PEDALA HARISH

+91 7993486333 ◇Guntur, India

pedalaharish8260@gmail.com ◇www.linkedin.com/in/p-harish-435572238

OBJECTIVE

Dedicated and detail-oriented cybersecurity professional seeking a Security Testing position to leverage hands-on experience with vulnerability assessment, penetration testing, and security tools to protect critical applications and infrastructure.

EDUCATION

Bachelor of Electrical and Electronics, KL University 2022--2025
Specialization: Industrial Automation

CGPA: 8.66

State Board of Technical Education in Electrical and Electronics, KHIT 2019 – 2022

Percentage: 87.51

Central Board of Secondary Education, SVBK 2019

SKILLS

CYBERSECURITY SKILLS

Security Tools: Burp Suite, Nessus, Nmap, Wireshark, Splunk (SIEM), Qualys, AWS CSPM

Knowledge & Standards: OWASP Top 10 (Injection, XSS, CSRF), V.A. (Identification, Reporting), Session/Access Control, Protocol Analysis, Firewall/ACL Management, Port Scanning, Incident Response Fundamentals (Triage, Containment), TCP/IP (Deep Understanding) Log Analysis, Security Monitoring, Alert Validation, Malware Analysis Fundamentals, Networking Fundamentals

Core Technologies: Python, Linux/Windows OS Management, HTTP/HTTPS, Web Application Architecture

Soft Skills: Analytical Problem Solving, Technical Communication, Detailed Documentation, Continuous Learning

PROFESSIONAL EXPERIENCE

Security Testing Intern July 2025 – Present

UMANG APP, National E-Governance Division, MEITY *Pragathi Vihar, New Delhi*

- Performed vulnerability assessments using industry-standard tools including Nmap, Nessus, and Burp Suite
- Executed penetration testing methodologies to identify security flaws in web applications and network infrastructure
- Developed and documented detailed test cases for security validation of authentication and authorization mechanisms
- Analysed application architecture to identify potential security weaknesses and attack vectors
- Created detailed vulnerability reports with remediation recommendations for development teams
- Monitored and analyzed security logs from the AWS CSPM platform
- Performed initial triage on high-severity alerts generated by the AWS CSPM platform (e.g., exposed S3 buckets, overly permissive (IAM roles), applying incident response fundamentals to classify risks and determine necessary containment steps.
- Collaborated with cross-functional teams to ensure security requirements are integrated into the development lifecycle

Integration Level Testing Intern Jan 2025 - May 2025

Efftronics System Pvt Ltd *Guntur, AP*

- Network Security Testing: Conducted integration-level testing of advanced monitoring systems (RDPM, Data Loggers, RTUs) with focus on secure data transmission and protocol integrity across TCP/IP-based railway networks.
- Vulnerability Identification: Analysed communication flows between field devices (e.g., sensors, CPU cards) and central control systems to detect unauthorized access vectors and data tampering risks in operational technology (OT) environments.
- Security Protocol Validation: Verified encryption standards and authentication mechanisms in wireless communication modules (RS232, GPRS) to prevent man-in-the-middle attacks in critical railway control systems.

PROJECTS

Automatic Medicine Reminder Using Arduino

- I have created a medicine reminder system that can be used for alerting users when it is time to take their drugs at appropriate timings of 1, 2 or 3 times a day. The project also aims at making it possible to send email/SMS notifications as well as possible integration with a patient monitoring system.

CERTIFICATIONS

- INTEGRATION LEVEL TESTING ON DATALOGGER, RDPM AND CHARGERS
- Introduction to AI
- Machine Learning with R programming

DECLARATION

- I hereby declare that the above-mentioned information is correct up to my knowledge and I bear the responsibility for the correctness of the above-mentioned particulars.