Anugrah K

+91-95396-94902 | anugrah.k910@gmail.com | linkedin.com/in/anugrah-k | github.com/anugrahk21

Technical Skills

Languages: Python, C/C++, Java, SQL
Security Tools: Burp Suite, Wireshark, Nmap, Metasploitable
Frameworks & Platforms: Linux, Git, VMWare/VirtualBox, VS Code
AI & GenAI: Prompt Engineering, LLM Integration (Gemini API), AI-Assisted Development, AI Safety
Core Areas: Web App Security, Network Security, Penetration Testing, Research & Development
Soft Skills: Technical Documentation, Critical Thinking, Research & Analysis, Attention to Detail

Certifications & Training

AI Security & Governance Certification Jan 2026
Securiti *Securiti Education*
- Formalized expertise in Generative AI guardrails by mastering governance frameworks to secure model integration
- Implemented risk strategies ensuring compliance with global AI safety laws
- Applied safety measures (input filtering, sanitization) for secure agents

Google Cybersecurity Professional Certificate Oct 2025 - In Progress
Google *Coursera*
- Mastering threat detection and incident response by conducting hands-on labs with Linux
- Analyzing patterns to identify vulnerabilities using industry-standard tools
- Building practical experience for industry-recognized cybersecurity skills

AI Agents Intensive Training with Google Nov 2025
Google *Kaggle*
- Acquired expertise in agentic architecture (RAG, orchestration, tool-use) through Google-led labs
- Built and deployed AI agents covering models, orchestration, memory, and evaluation
- Deployed a functional agentic workflow for the final capstone project, earning a verified Kaggle achievement badge

Projects

Project Cerberus: The AI Iron Dome | *Python, FastAPI, Google Gemini API, AI-Assisted Dev* Nov 2025
- Engineered a secure AI reverse proxy with a fail-closed architecture to neutralize prompt injection attacks
- Implemented a 3-layer defense engine, achieving a 95%+ block rate against common jailbreak attempts like DAN
- Deployed threat detection pipelines using FastAPI to mitigate key OWASP LLM Top 10 data exfiltration risks

Password Security Tool | *Python, Cryptography, Regex* Sep 2025
- Developed a password analyzer that calculates a precise 0-100 strength score based on randomness and complexity
- Built a secure password generator using Python's secrets module to ensure strong, unpredictable credentials
- Integrated a simulated breach detection system to demonstrate real-world attacks exploit compromised credentials

Publications & Patents

Smart IoT Cookware System May 2025
Patent Application *Patent Filed*
- Architected an IoT induction system using a 10x10 electromagnet grid for pixel-level thermal control
- Designed event-driven logic processing real-time infrared data, reducing theoretical energy waste by 40%
- Specified hardware fail-safes and logic gates for immediate cutoff when temperatures exceed 250°C

Education

Lovely Professional University Aug 2023 – Present
B.Tech in Computer Science & Engineering (Cybersecurity) *Punjab, India*
- Current CGPA: 7.42

Kendriya Vidyalaya Keltron Nagar 2021 – 2023
Secondary (X) – 77% | Senior Secondary (XII) – 80% *Kerala, India*