Paras Saxena

(551) 248-3207 | parassaxenausa@gmail.com | LinkedIn | Portfolio

Professional Experience

Associate | Cognizant Technology Solutions   August 2020 – December 2022

- Engineered and upheld a customer-facing pharma platform with advanced cybersecurity measures and a data privacy focus, decreasing threat vectors by 30% and elevating platform security through regular code reviews.
- Supervised a team of 4 developers in transforming a legacy web application to a new framework, boosting security and functionality, and finishing project 2 months ahead of schedule.
- Created automated deployment scripts with GitLab, enhancing deployment speed by 70% and reducing costs by 25%.

Research Associate | Carnegie Mellon University   June 2023 – Present

- Built a web application integrating public and shuttle transit systems.
- Prioritized data security and privacy, implementing strong protective measures and achieving a 98% user satisfaction rate.
- Incorporated user-friendly features for improved accessibility and ensured secure deployment for a reliable experience.

Applied Cybersecurity Projects

- **Malicious PCAP Dissection with Wireshark:** Utilized Wireshark for post-attack forensics to identify IOCs, uncover exfiltration methods, infected devices, and attacker malware.
- **CTF/System Exploitation:** Conducted CTF/System Exploitation by identifying and exploiting buffer overflow vulnerabilities, including stack canaries, ROP, JMPESP gadgets, and ASLR. Penetrated and secured websites and Android apps vulnerable to stored XSS and SQL injection.
- **TOR Bypass :** Crafted and executed a Python script using TOR proxies to bypass geo-based access restrictions, effectively routing exit relays globally, and significantly enhancing penetration testing capabilities and security assessment accuracy.
- **CVE's Exploration:** Replicated and investigated major CVEs Log4j, GoWasm, Cacti, and Typora. Established test environments and conducted research to expand attack surface, discovering new vulnerability vectors.
- **Fuzzing (AFL):** Leveraged AFL fuzzing and secure code review tools Qualys and CodeQL to discover vulnerabilities in critical binaries such as OpenSSL, TCPDUMP, and VIM, enhancing security and robustness against malformed inputs.
- **Buildit Breakit:** Architected a secure file system with strong encryption, authentication, and authorization; pinpointed and exploited vulnerabilities in competing systems, resulting in a 20% security increase.
- **Multiple Binary Exploitation:** Conducted code review, code analysis, & reverse engineering of binaries, exploiting vulnerabilities strings, pointers, memory, & integer overflows on platforms ranging from 16-bit IoT devices to 32 and 64-bit systems.
- **Malloc Implementation:** Designed a dynamic memory allocator optimized for efficiency and speed, using techniques segmentation and mini-blocks, enhancing memory management performance by 25%.
- **Enterprise Network Penetration Testing :** Conducted a real-world simulated penetration test to identify and exploit vulnerabilities within an organizational network, concentrating on network security, vulnerability assessment, and strategic security recommendations, enhancing network security posture by 40%.
- **AWS Cloud Security Enhancement and Optimization :** Enhanced AWS infrastructure with encryption, access control, and threat detection across S3, VPCs, and KMS, utilizing CloudTrail, CloudWatch, and AWS Config, boosting security posture and operational efficiency by 30%.

Skills

- **Tools:** Wireshark, Security Onion, pfSense, Kibana, Endian Firewall, Arpatch, OSSEC, Splunk, BeEF, ClamWin, Arkime, Snort, Squirt, Squid, vSphere, SalesForce, JIRA, GitHub, Metasploit, Nmap, SSO, MFA, OAuth, SAML, API Gateways.
- **Technologies:** Linux, VMWare, LDAP, Identity and Access Management, Active Directory, Docker, SQL, Azure, NIST Framework, MITRE ATT&CK Framework.
- **Programming Languages:** C, Go, C++, Python, HTML, CSS, JavaScript, Apex, Aura.

Certifications

- Security+ **CompTIA**   May 2024
- Certified in Cyber Security **(ISC)[2]**   July 2023
- CCNA R&S **Cisco**   August 2020
- In Progress **AWS Certified Security - Specialty** , **OSCP** , **CRTP**

Education

Carnegie Mellon University | Master of Science in Information Security   January 2023 – May 2024

- Courses: Information Security, Ethical Penetration Testing, Computer Networks, Secure Coding, Introduction to Computer Systems (15513), Browser Security, Distributed Systems, Cloud Security, Hacking 101.

Jaypee University of Engineering & Technology | Bachelor of Technology, Computer Science   June 2016 – June 2020

Accomplishments

- Published a paper on — Extension Auditing: Privacy-Preserving Extension (link).
- Led a team project at Cognizant, delivering a secure web application ahead of schedule.
- Achieved a 98% user satisfaction rate for a secure web application developed at Carnegie Mellon University.