

# Mohammad Ashbar

Cybersecurity Researcher

📍 Bangalore, Karnataka, India

☎ +91-8590786578

✉ mohammadashbar578@gmail.com

🌐 mohammadashbar

🌐 linkedin.com/in/mohammad-ashbar

## PROFILE SUMMARY

---

Motivated Computer Science Engineering graduate and Certified Ethical Hacker (CEH v13) with hands-on exposure to both offensive and defensive cybersecurity. Experienced in vulnerability assessment, penetration testing, and attacker methodologies, web application security along with SOC fundamentals such as SIEM-based log analysis, alert monitoring, and incident triage. Proficient with tools including Kali Linux, Nmap, Burp Suite, Metasploit, Nessus, Wireshark, and SIEM platforms. Strong understanding of OWASP Top 10, network security, and incident response workflows.

## INTERNSHIP

---

### •Cyber Security Intern

July 2025 - Present

TechByHeart

Bangalore

- Hands-on training in Ethical Hacking, Penetration testing, Web application testing, Vulnerability exploitation and Network Security.
- Used tools like Nmap, Burp Suite, Metasploit, Nessus, and Kali Linux for scanning, exploitation, and analysis.
- Assisted in log analysis, alert investigation, and basic incident documentation aligned with SOC workflows.

### •RPA Automation Intern

February 2025 - April 2025

NetConnect Global (NCG)

Bangalore

- Developed an Excel automation system called Shrimp using Microsoft Power Platforms (Power Automate, PowerApps, Dataverse, SharePoint).
- Delivered a scalable, secure, and audit-friendly solution for PwC, replacing their legacy workforce planning system.
- Gained hands-on experience with low-code development, workflow orchestration, and end-to-end solution deployment.

### •Cyber Security Intern

October 2023 - November 2023

CoE Digital Forensics Intelligence and Cyber Security

Mangalore

- Designed and developed a CTF (Capture The Flag) web platform focusing on real-world exploitation scenarios.
- Explored fundamental concepts in cybersecurity, such as secure coding practices, access control, and vulnerability management.
- Learnt essential skills in platforms like Kali Linux for penetration testing and ethical hacking.

## PROJECTS

---

### •Shrimp: A Scalable Excel Processing and Automation System Using Power Platform

*Shrimp is an enterprise-grade automation solution developed to streamline Excel-based workflows for a Big 4 consulting firm (PwC). It automates file splitting, controlled editing, secure distribution, and synchronization for workforce planning and operational processes.*

- Tools & technologies used: Microsoft Power Automate, PowerApps, SharePoint, Dataverse, OneDrive, Excel, URI-trigger-based desktop automation.
- The solution enabled efficient data handling by automating repetitive Excel tasks, enforcing field-level access controls, maintaining audit trails, and ensuring real-time sync between distributed files and a central master file.

### •Digital Forensics Toolkit for Evidence Extraction and Analysis

*The Digital Forensics Toolkit is a software solution developed to help forensic investigators and cyber security professionals analyze digital evidence extracted from data storage devices, system files, applications, and other relevant sources.*

- Tools & technologies used: Python, Node.js, Express.js for API development, MongoDB, VS code.
- These toolkits vary across several domains, including file analysis, network monitoring, e-mail forensics, malware detection, but they all share common functionalities.

### •CTF Web

*Developed a password manager with functionalities for password management, strength testing, and generation.*

- Tools & technologies used: HTML, CSS, JavaScript, bcrypt, JWT.

- Built a secure storage system, user authentication, real-time password strength evaluation, and a random strong password generator, ensuring high-level security and enhanced user experience.

### •Multiple Face Detection and Recognition

*A multiple face detection and recognition system designed to address the challenges associated with identifying and tracking multiple faces in diverse environments .*

- Tools & technologies used: Python, VS code, Thonny, Github Desktop.
- Built a system which offers a versatile solutions for various security applications,including access control,public surveillance and attendance monitoring.

### •Agro-culture management system

*Agro Culture is the farmer system where they can plan, monitor and analyze the activity of the farmers production system .*

- Tools & technologies used: HTML, MySQL.
- It manages farmer operation with one system and organizes data in one place. This creates in partnership with growers and buyers. It inspire farmer to produce and buyers to consume fresh goods.

## EDUCATION

---

- Sahyadri College Of Engineering And Management - Mangalore, India** 2021-2025  
*Bachelor of Engineering - Computer Science and Engineering*
- Chemnad Jamaath H S S - Kasaragod, India** 2019-21  
*Class XII/ PU : PCMB*
- St.Mary's High School - Bela, Kasaragod, India** 2019  
*Class X*

## SKILLS

---

- Tools & Software:** SIEM, Nmap, Burp Suite, Metasploit, Wireshark, Nessus, Netcat, SQLmap, Splunk, Wazuh, Microsoft Power Automate Desktop.
- Operating Systems:** Windows, Linux (Kali Linux).
- Programming Languages:** C, Python, HTML, CSS, Power Automate, SQL.
- Soft Skills:** Communication, Time Management, Analytical Thinking, Problem Solving, Incident Handling.

## CERTIFICATIONS

---

- Certified Ethical Hacker (CEHv13):** EC-Council
- Certified SOC Analyst (CSA):** EC-Council
- Certified Security Tester (CST):** Techbyheart
- ISO/IEC 27001:2022 INFORMATION SECURITY ASSOCIATE:** Skillfront
- RPA Master in Microsoft Power Automate Desktop:** Udemy
- Database and SQL:** Infosys

## LANGUAGES

---

- English, Hindi, Malayalam, Kannada, Arabic