

Anmol Chaudhary

✉ anmolchaudhary8317@gmail.com | 📞 +91 7453878899 | 🌐 anmolchaudhary01 | 📍 bustayaga

Objective

Aspiring Software Engineer with a Bachelor's degree in Computer Applications, seeking an entry-level opportunity in Software Development. Built academic projects involving web application development, system integration, and cloud-based security solutions, gaining practical exposure to building and securing software systems. Looking to apply this foundation toward writing clean, reliable code and growing within a collaborative engineering team.

Skills

- **Programming & Tools:** Python, Bash, SQL, Git, Salesforce Service Cloud, Genesys Cloud CX
- **Infrastructure & Cloud:** Microsoft Azure, Linux (Kali/Ubuntu), Windows Server, Active Directory, Docker, VMware/VirtualBox, SSH
- **Networking:** TCP/IP, DNS, DHCP, VLANs, Subnetting, OSI Model, OSPF/BGP basics, Wireshark, Nmap, Packet Analysis
- **Offensive Security:** Burp Suite, Metasploit, Gobuster, Netcat, Hydra, Hashcat, LinPEAS/WinPEAS, BloodHound, NetExec, Python exploit scripting
- **Defensive / SOC:** Microsoft Sentinel, KQL, SIEM Log Analysis, IOC Identification, MITRE ATT&CK, Incident Triage, Alert Tuning

Projects

Web Application Testing & Debugging

Academic Lab Project

- Built and tested 7 multi-tier web applications to identify and fix backend logic flaws, insecure API design, and access-control bugs.
- Used Burp Suite to trace API request/response flows and debug data-handling issues; debugged a Django-based application's template rendering logic to fix an unsafe server-side template injection flaw.
- Reviewed and patched insecure file-upload handling in two Node.js applications, and investigated and resolved a critical remote code execution issue in a Next.js application by analyzing its request-handling pipeline (CVE-2025-55182).
- Debugged a Node.js V8 process over SSH and diagnosed cron-job misconfigurations affecting system permissions.
- *Full technical write-ups documented at* 📄 github.com/bustayaga

Enterprise System Integration & Access Control Analysis

Academic Lab Project

- Analyzed and mapped a multi-server enterprise network environment using directory-service enumeration tools (BloodHound, NetExec) to understand access-control relationships in a Kerberos-authenticated system, identifying and correcting misconfigured permission chains.
- Debugged a credential-handling flow by analyzing captured network traffic (Wireshark) to trace a data-leak issue back to its source; diagnosed and resolved a Linux file-permission misconfiguration using capability analysis tools.
- Worked across a containerized (Docker) multi-service application to debug password-reset logic and an authenticated API endpoint, tracing the issue to two backend services and fixing credential handling in environment variables.
- *Full documentation available at* 📄 github.com/bustayaga

Cloud Log Analytics & Automated Alerting Pipeline

Personal Cloud Project — Microsoft Azure

- Designed and deployed a centralised log-ingestion and monitoring pipeline on Microsoft Azure using Microsoft Sentinel, integrating multiple data sources (firewalls, VMs, web applications) into a single system.
- Wrote custom KQL queries to build automated detection and alerting rules, similar to writing SQL-based analytical queries over large datasets.
- Simulated real-world scenarios to test the pipeline's accuracy, iterating on query logic to reduce false positives and improve reliability.
- *Setup documentation and reusable query templates published at* 📄 github.com/bustayaga

Applied Practice — HackTheBox Labs

Self-Directed Learning

- Completed 20+ hands-on lab machines on HackTheBox, applying and reinforcing concepts in web application debugging, system integration, network analysis, and cloud security through practical, self-paced exercises.

Education

Bachelor of Computer Application — Rabindranath Tagore University

2022 – 2025

Raja Rammohan Roy Academy, Dehradun

2020 – 2022