Rajan Kumar Barik

rajankumarbarik143@gmail.com DIGITALRAJAN22M rajan-kumar-barik anondgr

PROFESSIONAL SUMMARY

- **Offensive Security Engineer** with hands-on experience in penetration testing, bug bounties, and exploit research. Ranked in the top 2% of global cybersecurity competitions, actively securing applications through ethical hacking and red teaming.
- Committed to Continuous Learning & Staying Updated with the latest cybersecurity trends, tools, and attack techniques.

INTERNSHIP & EXPERIENCE

[VAPT Researcher & Bug Hunter] – [NullClass **]** Remote ***(****07/2024 – 08/2024****)***

- Conducted penetration testing on 3 **web apps** and 3 **Windows** systems, identifying and mitigating **15+** security vulnerabilities, reducing potential attack surface by **40%**.
- Performed **live bug hunting on HackerOne and Bugcrowd**, successfully reporting **3 valid security vulnerabilities**.
- Authored a **technical blog** analyzing the exploitation of a hard-difficulty active Hack The Box (**HTB**) machine, demonstrating **advanced penetration testing** techniques and in-depth vulnerability analysis.

EDUCATION

[Bachelor Of Computer Applications] – [Fakir Mohan University **]** *(Sep 2022 – Apr 2025)*

- **GPA: 8.5/10**

SKILLS

TECHNICAL SKILLS

Information Security

1. Penetration Testing (Web, APIs, Networks,) VAPT/WAPT
2. Active Directory & Cloud (AWS)
3. Threat Modeling & Source Code Review
4. Threat Research
5. Reverse Engineering & OSINT

Tools

1. **DAST:** Burpsuite
2. **SAST:** Snyk
3. **Pentesting:** Burpsuite,Wireshark,Metasploit,Nmap,Ghidra,Aircrack-ng,Impacket,BloodHound, Dirbuster,Nikto,John the Ripper,Hydra,Gobuster,SQLmap,Responder,Commix,Ffuf, ZAP (OWASP ZAP),Nessus,Hashcat,Amass,Shodan,Censys,BeEF,Sublist3r,Masscan,Evil-WinRM

Programming

1. C , C++ , Python , Bash (Intermediate)
2. Java , php , JavaScript , MySQL (Beginner)

SOFT SKILLS

- Critical Thinking & Problem-Solving
- Effective Communication & Team Collaboration
- Attention to Detail & Research Mindset
- Leadership & Mentorship

PROJECTS

[Anondgr] – [TryHackMe **]** (*02/2025 – Present*)

- Designed and developed a custom **TryHackMe** room focusing on Enumeration, Linux Privilege Escalation, and Steganography to enhance hands-on cybersecurity skills.
- Created **realistic attack scenarios** that simulate real-world security vulnerabilities, providing an engaging learning experience for security enthusiasts.

[Dgrnet] – [Custom Networking & Reverse Shell Tool] (*05/2024 – Present*)

- Developed **DGRNet**, a command-line tool similar to **Netcat**, enabling **reverse shell, bind shell connections, and text-based chat communication** within the terminal.
- Implemented **secure and stable communication channels** for penetration testing and red teaming scenarios.
- Tested across **multiple Linux environments**, validating its functionality in simulated attack scenarios.
- Optimized for **low-latency data transmission**, ensuring efficient and real-time command execution.

CERTIFICATIONS

Certified Network Security Practitioner (CNSP) – The SecOps Group *(23-Jan-2025)*

Credential ID - 9588585 (With Merits)

Ethical Hacking Essentials (EHE) – EC-Council *(20-Aug-2024)*

Credential ID - 355106

Endpoint Security – Cisco Networking Academy *(09-Oct-2024)*

ACHIEVEMENTS

Snyk Fetch the Flag CTF 2025

- Secured **130th** position out of **1,201** teams globally, competing among **5,892** players.

AI vs Human CTF Challenge – Hack The Box

- Achieved a global ranking of **14th** and an All India ranking of **2nd,** competing against **404** teams worldwide.

Cyber Apocalypse CTF 2025 – Hack The Box

- Secured **140th** place globally, competing against **8,130+** teams in one of the largest cybersecurity competitions.

Bugcrowd College Rules CTF – Hack The Box

- Secured **18th** place out of **64** teams, demonstrating strong offensive security and problem-solving skills.

Bug Bounty (HackerOne, Bugcrowd , ComOlho)

- Discovered critical security vulnerabilities, including Cross-Site Scripting (**XSS**), Sensitive Information Disclosure, and Web Application Firewall (**WAF**) Bypass, enhancing web application security.

ADDITIONAL DETAILS

- Active contributor to cybersecurity research, bug bounty programs, and CTF competitions**.**
- Regularly engage in ethical hacking challenges on platforms like Hack The Box and TryHackMe(**Top 1%**).
- Content creator on **YouTube**, sharing valuable insights on ethical hacking, bug bounty techniques, and cybersecurity best practices.
- Professional cybersecurity writer on **Medium**, sharing insights on penetration testing, CTF challenges, and vulnerability analysis.