Prakash Nadakuditi

Cybersecurity Engineer

Texas, USA | prakash.nadakuditi@gmail.com | cyberboy.net | (813)-869-4142

PROFESSIONAL SUMMARY

Dynamic Cybersecurity Engineer with 5+ years of offensive security and red-team expertise combined with cutting-edge AI security innovation. Proven track record in pentesting, cloud hardening, and AI-driven threat hunting. Adept at developing LLM injection testing frameworks, adversarial prompt engineering techniques, and AI-powered detection pipelines that reduce response times by up to 40%. Passionate about merging traditional cybersecurity best practices with emerging AI security strategies to safeguard enterprise environments.

TECHNICAL SKILLS

Red Teaming & Penetration Testing Tools: Cobalt Strike, Metasploit, Burp Suite, Nmap, OWASP ZAP, custom exploit tool development, AI-driven pentest assistants (SecGPT, RedAI, Pentester.ai), mobile app pen-testing

Cloud Security: AWS (IAM, KMS, GuardDuty, Security Hub), GCP, Azure, Terraform, Prisma Cloud CSPM & CWP

AI & Machine Learning Security: LLM injection testing, adversarial prompt engineering, AI-driven threat hunting pipelines, model hardening, secure prompt design

Security Automation & Detection: SIEM (Splunk, ELK), SOAR integrations, HPC analysis, anomaly detection

Network & Web Security: Wireshark, TCPDump, Nessus, Shodan, SQLMap, XSS/CSRF/SSRF exploitation, API security, Cryptography

Programming & Secure Development: Python, Ruby, Go, Swift, Java, C, C++; secure coding, SDLC, AI Code generation & testing.

Identity & Authentication: Identity management design, authentication controls, least-privilege enforcement

System Administration & Hardening: Linux/Windows OS hardening, patch management, system configuration

Processes & Frameworks: Threat modeling, MITRE ATT&CK mapping, and post-exploit reporting.

WORK EXPERIENCE

Security Engineer (R&D) **October 2024–Present**

Caspia Technologies, Texas, USA

- Spearheaded a real-time ransomware prevention mechanism using hardware performance counters, cutting malicious execution impact by 60%.
- Designed and implemented an AI-driven detection pipeline integrating machine learning models and custom HPC analysis, reducing response time by 40%.
- Led GenAI penetration tests using AI agents to simulate attacks, uncovering and fixing 75% of prompt vulnerabilities..
- Engineered adversarial prompt engineering techniques to simulate AI-driven attack vectors, improving model hardening and reducing evasion by 30%.

Cybersecurity Analyst Intern **May 2024–October 2024**

Resilience Inc, Texas, USA

- Led end-to-end penetration tests on financial platforms, uncovering critical OWASP Top 10 flaws and reviewing code to recommend secure coding fixes, reducing exploitable surface area by 50%.
- Integrated SOAR playbooks with Splunk and ELK for automated alert triage, decreasing analyst workload by 30% and false positives by 25%.
- Architected Python-based automation for vulnerability assessments, accelerating testing cadence by 40% and saving 30+ hours monthly.
- Conducted AI-powered threat hunting leveraging custom scripts, enriching alert context, and driving a 30% drop in high-risk incidents.

Security Engineer/Penetration Tester **April 2021–August 2022**

Tata Consultancy Services, Karnataka, India

- Executed red-team engagements in AWS, identifying 30+ misconfigurations (IAM, S3) and auditing identity management and authentication controls to enforce least-privilege.
- Built CSPM & CWP frameworks with Terraform and Prisma Cloud, reducing cloud attack surfaces by 40%.
- Automated remediation workflows using Terraform and Python, cutting manual effort by 40% and improving patching velocity.
- Piloted AI-driven anomaly detection PoC using AWS GuardDuty insights and custom ML models, achieving 85% detection accuracy for novel threat patterns.

External Penetration Tester **March 2018–June 2024**

Independent Bug Bounty Hunter, Florida, USA

- Discovered and responsibly disclosed 100+ critical vulnerabilities (RCE, SSRF) across 30+ targets, enhancing security posture and trust.
- Developed Bash and Python automation tools to scale scanning operations, increasing coverage by 50% and reducing manual tasks by 40%.
- Collaborated with clients and internal security teams to author threat models and detailed technical reports, accelerating remediation timelines by 70%.
- Published 5 industry whitepapers on advanced chaining techniques and adversarial model attacks, growing community engagement by 15%.

EDUCATION

Master of Science in Cybersecurity

The University of Tampa, Florida, USA *August 2022–May 2024* (GPA: 3.7)

Bachelor of Technology in Information Technology

PVP Siddhartha Institute of Technology, Andhra Pradesh, India *March 2017–April 2022* (GPA: 3.21)

CERTIFICATIONS

- Certified Ethical Hacker (CEH Master) — EC-Council
- CompTIA Pentest+ — CompTIA
- Certified Web Application Security Professional — EC-Council

ACHIEVEMENTS

- **BSides Tampa 2023 CTF Winner:** Led custom payload development and advanced lateral movement chains, securing 1st place.
- **OWASP Tampa Chapter Q2 CTF Champion:** Demonstrated exploit innovation to bypass layered defenses in real-world scenarios.
- **Spartans CTF 2024 1st Place:** Employed reverse engineering and cryptographic attacks to exfiltrate sensitive data, showcasing post-exploit mastery.