Sai Manikanta Teja Parwatha

Lansing, MI · (989) 824-6552 · tejaparwatha@gmail.com · linkedin.com/in/tejaparwatha

Summary

Penetration Tester & Security Analyst with 3+ years of experience in offensive security, vulnerability management, and SOC operations across government, healthcare, and enterprise environments. Conducted penetration testing of web apps, APIs, networks, and cloud platforms, including Azure Gov, AWS, and SaaS applications. Experienced building risk registers in Vanta for SOC 2, aligning findings with remediation plans and risk owners. Skilled in scripting, exploit validation, and reporting for both technical and executive audiences. Hands-on with red-team style assessments, incident response investigations, and regulatory testing (PCI DSS, HIPAA, NIST 800-53).

Certifications

- CompTIA Security+
- Pursuing CEH

Technical Skills

Penetration Testing & Vulnerability Management: Kali Linux, Burp Suite, Metasploit, Nmap, Wireshark, OWASP ZAP, SQLmap, John the Ripper, Aircrack-ng, Nessus Pro, Tenable, Qualys, Acunetix
Programming & Web Tech: Python, PowerShell, Bash, Java, C#, HTML, CSS, JavaScript, PHP
Cloud & Network Security: Azure Gov/Commercial, AWS (IAM, Security Hub), GCP (SCC); VPNs, WAF, TCP/IP, DNS, HTTP, FTP, SMTP
Security Principles: Encryption, Authentication, Authorization, Access Control, Risk Assessment, Threat Modeling, Remediation Tracking
Compliance & Governance: PCI DSS, HIPAA, SOC 2, FedRAMP, ISO 27001; Risk Registers, Audit Evidence, Security Policy Writing, Executive Reporting
Platforms: Windows Server, Linux (Ubuntu, RHEL, CentOS), VMware, Hyper-V, SQL Server, Oracle

Professional Experience

Penetration tester / Information Security Analyst Jun 2024 – Present
RICEFW Technologies Inc. – Lansing, MI (Client: State of Michigan)

- Performed web application and API penetration testing using Burp Suite Pro, OWASP ZAP, and custom scripts, identifying injection flaws and insecure authentication mechanisms.
- Built automated scripts to run manual pentest tasks (subdomain enumeration, passive/active reconnaissance, fuzzing) and to validate OWASP Top-10 risks across large web estates.
- Conducted internal and external network penetration tests using Nessus Pro (scanner agent), Nmap, and Metasploit, validating firewall, VPN, and NSG configurations against best practices.
- Performed FedRAMP-style infrastructure scans using Tenable (VMDR) and Nessus scanner agents for both agent-based and credentialed assessments, and integrated results into remediation trackers.
- Analyzed wireless access point security with Kali Linux tools (Wireshark), detecting rogue APs and weak encryption deployments.

- Reviewed SaaS and Azure Gov cloud deployments for IAM, encryption, and logging controls, reporting risks and aligning them with SOC 2 requirements.
- Contributed to disaster recovery tabletop exercises, documenting lessons learned and aligning procedures with business continuity and incident response requirements.
- Built and maintained a risk registry in Vanta, recording threats, risk owners, and mitigation strategies; used it to track closure of penetration test findings and evidence for SOC 2 readiness.
- Developed System Security Plans (SSPs) and remediation trackers, aligning controls with NIST 800-53 and SOC 2 compliance requirements.
- Automated parsing of vulnerability scan results (Tenable/Nessus/Qualys) and exploitation checks with Python and PowerShell, accelerating reporting timelines and producing reproducible PoCs.
- Authored penetration test reports with executive summaries, enabling leadership to prioritize remediation based on risk and business impact.
- Investigated incidents with packet captures (PCAP) in Wireshark and Sentinel logs, validating alerts and assisting incident response teams.
- Participated in red-team style phishing and credential compromise simulations, providing lessons learned for SOC monitoring improvements.
- Applied lab experience from CTFs and platforms (Hack The Box, TryHackMe) to develop reliable PoCs and repeatable test cases for remediation validation.

Offensive Security / Penetration Testing Specialist Jun 2022 – Nov 2022
Genzeon Technologies – Healthcare & Dental Network

- Performed penetration testing on healthcare applications, uncovering session fixation, weak crypto, and injection flaws in claims and payment systems.
- Conducted HIPAA and PCI DSS compliance assessments, testing technical safeguards for ePHI and cardholder data protection.
- Verified remediation effectiveness through repeat Nmap, Nessus and Metasploit scans, ensuring closure of high-risk vulnerabilities.
- Leveraged Qualys to perform credentialed vulnerability assessments across Windows/Linux servers and MSSQL databases; integrated findings into ticketing and audit evidence.
- Wrote secure coding guidelines for development teams, focusing on OWASP Top 10 risks common in healthcare applications.
- Scripted Bash/Python utilities to detect log tampering, expired certificates, and privilege escalation attempts; automated re-tests after remediation.
- Coordinated penetration tests with external vendors, validated remediation results, and prepared audit-ready documentation for regulators.
- Partnered with compliance officers to align security test results with HIPAA risk analysis requirements and PCI remediation roadmaps.
- Conducted workshops with engineering teams to walk through penetration test findings, explain exploit paths, and prioritize fixes.
- Created executive-level reports for client stakeholders summarizing regulatory gaps, open vulnerabilities, and mitigation plans.

- Reproduced lab-based exploit chains derived from CTF practice to validate critical findings and to build repeatable remediation test cases.

Support Analyst Apr 2021 – Jun 2022
Amazon Development Center – Hyderabad, India

- Provided operational support for global Amazon Selling Partners, advising on account authentication, secure access, and fraud prevention.
- Identified recurring patterns in suspicious logins and escalated systemic risks to security and compliance teams.
- Partnered with investigations teams to improve fraud controls and access management processes.
- Authored process documentation and knowledge base articles that reduced repeat issues and improved operational efficiency.
- Collaborated with engineering and risk teams to strengthen account recovery workflows, reducing unauthorized access cases.
- Performed case investigations with a pentest-minded approach, analyzing attack vectors such as credential stuffing and phishing.
- Educated sellers on secure password management and two-factor authentication, reducing account takeover incidents.
- Participated in internal CTF-style exercises and tabletop attack simulations to improve incident detection and response playbooks.

Education

- M.S. in Information Systems, Central Michigan University (2024)
- B.Tech, Kakatiya Institute of Technology and Science (2020)

- Recognized under the Government of India Responsible Disclosure program for identifying and reporting security vulnerabilities in public-facing systems.
- Active practice on HackTheBox, TryHackMe labs, Capture The Flag (CTF) challenges and community-driven competitions.
- Active submissions to Bugcrowd and HackerOne platforms, gaining hands-on experience with vulnerability triage, responsible disclosure, and PoC reporting.