Aditya Dindi

[REDACTED] | adityadindi.com | linkedin.com/in/adityadindi | https://medium.com/@pyrus369

Professional Summary

A highly motivated cybersecurity professional with hands-on experience in penetration testing, vulnerability assessment, and secure code reviews. Proven ability to identify and mitigate security risks in complex environments through real-world engagements and security research. Strong communicator, adept at translating technical findings into actionable recommendations for executive leadership. Certified OSCP and CompTIA Security+ with a passion for continuous learning and cybersecurity innovation.

Education

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

- Lead Web Application Penetration Tester on the UTSA Cyber Competitions Team
- President and Security+ Mentor at the CompTIA Student Chapter
- Internet of Things (IoT) Lab Researcher
- Cyber Security Lab (CSL) Red Team Operator and Infrastructure Engineer

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

- 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.

Researcher, Army Educational Outreach Program Apprenticeship ***August 2023 - Present***

- 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.
- Developing a firmware parser plugin for Ghidra, designed to address multi-architecture support commonly encountered in embedded systems.
- Designing and codifying a hybrid firmware and binary analysis workflow and environment using free and open-source software.

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

- 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.
- 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.
- Created a mapping capability to showcase process flow and decision making of MITRE ATT&CK techniques. Identified various paths ATT&CK techniques can take that helps identify adversary and benign behavior to build better analytic detections.

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

- Conducted Penetration Testing for sensitive government web applications, collaborating with cross-functional teams to analyze results, prioritize risks, and develop mitigation strategies.
- Delivered a detailed report outlining findings, identified vulnerabilities, and provided remediation recommendations.

Certifications

- OffSec Certified Professional (OSCP)
- CompTIA Security+ — *Expires:* August 2027
- CompTIA CySA+ — *Expires:* August 2027
- OffSec Web Expert (OSWE) — *Expected Completion Date:* March 2025

Skills

- Internal, External and Application Penetration Testing
- Web Development: *HTML/CSS, Git/Github/GitLab*
- Programming / Scripting Languages: *Java, Python, Bash, PHP*
- Security Blogs / Writeups: *writeups.adityadindi.com*
- Crafting Comprehensive and Impactful Reports
- Active on TryHackMe, HackTheBox, Portswigger
- Exceptional Verbal and Written Communication
- Amazon Web Services (AWS) Penetration Testing

Achievements

- 2023-2024: *Collegiate Penetration Testing Competition (CPTC): Central Regional Champion (1st Place)*
- 2023: *Cal Poly Pomona SWIFT: King Of The Hill (KoTH) (1st Place)*
- 2022-2024: *Collegiate Penetration Testing Competition (CPTC): Global Finalist*
- 2023: *HackTheBox CAE CTF: Southwest Regional Champion (1st Place)*
- 2024*: National Cyber League Spring Team Game: Top 6%*
- 2023: *Sandia National Laboratories Tracer Fire 12: (3rd Place)*
- 2022: *National Centers Academic Excellence Cyber Games (NCAE): Regionals (3rd Place)*
- 2022: *Hivestorm: Nationals (4th Place)*

Projects

Automated Cloud Cybersecurity Homelab

- Engineered a robust Cloud Cybersecurity Homelab in AWS (Amazon Web Services) using Terraform, tailored for automated deployment of an attack vs defend 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.
- The lab supports hands-on experimentation with real-world scenarios in a controlled, scalable cloud environment.

Red Team Engagement, TryHackMe Red Team Capstone

- Performed a Red Team Assessment on a fictional company's internal and external networks, including all VPN-accessible IP ranges.
- Managed to compromise a parent and child domain controller in an Active Directory environment, gaining full system level access.
- Compromised multiple Linux and Windows workstations / servers running critical services such as VPN, WebMail, and Website, achieving full access on each, and delivered a comprehensive report detailing findings.

Competitions

Lead Web Application Penetration Tester, Collegiate Penetration Testing Competition (CPTC)

- Achieved 1st Place in the CPTC9 U.S Central Region competition and proceeded to qualify for the Global Competition.
- 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.

Web & Database Lead, Collegiate Cyber Defense Competition (CCDC)

- Focused on defending and maintaining a simulated corporate network infrastructure against live cyber attacks
- Managed and and secured various IT services, including servers, databases, and web applications, while responding to real-time incidents and implementing mitigation strategies
- Collaborated with a team to protect critical assets, develop defensive strategies, and prepare comprehensive reports for evaluation by industry professionals.