VISHAl KUMAR

Offensive Pentesting | Web dev

Contact

imvyadaw@gmail.com
+91 8804645646
https://www.linkedin.com/in/imvyadaw/
https://github.com/imvyadaw
Alistonia Estate, Pi I & II, Greater Noida, Uttar Pradesh 201310

About Me

Final-year Computer Science diploma student focused on ethical hacking and penetration testing. Skilled in identifying vulnerabilities, exploiting weaknesses ethically, and improving security posture. Passionate about cybersecurity, automation, and continuous learnin

Technical Skills

- **Programming Language** : C, C++,Python, JavaScript, Java ,Html,Css
- **Web development (backend Django)**
- Kali Linux, Nmap, Metasploit, Wireshark, SQLmap, Hydra, John the Ripper, Hashcat, Aircrack-ng
- Network & Web Penetration Testing,
- **Databases**: MySQL, MongoDB
- **Version Control**: Git, GitHub

Soft Skills

- Communication, Teamwork, Problem-Solving
- Time Management, Adaptability
- Leadership, Discipline, Accountability

Certifications

- • Introduction to Cybersecurity – (Completed: 19 Feb 2025) | Learned fundamentals including CIA triad, firewalls, threats, and cryptography.
-
- Learn Ethical Hacking From Scratch (Udemy)
- Instructor: Zaid Sabih | (Completed Oct 2025)

Education

- **Diploma in Computer Science** at IIMT University, Greater **Noida** (8.50 GPA) (2023-2026)
- **Secondary School Certificate – Shri Parshuram Giri +2** High School (BSEB, Bihar), 56.24% (2023)

Projects

1. **Personal Portfolio Website** – Responsive portfolio with animations (HTML, CSS, Django)
2. **Login Page Project** – Interactive login page with validation (HTML, CSS, JS)
3. **Animation Page Project** – Dynamic -based animated web page (HTML, CSS, JS, GSAP)

Internship

- **Web Development Internship – CodSoft** ***(Jul 2025 – Aug 2025)***
- **Cyber Security – InternPE** ***(6 October 2025 – 2 November 2025)*** **Best Performer –Offensive Pentesting for beginners**

Professional Summary

- Motivated cybersecurity student with hands-on experience in ethical hacking, penetration testing, and vulnerability analysis. Skilled in using industry tools like Kali Linux, Burp Suite, Nmap, Metasploit, and Wireshark for assessing security risks and testing real-world attack surfaces. Comfortable with scripting in Python and Bash for automation and basic exploit customization, SQL injection, XSS, and common security misconfigurations. Focused on continuous learning, responsible security practices, and building technical depth to grow as an offensive security professional.