

Sathwik Mohan Vallala

571-373-6079 | sathwikv143@gmail.com | in/sathwik-mohan | About Me | Meet Me | VISA Sponsorship Required

SUMMARY

Driven cybersecurity enthusiast with a passion for building secure software. Years of experience leveraging analytical skills & a curious nature to identify & solve vulnerabilities in web applications. Proficient in secure code review, with knowledge of popular security tools & networking concepts. Actively engaged in the cybersecurity community, I continuously seek knowledge & best practices to build a more secure digital future. As a highly motivated individual driven by proactive security & continuous learning, I am eager to contribute my expertise to a team that shares my commitment to leaving no breach undiscovered.

EXPERIENCE

Product Security Engineer (CarbonBlack)

Nov. 2023 – Present

Broadcom Inc.

Herndon, VA

- Reduced potential attack surface by identifying & resolving critical security issues measured by CVSS scoring systems.
- Executed penetration testing, uncovering & exploiting vulnerabilities to strengthen application security.
- Applied threat modeling techniques to identify potential attack vectors & guide secure design decisions within engineering teams.
- Proactively detected & mitigated potential security risks during secure code reviews, preventing exploitation.
- Communicated complex technical security issues fostering understanding & buy-in from product teams.

Security Response Engineer

Apr. 2022 – Nov. 2023

VMWare Inc.

Herndon, VA

- Uncovered critical security issues through pentesting in a wide range of VMWare products.
- Employed penetration testing & secure code reviews to find the root cause of security vulnerabilities.
- Quantified security risks using industry-standard scoring systems (CVSS), ensuring informed decision-making.
- Collaborated on penetration testing projects to uncover & disclose security vulnerabilities before exploitation.
- Championed effective communication with product teams, ensuring timely & successful resolution of security issues.
- Streamlined security processes by developing & implementing automations, enhancing team efficiency & effectiveness.

Digital Forensic Researcher & Developer

Dec. 2020 – Mar. 2022

ADF Solutions Inc

Reston, VA

- Ensured accuracy & reliability of existing digital artifact collection modules through rigorous testing & verification procedures.
- Independently researched & developed new digital artifact collection modules, expanding the capabilities of the system.
- Demonstrated creativity & problem-solving skills by devising innovative solutions for collecting diverse digital artifacts.
- Demonstrated strong team spirit & adaptability by actively assisting colleagues & fulfilling diverse project requirements.
- Leveraged Python scripting expertise to create custom plugins for efficient parsing & extraction of various digital artifacts & evidence, streamlining investigative processes.
- Maintained a high level of quality assurance by conducting thorough testing & validation of developed plugins before integration into the operational DEI Tool.
- Responded effectively to customer & supervisor requests by developing specialized plugins to meet specific investigative needs, demonstrating flexibility & responsiveness.

Bug Bounty Hunter

Oct. 2019 – Oct. 2020

Freelance

- Uncovered web app vulnerabilities through ethical hacking (black/white/graybox).
- Responsibly reported vulnerabilities to website owners with detailed reports.
- Assessed app security using industry tools (OWASP ZAP, Nessus) & threat modeling.

Trainee Security Analyst - Internship

Jul. 2019 – Oct. 2019

SOC Experts

Bangalore, India

- Bolstered security with diverse SIEM tools (Splunk, QRadar, LogRhythm) for threat detection & response.
- Analyzed & monitored logs to uncover suspicious activity & potential incidents.
- Conducted basic digital forensics, collecting & analyzing evidence for investigations.
- Thrived in simulated SOC, collaborating effectively to identify & respond to security threats.

Security Analyst - Internship

Jun. 2017 – Jun. 2018

Berry9 IT Services Pvt Ltd

Hyderabad, India

- Mastered ethical hacking through personal projects, fueled by passion.
- Identified vulnerabilities in real-world healthcare pen testing project.
- Earned CEH certification, validating ethical hacking expertise.

EDUCATION

George Mason University

Fairfax, VA

Master's of Science in Digital Forensics & Cyber Analysis - 3.89/4.0

Jan. 2020 – Dec. 2021

Jawaharlal Nehru Technological University

Hyderabad, India

Bachelor's of Technology in Computer Science Engineering - 4.0/4.0

Aug. 2015 – Aug. 2019

PROJECTS

- Autopsy WhatsApp Plugin** | *Python, Forensics, Evidence* Apr. 2020 – May 2020
- Enhanced *Autopsy* capabilities by independently developing a new plugin, demonstrating expertise in forensics tool customization & automation.
 - Recovered & parsed digital evidence from the *WhatsApp* application on *Windows* systems, utilizing advanced data extraction & parsing techniques.
- Chat over network with Python** | *Python, Network, Encryption* Jun. 2018 – Jul. 2018
- Built a privacy-forward chat application with strong cryptography, empowering secure communication.
 - Implemented robust end-to-end encryption for secure communication, ensuring message confidentiality & protecting user data.
 - Enabled user control & independence by designing a self-hostable chat server, fostering privacy & data sovereignty.
- File Sharing** | *PHP, HTML, SQL, Network* Mar. 2018 – Apr. 2018
- Streamlined internal file sharing with a user-friendly platform designed for specific network needs.
 - Prioritized security by implementing password authentication to restrict unauthorized access to shared files.

CERTIFICATIONS & AWARDS

- Security Code Review Ninja - 2nd Degree Black Belt** | Secure Coding Dojo December 2023
- Digital Evidence Investigator** | ADF Solutions December 2020
- Certified Autopsy User** | Basis Technology October 2020
- Certified Ethical Hacker** | EC Council October 2017

TECHNICAL SKILLS

Professional: Forensic Analysis, Malware Reverse Engineering, Network Forensics, Memory Forensics, Penetration Testing, Incident Response, Log Analysis, Security Event Management, Ethical Hacking, Vulnerability Assessment, Threat Hunting, Open Source Intelligence, SAST, DAST

Tools: EnCase, FTK, Autopsy, Black Bag, X-Ways, AXIOM, Volatility, Tcpdump, Falcon, WinHex, OllyDbg, IDA, Ghidra, Snort, Zeek, Hashing, Write Blocker, Splunk, IBM QRadar, Log Rhythm, Metasploit, Burpsuite, ZAP, OWASP, Linux, Nmap, Wireshark, Ettercap, Aircrack-ng, SQLMap, Hydra, John the ripper, Nikto, Nessus, Open Source Security Tools

Programming Languages: Python, Bash, SQL, PHP