# Vansh

+91 78892-26115 | vanshbr2013@gmail.com | Portfolio | /vansh123 | /cs-vansh | Blog

## Experience

**Information Security Analyst**
Max Conformance — Sep. 2023 – Present

- Acquired knowledge about information security, compliance, and risk management.
- Managed infosec compliance with standards like ISO/IEC 27001:2022 by developing policies & procedures, implementing controls and leading security awareness training.
- Conducted security audits and performed risk assessments to evaluate the effectiveness of implemented controls.

## Education

**Bachelor of Technology – Computer Science** — CGPA : 9.35/10
Bhagwan Parshuram Institute of Technology — Nov. 2021 – Jun. 2025

**Coursework**: Data Structures and Algorithms, Object-Oriented Programming, Computer Networks, Operating Systems, Database Management System, Software Engineering

## Certifications

**Certified AppSec Practitioner** — Cert. ID - 9186113
The SecOps Group — Oct. 2024

- Certification on core web application security knowledge in vulnerability detection & exploitation and mitigation strategies.

**Google Cybersecurity Professional Certification** — Cert. ID - FNHXLPXAW6LA
Coursera — Apr. 2024

- Developed understanding of security principles, network protocols, and practical application of Linux, SQL, and Python.
- Explored dynamics of assets, threats, and vulnerabilities, gaining insight into cybersecurity risk management.
- Employed packet capture for anomaly detection, and learned about IDS, IPS, and SIEM tools for security monitoring.

## Projects

**Ticket Management System** | *Django* | Github

- A web application designed as an Incident Manager for small organizations.
- Developed functionalities for Customers to create and view tickets, and for Engineers to manage, track, and resolve tickets.
- Created visual components to compare different ticket statuses and track ticket resolutions over time.

**Timing Based Covert Channel** | *Python* | Github | Medium

- Developed a proof of concept for a timing-based covert channel to demonstrate covert communication techniques.
- Encoded data in binary and transmitted it via HTTP requests, using network latency to infer information from timing gaps.
- Enabled data reconstruction on the server by measuring time intervals between requests for accurate decoding.

**CyberArmory** | *Python* | Github

- Developed a cybersecurity tool designed to be used from the Command Line Interface (CLI).
- Implemented tools like Password Crackers (Dictionary and Bruteforce), WHOIS and IPWHOIS Lookups, SYN Flood, VirusTotal Scan, Recursive Directory Lister, and IP Geolocator.

**Other Projects**: *File Integrity Monitor* | *Bandwidth Monitor* | *Port Scanner*

## Skills

**Cybersecurity**: Risk Assessment and Management, Security Standards and Frameworks, Threat Detection and Mitigation
**Programming Languages**: C++, Python, Java
**Web Development**: HTML, CSS, JavaScript, Django
**Tools**: Linux Shell(Bash), PowerShell, Command Prompt (cmd), Git
**Soft Skills**: Attention to Detail, Problem-Solving, Critical Thinking, Leadership, Communication, Adaptability

## Milestones

Profile | **Ranked in Top 4% on TryHackMe** – Working on improving VAPT skills
Article | **Discovered IDOR in College's Third Party ERP** – Uncovered a vulnerability to access student records (SPII).
**Ranked among Top 3 in an Ideation Challenge at IIT Jammu** – Devised a solution for tracking police officers, ensuring their presence at assigned duty locations to mitigate theft and improve law & order.