ADITHYAN V

+91 9778041634 | adithyanv783@gmail.com

Portfolio: adithyanjkr.github.io/Portfolio

LinkedIn: linkedin.com/in/adithyan-v- | GitHub: github.com/adithyanjkr

Kollam, Kerala

1 Professional Summary

Cybersecurity Researcher and BCA graduate with an add-on specialization in Cyber Security, skilled in Offensive Security, Vulnerability Assessment & Penetration Testing (VAPT), Incident Response, SIEM monitoring and AI-assisted security automation. Completed the Certified IT Infrastructure & Cyber SOC Analyst (CICSA) course at Red Team Hacker Academy. Hands-on experience with web application security and security labs on TryHackMe and PortSwigger Academy. Seeking a Cyber Security Analyst, VAPT, or SOC Analyst role.

2 Skills

- **Cybersecurity**
  Offensive Security, Defensive Security, Vulnerability Assessment & Penetration Testing (VAPT), Web Application Security, SIEM Monitoring, Threat Intelligence, Incident Response
- **Offensive Security Tools**
  Burp Suite Professional, Metasploit, Sqlmap, Nmap, Katana, Hydra
- **Defensive Security Tools**
  Splunk, Wazuh, Snort, Wireshark
- **AI-Assisted Security & Automation**
  AI Agent Integration for Security Automation, Codex AI, Hermes Agent, HexStrike MCP, Playwright MCP
- **Operating Systems & Virtualization**
  Kali Linux, Windows, Ubuntu, VMware, VirtualBox
- **Networking**
  TCP/IP, OSI Model, DNS, DHCP, NAT, TCP/UDP, Routing & Switching
- **Programming & Scripting**
  Python (Basics), HTML, CSS

3 Internships

Cyber Security Analyst Intern (Virtual)
Future Interns | May 2026

- Completed a one-month virtual Cyber Security Analyst internship
- Developed three cybersecurity projects focused on Vulnerability Assessment & Penetration Testing (VAPT), API Security Analysis, and Phishing Email Detection.
- Awarded a Certificate of Completion and Letter of Recommendation for successful performance.

Cybersecurity with AI Intern (Virtual)
NIIT Foundation in collaboration with Cisco Networking Academy | August 2025

- Completed a one-month virtual cybersecurity internship.
- Designed and configured a secure enterprise network in Cisco Packet Tracer.
- Earned three Cisco certifications, including Cybersecurity.

4 PROJECTS

VIPER-SOC: Vulnerable IP & Payload Eradication Response

Technologies Used: Wazuh SIEM, Python, VirusTotal API, AbuseIPDB API, Kali Linux

Developed VIPER-SOC (Vulnerable IP & Payload Eradication Response), an automated incident response framework integrated with Wazuh SIEM for network threat detection and endpoint protection. Integrated AbuseIPDB for IP reputation analysis and VirusTotal for SHA-256-based malware detection, leveraging custom Python integrations, File Integrity Monitoring (FIM), and Wazuh Active Response to automatically block suspicious IP addresses and remove identified malicious files. Implemented rule-based response workflows to streamline threat containment, reduce manual intervention, and improve incident response efficiency.

XSS Detection Using Snort IDS

Technologies Used: Snort 3, Python, Flask, Kali Linux

Developed a hands-on web security lab to simulate and detect Cross-Site Scripting (XSS) attacks in real time using Snort 3 IDS, Python, Flask, and Kali Linux. Built an intentionally vulnerable Flask web application to demonstrate reflected XSS and implemented custom Snort rules to inspect HTTP traffic, detect malicious script-injection payloads, and generate real-time intrusion alerts. Demonstrated the detection process in a controlled local environment and documented security alerts, attack simulations, and mitigation techniques, including secure output encoding and input handling.

5 CERTIFICATIONS

- **EC-Council Certified SOC Analyst (CSA v2)**
- **Certified IT Infrastructure & Cyber SOC Analyst (CICSA v3) –** Red Team Hacker Academy
- **Advanced Diploma in Cyber Security and Cloud Computing** – STED Council & Skill Development Council Canada
- **Python Programming Certification -** Global India Techno Hub

6 ACHIEVEMENTS

- Secured 1st Prize in a CTF Competition at Red Team Hacker Academy as part of a three-member team, Team 0day.
- Identified and responsibly disclosed security vulnerabilities in Kerala Government web infrastructure through CERT-In, receiving official Case IDs.
- Ranked within the Top 4% on TryHackMe, demonstrating hands-on skills in penetration testing, SOC operations, and defensive security.
- Actively participating in bug bounty programs on HackerOne, Bugcrowd, and other platforms.

7 EDUCATION

Certified IT Infrastructure and Cyber SOC Analyst (CICSA v3) – Nov 2025 – June 2026
RedTeam Hacker Academy, Trivandrum

Bachelor of Computer Applications (BCA) -2022-2025
Indira Gandhi College of Arts and Science, Ernakulam

Diploma in Cyber Security & Cloud Computing (Add-On) - Apr 2024 – Apr 2025
Global India Techno Hub, Ernakulam