SRISHTI RATHI

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

PROFESSIONAL SUMMARY

Offensive Security Enthusiast specializing in web application security and vulnerability research. Experienced in identifying and documenting security flaws across live platforms, including **OWASP Top 10** and **GraphQL vulnerabilities**. Ranked in the **Top 1% globally** on TryHackMe, with hands-on expertise in penetration testing, Docker-based CTF design, and responsible disclosure workflows.

EDUCATION

J.C. Bose University of Science & Technology, YMCA, Faridabad 2022 - 2026

Bachelor of Engineering in Computer engineering | CGPA: 7.62/10

TECHNICAL PROFICIENCIES

- **Offensive Security & Pentesting:** Web App Penetration Testing, OWASP Top 10, OWASP Testing Guide, PTES, Business Logic Testing, Authentication/Authorization Testing, API Testing, Black-Box Testing.
- **Web Security & Vulnerabilities:** RCE, SSRF, SSTI, IDOR, SQL Injection, XSS, CSRF, XML External Entity (XXE), JWT Vulnerabilities, Web LLM attacks, Web Cache Deception, Web Cache Poisoning, GraphQL vulnerabilities, CORS attacks, Path Traversal, OAuth 2.0 vulns, Information Disclosures, etc.
- **Operating Systems:** Kali Linux, Parrot OS, Windows
- **Tools & DevOps:** Burp Suite Professional, OWASP ZAP, SQLMap, SSTIMap, ffuf, katana, httpx, Nmap, Docker, VirtualBox, Git, Postman, Custom Python/Bash Scripts
- **Techniques:** Vulnerability Scanning, Web Application Testing, Network Enumeration, Bug Bounty Hunting

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.
- Strengthened expertise in **responsible disclosure workflows, web application security testing**, and **bug bounty methodologies** through continuous practice and learning.

PROJECTS

WP-OWASP-Capture The Flag (CTF) LINK **Aug 2025 - Sept 2025**

- Developed a **Dockerized WordPress CTF lab** with per-team randomized flags (CTF_FLAG) for secure, reproducible play; challenges mapped to OWASP Top 10 (IDOR, SQLi, Path Traversal, Auth Bypass, CSRF).
- Automated orchestration and reset utilities using Docker Compose and entrypoint scripts, enabling scalable multi-team deployment

Vulnerability Scanner - Bash-Based Recon & Exploit Toolkit I LINK **Feb 2025 - May 2025**

- Built an automated **Bash-based Vulnerability Scanner** integrating tools like **Nmap, Hydra, Gobuster,** and **SearchSploit** to perform reconnaissance, brute-force attacks, directory enumeration, and exploit mapping across network targets.
- Engineered a modular scan management system with structured result storage per IP, interactive scan control, and automatic zipping of reports for easy archival and audit readiness.
- Demonstrated practical offensive security skills by streamlining penetration testing tasks into an efficient, reusable toolkit aligned with real-world ethical hacking workflows.

CERTIFICATES & ACHIEVEMENTS

- **Junior Cybersecurity Analyst Career Path** — Cisco
- **Jr. Penetration Tester** — TryHackMe **(Ranked Top 1% globally)**
- **Networking Basics & Introduction to Cybersecurity** — Cisco