Kaushal Mallya

CyberSecurity Analyst | CRTP | eJPT

+91 866 044 9019
kaushal.mallya.1@gmail.com
linkedin.com/in/chaeyib
Bengaluru, India

SUMMARY

Motivated CyberSecurity Analyst with 3+ years of hands-on experience in identifying and reporting security vulnerabilities. Proven ability to adapt to evolving threats and technologies, coupled with a passion for continuous learning and professional development.

PROFESSIONAL EXPERIENCE

LTIMindtree

Senior Consultant - Information Security ***Aug 2024 - Present***

- Designed and implemented advanced detection mechanisms for an Endpoint Detection and Response (EDR) product, aligned with the MITRE ATT&CK framework.
- Developed and optimized detection rules, reducing false positives and ensuring precise alerting for malicious activities.
- Investigated and graded customer-reported security incidents, delivering actionable recommendations and strengthening defenses.
- Collaborated with cross-functional teams to enhance detection capabilities and align EDR functionalities with evolving threat landscapes.

ZeroFox

Vulnerability Analyst ***Jun 2023 - Aug 2024***

- Identified and reported 50+ vulnerabilities across web and network infrastructure.
- Escalated critical alerts to customers, ensuring timely resolution of high-priority issues.
- Conducted in-depth penetration testing for web applications and Active Directory environments, uncovering critical misconfigurations and recommending remediation.
- Designed payloads to bypass advanced security measures.

Associate Analyst ***May 2021 - Jun 2023***

- Automated all daily processes using Python scripting, increasing operational efficiency to 100% and eliminating manual workload.
- Produced detailed CVE analysis reports in collaboration with Threat Intelligence teams, enhancing threat landscape visibility.

Group Cyber ID Technologies

Digital Forensic Intern ***Apr 2021***

- Investigated digital evidence for 10+ forensic cases in collaboration with law enforcement agencies, supporting legal investigations and resolutions.
- Analyzed diverse evidence formats, including smartphones, CCTV footage, and hard drives, ensuring legal compliance and accuracy in reporting.

TechIQ Labs

Security Intern ***Nov 2020***

- Implemented and managed Sophos Intercept X for Endpoint Security for workstations.
- Installed SSL certificates on various servers for internal testing.

EDUCATION

M. Sc. in Cyber Forensics & Information Security (pursuing)
University of Madras, Chennai 2022 - Present

PG Diploma in Cyber Security & Cyber Forensics
Raksha Shakti University (now Rashtriya Raksha University), Gujarat 2019 - 2020

B. Sc. in Forensic Science
Jain University , Bengaluru 2016 - 2019

CERTIFICATIONS

Certified Red Team Professional (CRTP)
Pentester Academy — Jul 2022

Junior Penetration Tester (eJPT)
INE — Apr 2022

Certified Ethical Hacker (CEH)
EC-Council — Mar 2021

PROJECTS

amass, OWASP
Contributed to the OWASP command-line attack surface mapping tool by identifying bugs, analyzing the source code, and reporting issues to developers, enhancing its functionality.

SKILLS

- **Technical:** Web Application Security, Network Penetration Testing, EDR Detection Engineering
- **Programming:** Python, Bash
- **Soft Skills:** Analytical Problem-Solving, Effective Communication

TOOLS

- **Scanning & Exploitation:** nmap, nuclei, ZAP, DefectDojo, BurpSuite, amass, sublister, katana, gobuster, ffuf, sqlmap, dalfox, hydra
- **Post-Exploitation:** PowerSploit, BloodHound, Mimikatz, Metasploit Framework, linpeas, winpeas
- **Scripting & Forensics:** Python, Jadx, Apktool, Wireshark, OllyDbg, Ghidra, IDA

AWARDS

Star Impact - 2023
Recognized for exceptional contributions to streamlining organizational workflow by automating processes and for identifying critical vulnerabilities, and delivering actionable remediation strategies that significantly improved client security postures.