

Tulasi Sai Charan Sharma Gaddam

📍 Prospect, CT, USA

✉️ tulasisaicharansharmag@gmail.com

☎️ +1 (475) 317-4696

🌐 LinkedIn: www.linkedin.com/in/tulasi-sai-charan-sharma-gaddam

SUMMARY

Cybersecurity professional with **5+ years of combined experience in offensive security, penetration testing, red team operations, and digital forensics**, specializing in **real-world attack simulation, vulnerability exploitation, and threat emulation** across web, API, mobile, network, and cloud environments. Strong expertise in **MITRE ATT&CK-aligned testing, OWASP Top 10, API security, and adversary emulation**. Proven ability to document risk, communicate findings to stakeholders, and collaborate with blue teams to strengthen enterprise and regulated security postures.

TECHNICAL SKILLS

Offensive Security & Red Teaming

- Web, API, Network, Mobile & Cloud Penetration Testing
- MITRE ATT&CK, OWASP Top 10 & API Top 10
- Adversary Emulation & Attack Simulation

Security Tools

- Burp Suite, Metasploit, Nmap, Nessus, Qualys
- OWASP ZAP, Acunetix, NetSparker, IBM AppScan, HP Fortify
- DirBuster, Hydra, FFUF, Kali Linux
- Wireshark, Tcpdump

API & Application Security

- Postman, SoapUI, API Fuzzing
- JWT / OAuth Exploitation
- REST, GraphQL, JSON, XML

Mobile Security

- MobSF, Genymotion, ADB Shell
- Frida, Objection, Drozer
- APKTool, Quark, Inspeckage, Xposed

Digital Forensics & IR

- EnCase, FTK, Cellebrite UFED
- Autopsy, Sleuth Kit, Magnet AXIOM
- Volatility, Redline, Oxygen Forensics

Cloud & Containers

- Docker
- AWS, Azure, GCP (Foundational Security)

Programming & Scripting

- Python, JavaScript, Bash

PROFESSIONAL EXPERIENCE

Cybersecurity Red Team Analyst

Security Research & Enterprise Labs (Academic + Industry Projects)
Jan 2024 – Present | Connecticut, USA

- Conduct **advanced red team and penetration testing engagements** simulating real-world adversary behavior across web, API, network, and cloud environments.
- Perform **MITRE ATT&CK-aligned attack simulations**, including initial access, privilege escalation, lateral movement, and data exfiltration.
- Execute **web and API security testing** using Burp Suite, Postman, OWASP ZAP, Acunetix, and manual exploitation techniques.
- Conduct **network vulnerability assessments** using Nmap, Nessus, Qualys, and Metasploit.
- Collaborate with blue teams to validate alerts, improve detection logic, and enhance incident response workflows.
- Deliver **executive-ready penetration testing reports** with risk ratings and remediation guidance.

Penetration Tester / Offensive Security Analyst

University Cybersecurity Labs & Client-Based Simulations Aug 2023 – Dec 2023 | USA

- Performed **end-to-end penetration testing** across web applications, APIs, internal networks, and mobile platforms.
 - Identified and exploited **OWASP Top 10 and API Top 10 vulnerabilities**, including IDOR, authentication bypass, and injection flaws.
 - Conducted **mobile application security assessments** using MobSF, Drozer, Frida, and reverse-engineering tools.
 - Supported **forensic investigations** using Volatility, Autopsy, and FTK.
 - Created detailed technical and non-technical documentation for remediation planning.
-

Cybersecurity Analyst (Offensive Security Focus)

Capstone Projects & Security Operations Collaboration Jan 2023 – Jul 2023 | USA

- Supported **offensive security testing initiatives** and assisted in evaluating SOC detection effectiveness.
 - Conducted **API fuzzing and authentication testing** using Burp Suite, Postman, and custom scripts.
 - Participated in **threat modeling, attack path analysis, and tabletop incident response exercises**.
 - Assisted in post-incident analysis and security documentation aligned with compliance requirements.
-

Junior Penetration Tester

Cybersecurity Training Programs & Industry Labs Jul 2021 – Aug 2022 | Hyderabad, India

- Conducted **web application and network penetration testing** using Burp Suite, OWASP ZAP, Nmap, Nessus, and Metasploit.
 - Identified vulnerabilities related to authentication, authorization, and insecure configurations.
 - Developed **proof-of-concept exploits** to demonstrate business impact.
 - Documented findings using professional penetration testing report standards.
-

Cybersecurity Intern / Security Operations Trainee

Academic & Practical Security Engagements

Jun 2019 – Jun 2021 | India

- Assisted in **vulnerability assessments, security testing, and monitoring activities**.
 - Performed **network traffic analysis** using Wireshark and Tcpdump.
 - Supported **digital forensic investigations** including disk and memory analysis.
 - Built strong foundations in networking, operating systems, and cybersecurity fundamentals.
-

EDUCATION

Master's in Cybersecurity

Sacred Heart University, Fairfield, CT, USA
Mar 2024 – Jun 2025

Bachelor's in Computer Science

Malla Reddy College of Engineering, Hyderabad, India
Aug 2019 – Aug 2023

CERTIFICATIONS

- Certified Ethical Hacker (CEH)
- Computer Hacking Forensic Investigator (CHFI)
- CompTIA Security+