PAVAN PAVITHRAN

+971 52 760 7194 | Email: pavanpavithran44@gmail.com | LinkedIn: www.linkedin.com/in/pavan-pavithran |
Portfolio: drpaps.github.io | GitHub: github.com/DrPaps

SUMMARY

Security-focused Engineering Physics graduate with hands-on experience in threat monitoring, incident response, and vulnerability assessment. Proficient in tools such as Wireshark, Splunk, Nmap, and Nessus. Strong foundation in TCP/IP, attack vectors, and the MITRE ATT&CK framework. Certified in CEHv13 and CompTIA Security+, with a proven track record in detecting and reporting real-world threats through CTF and internship experience.

SKILLS

Tools: Nmap, Burp Suite, Nessus, Metasploit, Wireshark, OWASP ZAP, hydra, SQLmap, Splunk

Networking: TCP/IP, DNS, VPNs, Firewall, Proxies

Operating Systems: Kali Linux, MacOS, Windows

Programming: Bash, Python, C++, Java, HTML, Qiskit

Frameworks & standards: OWASP Top 10, MITRE ATT&CK, CVSS

Soft Skills: Report writing, cross-team collaboration, adaptability to new tools and environments

CERTIFICATIONS

CompTIA Security+ Sy0-701

EC-Council CEHv13

Advanced Penetration Tester (RedTeam Hacker Academy)

EDUCATION

University of Illinois Urbana Champaign | Bachelor of Science Engineering Physics 09/2020 – 05/2024

- Additional electives completed for computational physics track.
- GPA: 3.24

PROFESSIONAL EXPERIENCE

CYBERSECURITY INTERN | RedTeam, Dubai 05/2025 – 06/2025

- Conducted vulnerability assessments and penetration testing for client networks, web applications, and internal systems.
- Identified security flaws like SQL injection (SQLi), Cross-Site Scripting (XSS), and broken authentication vulnerabilities.
- Detected and exploited security flaws in staging environments using Burp Suite, ZAP, and Metasploit.
- Performed internal network penetration testing using Nmap and Nikto to evaluate network security.
- Wrote clear, concise vulnerability assessment reports with findings, risk assessments, and remediation strategies.
- Collaborated with IT teams to prioritize and resolve security issues in a timely manner.
- Assisted in setting up automated vulnerability scans using Nessus and OpenVAS.

SDE INTERN | University Affiliated startup, Champaign, IL 05/2024 – 08/2024

- Developed and maintained Java-based features for an internal exposure management system, improving reliability and control.
- Introduced a Spring Boot REST API that enhanced user visibility into exposure adjustments, reducing manual lookup time.
- Implemented clean coding practices by engaging in code reviews and maintaining code coverage exceeding 90%.

TEACHING ASSISTANT | University of Illinois Urbana Champaign, IL 05/2021– 12/2021

- Guided incoming international students through academic and cultural adaptation through university course LAS100.
- Facilitated group discussions and evaluated student assignments on a weekly basis.

PROJECTS

VAPT ON E-COMMERCE APPLICATION

- Conducted a penetration test of a sample e-commerce website to identify vulnerabilities.
- Discovered XSS and SQL injection vulnerabilities using Burp Suite and SQLmap.
- Created a detailed report with risk analysis and suggested remediation steps.

CTF CHALLENGES

- Participated in various CTF platforms like TryHackMe and Hack The Box.
- Solved over 100 CTF challenges related to web exploitation, buffer overflows, and Linux privilege escalation.
- Improved problem-solving and penetration testing skills through hands-on exercises.
- Ranked top 5 in TryHackMe Monthly leaderboard for May 2025.

RESEARCH PROJECT

- Collaborated with a team of students with the help of a professor to develop a model to detect and count the number of Western Corn Rootworm Beetles in corn fields in mid-western United States.
- Utilized an Arduino microcontroller with a camera module and a YOLOv5 deep learning model.