SRISHTI RATHI

rathisrishti@gmail.com | 7011553466 | LinkedIn | GitHub | TryHackMe | Portfolio

PROFESSIONAL SUMMARY

Application Security enthusiast with hands-on experience in web and API security testing, vulnerability assessment, and secure design review. Strong understanding of **OWASP Top 10** and **OWASP API Top 10**, with practical exposure to identifying and validating vulnerabilities such as **IDOR, XSS, SQL injection, authentication and authorization flaws, business logic issues, and JWT misconfigurations**. Experienced in using tools like **Burp Suite, Postman, Nmap, and manual testing techniques** to uncover real-world security issues. Skilled in writing clear, impact-driven vulnerability reports with proper risk assessment and remediation guidance. Passionate about continuous learning, bug bounty research, and building secure-by-design applications.

EDUCATION

J.C. Bose University of Science & Technology, YMCA, Faridabad — 2022 - 2026
Bachelor of Technology in Computer Engineering | CGPA: 7.62/10

TECHNICAL PROFICIENCIES

- **Vulnerability Assessment & Penetration Testing (VAPT):** OWASP Top 10, API Security, GraphQL Vulnerabilities, Business Logic Flaws, Authentication & Authorization Testing, Web Exploitation Techniques, Attack Surface Mapping, Vulnerability Validation
- **Operating Systems:** Kali Linux, Parrot OS, Windows
- **Tools & DevOps:** Python, Bash, Git, Docker, Burp Suite Professional, Nmap, ffuf, SQLMap, katana, SearchSploit, Postman, Wireshark, Ghidra (foundational)

EXPERIENCE

Independent Security Researcher | Bug Bounty Programs

July 2025 – Present

- Conducted in-depth security assessments on live web applications using OWASP and PTES methodologies, focusing on real world exploitation and responsible disclosure.
- Identified a **GraphQL query complexity flaw** that could lead to **Denial of Service (DoS)** conditions; responsibly reported to the program and provided mitigation strategies (query depth limiting, rate-limiting).
- Discovered an **Insecure Direct Object Reference (IDOR)** vulnerability affecting unauthorized data access; confirmed as a duplicate during triage but contributed detailed reproduction steps and remediation guidance.
- Documented findings in **clear, analyst-oriented formats**, simulating **client-facing RFI responses and threat intelligence reporting workflows**.

PROJECTS

Vulnerability Scanner - Bash-Based Recon & Exploit Toolkit | LINK

- Built an automated Bash-based vulnerability scanner integrating **Nmap, Hydra, Gobuster, and SearchSploit** for reconnaissance, enumeration, and exploit intelligence gathering.
- Engineered modular scan workflows with structured per-IP result storage and automated report archiving, supporting repeatable security research.
- Applied automation to reduce manual effort in reconnaissance, enabling faster correlation of findings during security investigations.

Tech Stack: Bash, Nmap, Hydra, Gobuster, SearchSploit, Linux (Kali), Git

WP-OWASP-Capture The Flag (CTF) | LINK

- Developed a **Dockerized WordPress-based CTF lab** with per-team randomized flags for secure, reproducible training environments.
- Designed intentionally vulnerable scenarios mapped to **OWASP Top 10** (IDOR, SQLi, CSRF, Path Traversal, Auth Bypass) to demonstrate attacker techniques and exploitation paths.
- Used the lab to simulate **adversary behaviour and attack chains**, supporting security education and threat modelling use cases.

Tech Stack: WordPress, Docker, Docker Compose, PHP, MySQL, Linux, Bash, OWASP Top 10

CERTIFICATES & ACHIEVEMENTS

- **Junior Cybersecurity Analyst Career Path** — Cisco
- **Jr. Penetration Tester** — TryHackMe **(Ranked Top 1% globally)**
- **Networking Basics & Introduction to Cybersecurity** — Cisco
- **Winner – Smart India Hackathon (SIH)**, National-level hackathon recognized by Government of India; collaborated in a competitive environment to design and deliver a scalable, real-world technical solution.