Ritvik Singh

+91 9779720974 — singhritvik1411@gmail.com — LinkedIn — GitHub — Portfolio

Objective

Cyber Security Analyst with experience in vulnerability assessment, web application security, SIEM monitoring and incident response support. Skilled in security analysis, log investigation and strengthening enterprise security through practical cybersecurity solutions.

Experience

Cyber Security Analyst Mar 2025 – Present
Cybrotech Digiventure Pvt. Ltd., New Delhi *cybrotech.us*

- Conducted Web Application and Network Penetration Testing aligned with the OWASP Top 10, identifying injection flaws, authentication weaknesses, privilege escalation paths, and security misconfigurations.
- Performed vulnerability assessments using Nessus and Nmap, analyzed CVEs, and delivered risk-based remediation recommendations.
- Designed and implemented Data Loss Prevention (DLP) policies for endpoint monitoring, sensitive data protection, and unauthorized file transfer detection.
- Monitored and investigated security events using Wazuh SIEM, performing log analysis, event correlation, alert investigation, and incident triage.
- Developed security documentation including risk assessments, vulnerability assessment reports, and security policies aligned with ISO/IEC 27001:2022 while collaborating with development teams to improve API security and secure coding practices.

Technical Skills

Cybersecurity: Vulnerability Assessment & Penetration Testing (VAPT), Web Application Security, API Security, OWASP Top 10, MITRE ATT&CK, SIEM, Incident Response

Security Tools: Burp Suite, Wazuh, Nmap, Metasploit, Wireshark

Programming: Python, SQL, Bash

Technologies: FastAPI, React, Node.js, PostgreSQL, Docker, Nginx

Certifications

Certified Ethical Hacker (CEH v13) — EC-Council 2024
Credential ID: ECC5182964073 — Certificate

Google Cybersecurity Professional Certificate — Coursera 2024

Introduction to Cybersecurity — Cisco 2024

Projects & Security Research

SentinelASM – Attack Surface Management (ASM) Platform GitHub React • FastAPI • PostgreSQL

- Built a full-stack Attack Surface Management (ASM) platform that automates **8+ external security checks**, including asset discovery, vulnerability assessment, and risk scoring.
- Implemented DNS enumeration, WHOIS lookup, SSL/TLS inspection, HTTP security header analysis, TCP port scanning, technology fingerprinting, and SPF, DKIM, and DMARC validation.
- Integrated CVE intelligence, AI-assisted remediation, JWT authentication, interactive dashboards, PDF reporting, and Docker-based deployment using SQLite (development) and PostgreSQL (production).

Data Loss Prevention (DLP) System GitHub React • Node.js • PostgreSQL • .NET

- Designed an enterprise Data Loss Prevention (DLP) platform supporting **6+ endpoint monitoring capabilities** for centralized policy management and incident response.
- Implemented file activity monitoring, sensitive data detection, clipboard monitoring, screenshot capture, USB/device control, and policy-based enforcement.
- Architected a scalable solution using React, Node.js, PostgreSQL, and a C#/.NET Windows agent, with local deployment and planned migration to a secure VPS using Nginx and HTTPS.

SafeSphere – Personal Cybersecurity Platform GitHub

- Built a full-stack cybersecurity platform for phishing detection, social engineering analysis, website reputation assessment, email security analysis, QR code verification, and password security using threat intelligence and OCR.
- Developed a scalable SaaS application using React, FastAPI, PostgreSQL, Redis, and Docker featuring AI-assisted threat analysis, SPF/DKIM/DMARC validation, personalized security scoring, and real-time security recommendations.

TryHackMe Writeups Collection GitHub

- Published **12+** technical walkthroughs covering enumeration, privilege escalation, web exploitation, Active Directory, and Windows/Linux penetration testing.

BadUSB / HID Injection Demonstration GitHub Digispark • Arduino

- Developed a Digispark-based HID injection proof-of-concept demonstrating automated keyboard emulation, payload execution, and defensive techniques against USB-based attacks.

Education

Bennett University Greater Noida, Uttar Pradesh
Bachelor of Technology in Computer Science and Engineering *2022 – 2026*

∗ Relevant Coursework: Cybersecurity, Network Security, Cryptography, Computer Networks, Operating Systems.