Vikash Bharti

+91 7250224540 | cybersheenu@gmail.com | https://www.linkedin.com/in/vikashbharti21/

CAREER OBJECTIVE

Seeking an opportunity in cybersecurity to utilize my foundational skills in threat detection, penetration testing, and incident response, while growing into a skilled security professional and contributing to the organization's security posture.

PROJECTS

Vulnerability Assessment of a Web Application

- Indentified and reported 15+ vulnerability using OSWAP Top 10 methodology.
- Performed vulnerability scanning and manual testing on a demo web application to identify issues like SQL Injection, XSS, and Broken Authentication.
- **Tools:** Burp Suite, OWASP ZAP

Web Recon

- Performed reconnaissance on a test domain using subdomain enumeration, port scanning, and directory brute forcing
- **Tools:** Nmap, Subfinder, Dirsearch
- **Outcome:** Learned real-world scanning and recon methodology used in bug bounty.

Log Analysis & Incident Detection

- Analyzed system logs and security alerts to detect brute-force attempts, unauthorized access, and malware indicators.
- **Tools:** SIEM (Splunk/Wazuh), Linux Logs
- **Outcome:** Developed understanding of SOC operations and incident response workflow.

EDUCATION

GNIOT Institute of Professional Studies **Sep 2024 - 2027**

Bachelor of Computer Applications, Computer Applications

- **GPA:** 70%/7.3%

KEY SKILLS

- **Network Security**: Network Security, Basic knowledge of TCP/IP, packet analysis, and detecting suspicious traffic.
- **Penetration Testing Basics**: Penetration Testing Basics, Hands-on practice in recon, scanning, and exploiting common vulnerabilities
- **Vulnerability Assessment**: Skilled in identifying and analyzing security weaknesses in web and network systems.

CERTIFICATIONS

- **Computer Networks Fundamentals:**Cyber Quince
- **Learn Cyber Security From Scratch: Practical Guide**
- **Cybersecurity and Ethical Hacking**
- **eJPT**

ACHIEVEMENTS

- **TryHackMe:**Ranked in top **33%** on"Active Learner on TryHackMe.
- Successfully exploited OWASP Top 10 vulnerabilities in lab environments
- Completed multiple online cybersecurity challenges and labs
- Participated in Capture The Flag (CTF) events and solved multiple challenges.