

PARAS SAXENA

parassaxenausa@gmail.com · +1(551)248-3207 Pittsburgh, Pennsylvania, USA, 15217 · <https://www.linkedin.com/in/paras-saxena-cmu/> · <https://paras98.github.io/portfolio/>

OBJECTIVE

Computer science graduate with a strong passion for security and privacy. Experienced in development and secure coding with over 3 years of work experience in various IT projects seeking full-time opportunities.

EDUCATIONAL QUALIFICATION

Carnegie Mellon University — Pittsburgh, PA — Master's in Information Security — Jan 2023 - May 2024

Major Computer Science

Courses Taken **Secure Coding**: Code analysis/ security reviews, secure coding practices, building a secure file system, **Hacking101**: Micro corruptions, AFL, CVE's replications and analysis **Introduction to Information Security**: Cryptography, Access Control, Vulnerabilities, Policy, Privacy, Management **Applied Information Assurance**: Defense-in-Depth, Foundations, Threats, Host Security, Network Security, Network Monitoring, Cryptosystems, Encryption, Incident Response, Digital Forensics, Security Protocol. **Cyber Risk modeling**: legal compliance, threat modeling, MITRE ATTACK, the Common Vulnerabilities and Exposures database, and popular risk frameworks (STRIDE, PASTA, NIST, Vulnerability Assessment, etc.) **Fundamentals of Telecommunication, Introduction to Computer Systems (15513), Browser Security*, Distributed Systems*, Cloud Security*, Ethical Penetration Testing*, Negotiations ***.

Jaypee University of Engineering and Technology — MP, India — Bachelor of Technology in Computer Science and Engineering — June 2016 - June 2020

Major: Computer Science

WORK EXPERIENCE

Carnegie Mellon University — **Research Associate** — Pittsburgh, USA — June 2023 - Present

- Developed a web application for combining public and shuttle transit systems, implementing network security protocols and web application security best practices to enhance data security and privacy.
- Designed to cater to the unique requirements of senior citizens, enhancing their mobility. Prioritized data security and privacy through strong protective measures.
- Incorporated user-friendly features for improved accessibility and ensured secure deployment for a reliable experience.

Carnegie Mellon University — **Teaching Assistant (Introduction to information security)** — Pittsburgh, USA — June 2023 - December 2023

- Setup of Lab(Ctf) server, executed recitation for homework, teaching, conducted Office hours to help solve doubts. responsible to mentor 13 students.
- Collaborated with TAs to invent new homework

Cognizant Technology Solutions India Pvt. Ltd. — **Associate (Developer)** — Pune, India — August 2020 - December 2022

- Successfully developed and maintained a secure customer-facing pharma platform with robust cybersecurity measures and a data privacy focus, reducing possible threat vectors on the platform, performed code reviews.
- Led a team of 4 developers in transforming a legacy web application to a new framework with enhanced security and functionality within time constraints.
- Developed automated secure deployments scripts using GitLab, integrating security tools for data protection, and created automated security testing scripts to streamline code audits and security checks, reducing deployment time by 70% and further reducing the cost.

PROJECTS

Enterprise Network Penetration Testing — (Feb 2024 – March 2024) Led a real-world simulated penetration test to identify and exploit vulnerabilities within an organizational network. Focusing on network security, vulnerability assessment, and strategic security recommendations.

AWS Cloud Security Enhancement and Optimization — (March 2024 - April 2024) — Strategically secured and optimized AWS infrastructure, focusing on encryption, access control, and threat detection across key AWS services such as S3, VPCs, and KMS. Executed best practices for infrastructure audits, compliance, cost management, and continuous monitoring using advanced tools like CloudTrail, CloudWatch, and AWS Config to enhance security posture and operational efficiency.

CVE's Exploartion — (September 2023 - December 2023) — Investigated and replicated CVEs, including Log4j, GoWasm, Cacti, and Ty-pora, by establishing the necessary environments. Conducted extensive research to identify and expand the attack surface, leading to the discovery of novel vulnerability vectors

Fuzzing (AFL) — (September 2023 - December 2023) — Utilized AFL for vulnerability discovery in binary files.

Buildit Breakit — (September 2023 – December 2023) — Created a secure file system from scratch, incorporating robust authentication and authorization mechanisms to enhance security. Also participated in breaking other teams' file systems to identify and exploit vulnerabilities.

Multiple Binary Exploitation — (September 2023 - December 2023) —ranging from Strings, Pointer, Memory, Integer overflow, and micro-corruptions.

Malloc Implementation — (September 2023 - December 2023) — from scratch implicit to explicit to segmentation to optimization via (footer less and mini blocks)

Malicious PCAP Dissection With Wireshark — (January 2023 – May 2023) — Conducting network post-attack forensics through Wire-shark to identify IOC which led to the identification of exfiltration method, infected devices, malicious activities, and the malware utilized by the attacker. Tools Used: Wireshark, Malware Databases, Network Protocols

CTF/System Exploitation — (PicoCTF, US Cybergames, Defcon31, Blackhat 2023) — Analyzed and exploited vulnerabilities due to buffer overflow such as stack canaries, ROP and JIMPESP gadgets, ASLR etc. Exploited website and android app vulnerable to stored XSS, SQL injection and Blind SQLi. Developed a python script using TOR proxies to bypass geo-based access restrictions by routing exit relays

across the globe.

Published Paper

Extension Auditing: Privacy-Preserving Extension (IRJET) — *April 2024*

Co-authored research paper published in Volume 11, Issue 04. Conducted extensive dynamic and static code reviews to identify and mitigate security vulnerabilities in digital extensions, Applied threat modeling techniques, API testing to assess and enhance application security.

TECHNICAL SKILLS

Security Tools: Metasploit, n-map., Wireshark, OWASP ZAP, AppScan, WebInspect, Fortify, Veracode, Checkmarx **Programming Languages:** C, Go, C++, Python 3, HTML, CSS, JavaScript, Apex, Aura **Frameworks/Libraries:** React.JS, Bootstrap, LWC.

CERTIFICATION

Certified in Cyber Security — **(ISC)²** — July 2023 — CCNA R&S — **Cisco** — August 2023

Introduction to Cyber Security Specialization — **NYU Tandon School of Engineering** — January 2021

In Progress — **AWS Certified Security - Specialty** — **Security+**

SKILLS

Security: Secure Coding Practices,Vulnerability Assessment, Cybersecurity Frameworks (MITRE ATT&CK, STRIDE, PASTA, NIST)
,Cryptography, Binary Exploitation, IDS, SIEM