Sathwik Mohan Vallala

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

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 product 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*

- Analyzed incoming security vulnerability reports, assessed urgency, & ensured timely responses.
- Validated & assessed reported vulnerabilities, assigned severity levels (CVSSv3.1), & documented exploitation steps & mitigation strategies.
- Coordinated vulnerability communication across internal teams & planned customer communication.
- Collaborated with researchers for responsible vulnerability disclosure & published VMware Security Advisories (VMSA) to inform customers about required actions.
- Defined & implemented corrective actions like mitigations, IOCs, workarounds, remediations to address vulnerabilities & minimize customer risk.
- Proactively monitored for exploit activity & updated advisories to reflect the evolving threat landscape.
- 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
*Master's of Science in Digital Forensics & Cyber Analysis - **3.89/4.0*** *Fairfax, VA*

Jewaharlal Nehru Technological University
*Bachelor's of Technology in Computer Science Engineering - **4.0/4.0*** *Hyderabad, India*

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

- Vulnerability Assessment
- Penetration Testing
- SAST
- Log Analysis
- Forensic Analysis
- Memory Forensics
- SaaS
- Application Security
- Incident Response
- DAST
- Security Event Management
- Malware Reverse Engineering
- Open Source Intelligence
- Threat Hunting
- Secure Code Review
- AWS Security
- Ethical Hacking
- Network Forensics
- Cloud Security

Tools

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

Scripting

- Python
- PHP
- Bash
- JavaScript
- SQL