Divakar K

divakar.k2023@gmail.com | +91 93420 06729

SUMMARY

- SOC and Cloud Security–focused Cybersecurity Engineer with hands-on experience in log analysis, network monitoring, Linux security, and vulnerability assessment. Actively collaborates in lab-based incident detection and cloud security simulations using IAM and secure monitoring practices to strengthen overall security posture.

EXPERIENCE | Internship

4th Aug - 20th Sep | Elevate labs

- Performed penetration testing on multiple web and mobile applications using automated and manual techniques aligned with OWASP Top 10, identifying critical flaws such as XSS, SQL Injection, and authentication bypass issues.
- Executed vulnerability scanning and service enumeration using Nmap, Burp Suite, and manual payload crafting, successfully detecting SQL injection, XSS, IDOR, and authentication flaws with high accuracy.
- Executed vulnerability scanning, reconnaissance, and service enumeration using Nmap and Burp Suite, improving detection coverage across exposed endpoint.
- Validated security controls by performing post-remediation retesting, ensuring exploited vulnerabilities were fully patched and eliminating recurrence of critical flaws.

PROJECTS

WEBSITE VULNERABILITY SCANNER | WEB SECURITY PROJECT

2025 – 2026 | Self Project

- Built a Python-based web vulnerability scanner using Flask and BeautifulSoup to detect XSS, SQL Injection, and CSRF vulnerabilities aligned with OWASP Top 10, with an integrated dashboard for streamlined vulnerability reporting and triage.
- **GitHub:** WEB-APPLICATION-VULNERABILITY-SCANNER

TOR DEANONYMIZATION FORENSICS SYSTEM | Hackathon

2025 – 2026 | Team Project

- Simulated a Tor network using Chutney for relay-level forensic traffic analysis, engineered features from captured data, and built an XGBoost–based detection model to identify deanonymization patterns, delivering a compact cybersecurity ML solution through team collaboration.
- **GitHub:** TOR-DEANONYMIZATION-FORENSICS-SYSTEM

SQL INJECTION DETECTION | WEB SECURITY PROJECT

2025 - 2026 | Personal Project

- Built a SQL Injection practice lab using Flask and PHP to demonstrate vulnerable vs. secure query handling, and developed a Python–based detection engine to identify malicious payloads and log real-time attack attempts for forensic analysis.
- **GitHub:** SQL-INJECTION-DETECTION

EDUCATION

RAJALAKSHMI INSTITUTE OF TECHNOLOGY

Bachelor of Computer and Communication Engineering
Expected July 2027 | Chennai - 600010
CGPA: 7.2 / 10

SKILLS

PROGRAMMING

Python • Java • MySQL

CYBERSECURITY - TOOLS

Nmap • Burp Suite • Metasploit Framework • Wireshark • SQLmap • OWASP ZAP • Splunk
Gobuster • Hydra • Tenable Nessus • Git/GitHub • Linux • Windows

SOFT SKILLS

Communication • Problem Solving • Logical Thinking • Adaptability

CERTIFICATIONS

- CCEP – Red Team Leader
- AWS Cloud Certification
- AWS Security Encryption
- CyberSecurity – Cisco
- GRC | Mindset, Methods, Skills
- ISO/IEC 27001:2022 INFORMATION SECURITY ASSOCIATE™

LINKS

Github: **Divakar-K**
LinkedIn: **Divakar-K**
Portfolio: **Divakar-K-Portfolio**