

Rejen Thompson

Cybersecurity Enthusiast — VAPT Specialist

+91 7418242633

rejen22110019@snuchennai.edu.in

rejen-thompson

GitHub

Blog

Professional Summary

Cybersecurity enthusiast with hands-on experience in offensive security, vulnerability assessment, and penetration testing. Proven expertise in identifying critical vulnerabilities (e.g., XSS, SQLi, IDOR), developing security tools, and contributing to CVE databases. Aiming to leverage technical skills in VAPT roles to enhance organizational security postures.

Education

Shiv Nadar University, Chennai

GPA: 8.0/10

Relevant Courses: OS, Computer Networks, Cybersecurity, Cryptography, Network Security, Cloud Security, System Security, Cyber Forensics, Web Technologies

Thamarai International School, Thanjavur

Experience

CyberXtron - Offensive Security Engineer

January 2024 - August 2024

- Conducted **penetration tests** and identified 7 critical vulnerabilities (1 CVE) in PHP Gurukul, including **XSS, SQL Injection, and IDOR**, protecting 5,000+ users.
- Developed **ShadowSpot**, an EASM tool to detect exposure in external assets and monitor vulnerabilities.
- Engineered **DarkFlash**, a dark web monitoring system, utilizing advanced scraping techniques and Elasticsearch pipelines.
- Enhanced **Elasticsearch workflows** for seamless data ingestion from external sources, improving log management.

Bridge - Technical Cybersecurity Content Writer

November 2024 - December 2024

- Authored technical content on **cybersecurity topics**, including vulnerability assessments and hands-on lab scenarios.
- Simplified complex concepts for diverse audiences, enhancing content accessibility and engagement.

Projects

Security Vulnerability Monitoring System [Python, ELK Stack, Docker]

Sep - Oct 2024

- Designed and implemented a **real-time monitoring system** for global threat tracking, visualized in Kibana.
- Developed **centralized log management pipelines**, optimizing ingestion and visualization workflows.
- Leveraged Elasticsearch and Logstash to create structured, scalable data processing pipelines.

SecureAuth [Python, MySQL, Cryptography]

May 2024

- Implemented **AES-256 encryption** and **HMAC** for secure credential storage and data integrity.
- Utilized **prepared statements** to prevent SQL injection and built modular components for user management.
- Ensured secure session management and implemented robust authentication mechanisms.

Skills

- Programming Languages:** Python, C, SQL
- Frameworks and Methodologies:** MITRE ATT&CK, PASTA, OWASP TOP 10
- Penetration Testing Tools:** Burp Suite, Metasploit, Nessus, Nmap, ZAP
- Network and Cloud Tools:** AWS, Wireshark, Bettercap, Aircrack-Ng
- Log Analysis Tools:** Kibana, Elasticsearch, Logstash

Certifications

- Google Cybersecurity Professional Certificate Feb - May 2024
- TCM Security - Practical Ethical Hacking, OSINT, Bug Bounty Nov - Dec 2024
- INE Security - EJPT (In Progress)
- TryHackMe - Advent of Cyber 2024 Dec 2024

Achievements and Bug Bounty

- Identified and exploited **insecure API endpoints** in a travel website's payment gateway, leading to unauthorized transaction manipulation. Findings led to securing 1,000+ monthly transactions.
- Discovered and reported 7 critical vulnerabilities in **PHP Gurukul**, leading to **1 CVE** and securing 5,000+ users.
- Achieved top placements in CTF competitions: 4th in Edita CTF, 6th in VIT CTF.
- Completed **30+ TryHackMe rooms** and engaged in PortSwigger Labs, OWASP Juice Shop, and Natas.
- Organized **Freshers' Day 2024** and led the core team for a major college event.