Anshul Choudhary

LPU, Phagwara, Punjab 144411 India
☎ +91 7413864904 • ✉ anshulchoudhary227@gmail.com
in https://linkedin.com/in/0xrad1ant • https://github.com/0xrad1ant

Objective

To secure a challenging role as a Cybersecurity Analyst in a reputed organization where I can utilize my skills in vulnerability assessment, penetration testing, and secure application development, contribute to impactful projects, and grow as a professional while achieving organizational goals.

Education

Lovely Professional University **Jalandhar, Punjab**
Bachelor of Technology in Computer Science and Engineering, CGPA: 6.2 *2026*
Relevant Coursework: Data Structures and Algorithms, Operating Systems, Database Management Systems, Artificial Intelligence, Computer Networks, Software Engineering

Yadav Public School **Jodhpur, Rajasthan**
Senior Secondary School Certificate (12th Grade), Percentage: 78% *2022*
Key Subjects: Physics, Chemistry, Mathematics, Computer Science

Yadav Public School **Jodhpur, Rajasthan**
Secondary School Certificate (10th Grade), Percentage: 82% *2020*
Achievements: School Topper, 2nd rank in SOF

Technical Skills

Programming Languages: Python, Shell Scripting, Bash

Tools/Technologies: Git, Docker, Burp Suite, Metasploit, Nessus

Operating Systems: Linux, Windows

Databases: MySQL

Frameworks: React.js, TensorFlow

Projects

Project Title: *BurnBin – Secure One-Time Notes*
Description: Developed a secure note-sharing application using Cloudflare Workers and KV storage. The system allows users to post confidential messages and receive a one-time access link. Notes self-destruct upon being accessed, ensuring secure and ephemeral data transmission.
Technologies Used: Cloudflare Workers, KV Storage, JavaScript, HTTP APIs, UUID
Impact/Achievements: Enabled secure flag/password sharing in CTF environments and private communications. Gained practical experience in serverless deployment and secure ephemeral data handling.
Demo/Code Link: https://bin.itsradiant.me

Project Title: *Malware Analysis Sandbox*
Description: Set up a sandboxed virtual machine to safely analyze malware behavior using reverse engineering and network traffic analysis. Documented how malware interacts with the system and network, identifying key patterns and behaviors.
Technologies Used: VirtualBox, Wireshark, Ghidra, IDA Pro.
Impact/Achievements: Gained hands-on experience with malware analysis and reverse engineering, improving threat intelligence and incident response skills.
Demo/Code Link: NA

Project Title: *Host and Monitor a Honeypot*
Description: Deployed and configured a honeypot to simulate vulnerable services and attract real-world attackers. Integrated logging and monitoring tools to analyze attack patterns.
Technologies Used: Cowrie, VM Ware
Impact/Achievements: Collected real attack data, enhanced understanding of attacker behavior, and strengthened skills in threat detection and response.
Demo/Code Link: NA

Project Title: *Custom OSINT & Web CTF Challenges*
Description: : Designed and hosted a series of OSINT and Web-based Capture the Flag challenges aimed at sharpening investigative and exploitation skills. The challenges required participants to uncover hidden social media handles, analyze Wayback Machine archives, bypass client-side restrictions, and solve obfuscated audio clues.
Technologies Used: JavaScript, Cloudflare Workers, Wayback Machine, DTMF encoding, Bash scripting, HTML/CSS, Web exploitation techniques.
Impact/Achievements: Developed a publicly accessible CTF platform that simulates real-world scenarios, helping participants enhance their OSINT, enumeration, and web exploitation capabilities.
Demo/Code Link: ctfd.decrypt4.me

Certifications

NA

Achievements

TryHackMe Performance: Ranked in the top 8% globally on TryHackMe cybersecurity challenges.

Hosted Custom CTF Challenges: Designed and deployed publicly accessible OSINT and Web-based CTFs that simulate real-world scenarios, sharpening the skills of hundreds of participants.

Cybersecurity Lead – TFUG Jalandhar: Leading the cybersecurity track at TensorFlow User Group (TFUG) Jalandhar. Organizing workshops, CTFs, and hands-on sessions to foster learning and collaboration in the local security community.