Aditya Dindi

adindi369@gmail.com | adityadindi.com | linkedin.com/in/adityadindi

Experience

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

- ➢ Conducted a comprehensive black-box web application security assessment on a custom-built application using the OWASP Top 10 framework, culminating in a detailed professional report that was presented to executive leadership.
- ➢ Performed whitebox penetration tests on Paycom's applications under the guidance of full-time security professionals, identifying vulnerabilities, documenting them in Confluence, and creating tickets in Jira to recommend improvements that enhance system security.
- ➢ Executed extensive code reviews on PHP code to identify and resolve security vulnerabilities, focusing on future maintainability and collaborating with an agile team to implement best practices and design patterns, utilizing Git / GitLab to manage and streamline the process of task completion.

Independent Security Researcher ***February 2024***

- ➢ Discovered improper input sanitization in a Microsoft Products web application, leading to stored Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) vulnerabilities, which posed a risk of account takeover affecting millions of users.
- ➢ Authored a comprehensive report detailing identified vulnerabilities and step-by-step reproduction instructions, ensuring clear communication of security risks and remediation strategies.

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

- ➢ Developed a firmware parser plugin for Ghidra, designed to address multi-architecture support commonly encountered in embedded systems using Java and Python.
- ➢ Conducted an in-depth literature review on Firmware Analysis Methodology in Binary Analysis of Embedded Systems, utilizing Zotero for effective organization, citation management, and reference tracking.

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

- ➢ Developed a MITRE ATT&CK Defender™ training course teaching a MITRE ATT&CK Technique and its sub-techniques with detailed Threat Research and Adversary Emulation testing.
- ➢ Researched the current state of the Army's Red Team and contributed to a report outlining a 5 year roadmap for the enhancement of the Army's Testing and Evaluation (T&E) capabilities.

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

- ➢ Performed a security assessment on a National Guard prototype designed to bolster critical infrastructure resilience. The pentest focused on identifying and mitigating vulnerabilities to enhance system reliability and protect against potential threats.
- ➢ Delivered a detailed report outlining findings, identified vulnerabilities, and provided remediation recommendations.

Certifications

- ➢ OffSec Certified Professional (OSCP)
- ➢ HackTheBox Certified Bug Bounty Hunter [In-Progress]
- ➢ CompTIA Security+
- ➢ CompTIA CySA+

Education

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

- ➢ Vice President and Security+ / CySA+ Mentor at the CompTIA Student Chapter
- ➢ Web Application Penetration Tester on UTSA Cyber Competitions Teams
- ➢ RowdyCon Lead Organizer and Finance Lead - UTSA Cybersecurity conference

Projects

Automated Cloud Cybersecurity Homelab

- ➢ Engineered a robust Cloud Cybersecurity Homelab in AWS (Amazon Web Services) using Terraform and AWS CLI, tailored for automated deployment of an attack vs defense range.
- ➢ This environment features a Kali Linux attacker machine, a Windows victim machine, and a Security monitoring machine running Ubuntu, equipped with advanced tools like Splunk and Nessus, enabling comprehensive security testing and analysis.

Competitions

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

- ➢ Conducted a full penetration test and identified vulnerabilities in a simulated corporate network infrastructure.
- ➢ Collaborated with a team to respond to client questions, discovered security gaps, and produced professional reports within tight deadlines, demonstrating both technical and business skills.
- ➢ Created and delivered executive-level presentations that effectively communicated complex technical findings and strategic recommendations to non-technical stakeholders, showcasing strong communication and leadership.