed sensitive-file read bypasses across quoting, path normalization, and NTFS streams.
- Built Razorpay payments and anonymous trials across the FastAPI backend and VS Code extension: signature verification, webhooks, idempotent upgrades, and per-install and per-IP limits.

Waysorted Infotech Pvt. Ltd. **Mar 2026 – Jun 2026**
Full-Stack Developer Intern, Figma plugin (TypeScript, Node.js, Express, PostgreSQL) *Remote / Hybrid*

- Built HTML-to-Figma and Canva-to-Figma importers that produce editable frames, and an AI palette generator with contrast checks.

Open Source

60+ merged pull requests across 12 projects | All merged PRs

- **Google Gemini CLI** (TypeScript, 100k+ stars, 5 merged): Added an experimental LXC container sandbox and fixed MCP bugs where a name collision overwrote user config and restarts reused stale settings.
- **Mastra** (TypeScript, 29k+ stars, 2 merged): Fixed symlink path resolution for bubblewrap workspace mounts and recovery from model prefill errors.
- **Kubescape Kubevuln** (Go, CNCF, 7 merged): Fixed VEX data-integrity bugs in a Kubernetes CVE scanner, including non-deterministic SHA-256 fingerprints caused by Go map ordering.
- **Faust compiler** (C++, 16 merged) and **Palisadoes Talawa** (TypeScript, 21 merged): Compiler backend fixes and API rate limiting.

Projects

FitKalp, Multi-Tenant Gym SaaS with AI Assistant | github.com/h30s/fitkalp-web **2026**
Next.js 14, TypeScript, PostgreSQL, Prisma, Auth.js, Supabase

- Built an AI operations assistant with typed tool schemas, permission checks, and approval gates before any database write, inside a CRM used by 5+ gyms in early access.
- Designed tenant isolation with 42 PostgreSQL row-level security policies, covered by a suite of 278 automated tests.

Truvo, AI Product Data Platform | github.com/h30s/truvo **2026**
TypeScript, React, Express, PostgreSQL, Prisma, Redis, BullMQ, Claude API

- Turned supplier PDFs, scans, XLSX, and CSV files into structured product records using Claude tool calling, vision models for scans, and a rule-based fallback.
- Ran parsing in BullMQ workers; every value keeps its source file, page, and row, and conflicts go to human review.

Technical Skills

AI & LLMs: LLM agents, tool calling, MCP, context management, agent sandboxing, Claude API, vision extraction
Languages: Python, TypeScript, Go, C++, JavaScript, SQL
Backend & Data: Node.js, Express, FastAPI, REST APIs, GraphQL, PostgreSQL, Redis, BullMQ, Prisma
Frontend & Tools: React, Next.js, Tailwind CSS, Docker, LXC, Kubernetes, Linux, Git, GitHub Actions, Playwright

Achievements

- **5x Hackathon Winner:** Innotech'24 (1st of 100+ teams), ADK-TS 2025 MCP Expansion track (1st), Hacktivism II (2nd), OxBuild (2nd), Four.meme Sprint (3rd).
- **300+ LeetCode problems** (184 Medium, 33 Hard). Featured on Ministry of Education TV for engineering work.