Aditya Dindi

[Email] | adityadindi.com | linkedin.com/in/adityadindi

Experience

Application Security Intern* | Paycom** ***May 2024 - August 2024

- Conducted a black-box web application security assessment on a custom-built application, leveraging Burp Suite Professional and the OWASP Top 10 Framework. Delivered a detailed professional report with actionable insights, presented directly to executive leadership to enhance application security.
- Performed white-box penetration tests on Paycom's application, uncovering critical vulnerabilities. Documented findings in Confluence and created Jira tickets, leading to measurable improvements in system security under the mentorship of full-time security professionals.
- Streamlined secure development processes by performing extensive code reviews on PHP code to identify and mitigate vulnerabilities. Collaborated with an agile team to implement sustainable best practices and design patterns, utilizing Git/GitLab for task management.

Security Researcher* | Army Educational Outreach Program Apprenticeship** ***August 2023 - Present

- Engineered a firmware parser plugin for Ghidra, addressing multi-architecture challenges in embedded systems by utilizing Java and Python, significantly enhancing the tool's analysis capabilities.
- Conducted a comprehensive literature review on Firmware Analysis Methodology in Binary Analysis of Embedded Systems, leveraging Zotero for precise organization, citation management, and reference tracking, contributing to improved research efficiency and collaboration.

Cyber Operations Intern* | MITRE** ***May 2022 - August 2023

- Designed and delivered a MITRE ATT&CK Defender™ training course, equipping professionals with expertise in ATT&CK Techniques and sub-techniques through advanced Threat Research and Adversary Emulation testing.
- Authored a strategic 5-year roadmap for enhancing the Army's Red Team Testing and Evaluation (T&E) capabilities, based on comprehensive research and analysis of current operations.

Penetration Tester* | National Guard Bureau (Contract)** ***April 2023 - June 2023

- Conducted a comprehensive security assessment of a National Guard prototype, identifying and mitigating vulnerabilities to enhance critical infrastructure resilience and system reliability.
- Authored and presented a detailed findings report, outlining identified vulnerabilities and providing actionable remediation recommendations to strengthen system security.

Certifications

- OffSec Certified Professional (OSCP)
- HTB Certified Bug Bounty Hunter (CBBH) [In-Progress]
- CompTIA Security+, CySA+
- AWS Certified Cloud Practitioner

Education

University of Texas at San Antonio | *Bachelor of Business Administration in Cyber Security* ***Expected Graduation: August 2025***

- RowdyCon Lead Organizer and Finance Lead - UTSA Cybersecurity conference

Projects

Microsoft Vulnerability Discovery and Disclosure ***February 2024***

- Identified critical security vulnerabilities in a Microsoft Products web application, including improper input sanitization leading to stored XSS and CSRF, which posed a significant risk of account takeover for millions of users.
- Authored a detailed vulnerability report, including step-by-step reproduction instructions and remediation strategies, ensuring effective communication of security risks to stakeholders.

Web CTF Challenge Development ***November 2024***

- Developed 9 web-based CTF challenges, demonstrating expertise in OWASP Top 10 Vulnerabilities, with difficulty levels ranging from beginner to advanced, leveraging Docker for secure and scalable deployment.
- Provided real-time support and guidance to participants, effectively addressing inquiries and enhancing their understanding of web application security concepts.

Competitions

Collegiate Penetration Testing Competition (CPTC)* |** *2023 Central Regional Champion* ***August 2022 - January 2024

- Executed a penetration test on a simulated corporate network, including Active Directory, Web Applications, and AWS Cloud, identifying vulnerabilities, assigning CVSS scores, and addressing OWASP Top 10 risks using the PTES methodology.
- Collaborated with a team to deliver professional reports, address client inquiries, and present strategic recommendations to non-technical stakeholders, showcasing technical expertise, communication, and leadership skills.
- Advanced to the Global Finals as one of the Top 15 teams from all regional qualifiers.