

# PAPPALA CHANDRA SEKHAR

Backend Developer | Python | Cybersecurity Fundamentals

Phone: 6281400460 | Email: sekhar3342@gmail.com

GitHub: <https://github.com/sekhar6281> | LinkedIn:

<https://www.linkedin.com/in/chandrasekhar-pappala-a20b693a3>

---

## PROFESSIONAL SUMMARY

Entry-level Python Backend Developer with skills in Python, SQL, and backend development, along with knowledge of computer networks and cybersecurity fundamentals. Experienced in Linux, Git, and database operations. Strong understanding of OSI model, IP addressing, protocols, and security principles. Eager to build secure and scalable applications and contribute to software development and cybersecurity roles.

## TECHNICAL SKILLS

**Programming Languages:** Python, JavaScript

**Web Technologies:** HTML, CSS

**Backend Development:** ORM Queries, CRUD Operations, Backend Logic Development

**Databases:** SQL, SQLite3

**Computer Networks:** OSI Model, TCP/IP, DNS, HTTP/HTTPS, TCP/UDP, Port Numbers

**Cyber Security:** CIA Triad, Authentication and Authorization, Malware Fundamentals, Cyber Kill Chain, Types of Cyber Attacks, MITRE ATT&CK; Framework

**Tools & Platforms:** Git, GitHub, Linux (Ubuntu), Vim, Nano

**Debugging:** Python Debugger (pdb)

## PROJECTS

### Student Management System (Python, SQLite3)

- Developed backend application to manage student records, marks, and results.
- Implemented CRUD operations using Python and SQLite3 database.
- Used ORM-style queries for efficient database operations.
- Utilized Python debugging tools (pdb) to identify and fix backend issues.

### Web Access Log Analytics – Using Splunk

- Monitored and investigated security alerts using Splunk SIEM platform.
- Created SPL queries to analyze web traffic and HTTP status distribution.
- Designed dashboard to visualize Top IPs, Event IDs, and HTTP status codes.
- Implemented chart visualizations to identify traffic patterns and anomalies.

### Email Header Analysis and Authentication Check – Using Proofpoint

- Analyzed email headers to extract sender IP, relay path, and authentication results.
- Verified SPF, DKIM, and DMARC to detect spoofing and validate sender identity.

- Used MXToolbox to analyze DNS records, blacklist status, and sender reputation.
- Investigated suspicious URLs using VirusTotal, URLScan.io, URLVoid, and Palo Alto tools.

## **EDUCATION**

Bachelor of Technology (Computer Science and Engineering)  
Bapatla Engineering College  
Year of Graduation: 2023

## **CERTIFICATIONS**

- Python Certification – W3Schools
- Introduction to Cybersecurity – Udemy, Great Learning
- Network Security Basics – Coursera

## **DECLARATION**

I hereby declare that the information provided above is true and correct to the best of my knowledge and belief.