Suman Kumar Chakraborty

✉ chakrabortysuman487@gmail.com ☎ +91-9836756767 in https://www.linkedin.com/in/suman-chakraborty-b857901b1

PROFILE SUMMARY

Curious and driven security researcher with a focus on field of penetration testing, red team simulations and developing security tools. Committed to advancing cybersecurity through innovative research and creative solutions.

PROFESSIONAL EXPERIENCE

Zeron

Research And Development Associate — Jul 2023 – present
Remote, India

- Developed Risk Scoring Model for EASM increasing accuracy of the existing model by 80%.
- Enhanced the EASM core engine, widening attack surface detection by 38%.
- Designed KPIs, data points, and customer flows for intuitive navigation increasing attention retention from 40% to 60%.
- Performed penetration testing and red team engagements of over 13 clients.

Security Research Intern — Nov 2022 – Jun 2023
Kolkata, India

- Took part in penetration testing activities of more than 7 clients with detailed reporting.
- Developed 37% of the core in the initial phases of External Attack Surface Management (EASM).

IEMLabs — Oct 2022 – Nov 2022
Cyber Security Research Intern — Kolkata, India

- Participated in VAPT of 3 clients with detailed professional reporting.
- Conducted more than 4 security awareness campaigns for government agencies.

EDUCATION

Bachelor of Computer Applications — 2020 – 2023
Institute of Engineering & Management, Kolkata — Kolkata, India
CGPA - 9.33
Top 0.6% of batch BCA 2020-23

CERTIFICATES

Certified Red Team Professional (CRTP) ↗
Altered Security
Issued Dec 2024 - Expires Dec 2027
Student ID: ADLID8228

Certified Ethical Hacker(CEH) Practical ↗
EC-Council
Issued Aug 2022 - Expires Aug 2025
Certification Number: ECC9364701528

ACKNOWLEDGEMENTS

Privilege Escalation Vulnearbility ↗ — Jan 2024
Docker Inc.

- Identified critical privilege escalation vulnerability in Docker Desktop Installer release page.

PROJECTS

SubPDF ↗

- Python-based tool for extracting domains and subdomains from PDF files. Supports multi-threading for fast, concurrent processing of multiple PDFs. Helps in increasing the attack surface by atleast 20%.

Bucket Hunter ↗

- Python based tool for discovering and analysing cloud storage buckets including AWS S3, GCP Storage, Azure Blob, DigitalOcean Spaces and Alibaba Cloud OSS Helps identify accessible buckets, extract useful data and simplify file exploration.

GodGenesis ↗

- Python3 based Command and Control framework focused on post-exploitation and evasion, ranked 5th among top 7 security tools of 2023 by Offensive Security Offers. This tool was also featured on YouTube by TrTec with sponsorship from CYNET

PUBLICATIONS

CVE-2024-39904: High Severity (CVSS 8.8) Code Execution Vulnerability in VNote via Local Path Traversal ↗ — Jul 2024
Vnote

- Discovered and fixed a CVSS 8.8 (high) level severity code execution vulnerability in VNote prior to version 3.18.1 caused by local path traversal, enabling arbitrary program execution via crafted file:/// ↗ URI links.

Vulnerability Weightage and Prioritization Model: Derived from Real Data and Community Insights — Jul 2025
IEEE COMPSAC

- Developed a dynamic vulnerability prioritization model integrating CVSS, EPSS, CWE, CAPEC, and real-world threat data for accurate risk assessment. Improved vulnerability management by calculating weighted scores based on exploitation trends, advisories, and community-driven intelligence

Extending the Attack Graph Model: Integrating Reconnaissance Stages — Jul 2025
IEEE COMPSAC

- Extended the NIST Attack Graph Model by integrating reconnaissance phases, enabling more realistic cyber risk quantification.Demonstrated efficacy through a detailed case study, showing improved overall vulnerability metrics and refined attack path modeling.

Vendor PulseGen: Generative Vendor Risk Management Platform — Jul 2025
IEEE COMPSAC

- Designed and implemented quantitative risk scoring models (QRS, CRS, ESR) for vendor assessment using structured inputs and CVE-based analytics. Enabled explainable, LLM-integrated scoring pipelines without fine-tuning, ensuring privacy-preserving and modular VRM evaluations.