SAYANI MAITY

Information Security Analyst | VAPT | Digital Forensics
Kolkata, West Bengal, India | Open to Remote Opportunities
Portfolio |Github | Linkedin

PROFILE

Security-focused Professional with hands-on experience in cybersecurity, combining a Digital Forensics background with an offensive-security orientation and practical security engineering. Strong foundation in cybercrime investigation, threat analysis, application security, and adversarial assessment, with the ability to understand how weaknesses can be discovered, exploited, investigated, and mitigated. Interested in building security-focused solutions and automation that improve detection, investigation, and overall cyber resilience, backed by hands-on work with Python and security tooling. Ranked among the Top 5% of TryHackMe users globally, demonstrating strong practical cybersecurity and hands-on problem-solving capabilities.

PROFESSIONAL EXPERIENCE

ISOAH Data Securities Pvt. Ltd. | Kolkata, India (March 2026 - June 2026)
VAPT Internship —

- Executed black/grey-box VAPT on web applications, APIs, and network infrastructure using Burp Suite and Nmap, identifying critical vulnerabilities aligned with the OWASP Top 10.
- Audited Microsoft 365 and Admin Centre infrastructure to uncover privilege exposures, access-control gaps, and critical security misconfigurations.
- Triaged Nessus/OpenVAS vulnerability scans, created functional Proof of Concepts (PoCs), and delivered technical remediation reports with CVSS-based risk scoring.
- Performed penetration testing across high-risk attack surfaces, conducting technical assessments and documenting exploitable security weaknesses.

SKILLS & EXPERTISE

- **Security Testing & Red Teaming:** WAPT, VAPT accross (Web, Android, API, Networks), Black-Box Testing, End-to-End Red Team Operations, Reverse Engineering, Penetration Testing, Network Security, Firewall, IDS/IPS
- **Vulnerability & Attack Techniques:** SQL Injection, Stored XSS, IDOR, Privilege Escalation, Broken Authentication, CSRF, Authentication Bypass
- **Digital Forensics & Incident Response:** Digital Forensics, Computer Forensics, Mobile Forensics, Memory Forensics (RAM/Volatility), Intermediate OSINT Investigations
- **Offensive Security:** Malware Payload Development, Custom Phishing Simulations, Offensive Operations, Incident Response Workflow Optimization
- **Automation & Scripting:** Python, Bash, Shell Scripting
- **Security & Forensics Tools:** Burp Suite Pro, Metasploit, Nessus, Nmap, ZAP, Autopsy, Magnet AXIOM, Cellebrite, Wireshark, OpenVAS
- **Standards & Frameworks:** OWASP Top 10, MITRE ATT&CK
- **Operating Systems:** Kali Linux, BlackArch, Parrot OS, Ubuntu, CentOS, Windows

EDUCATION

B.Sc. in Digital Forensics | CGPA: 7.89 (August 2023 – November 2026)
Indian School of Ethical Hacking (ISOEH), Kolkata, India, under Maulana Abul Kalam Azad University of Technology, West Bengal, India, (MAKAUT).

CERTIFICATIONS

- (CEH) v13 AI Certified. (*link*) — Ethical Hacking & Penetration Testing (Jan 2026)
- CHFI v11 Certified. (*link*) — Digital Forensics & Cybercrime Investigation (Aug 2026)
- CRPO (*link*) — Risk & Process Optimization (Sept 2026)
- CSCSO (*link*) — Cybersecurity Operations & Security Controls (Sept 2026)
- TryHackMe Advent of Cyber 2025 (*link*) — Hands-on Cybersecurity & CTF (Dec 2025)
- *CPPS (link), CRTOM (link), CCEP (link), CTIGA (link)* —Cybersecurity & Risk Management (Dec 2025)

PROJECTS

1. **Forensic Analyzer –** (*link*)
   - Develop a Web-based Digital Forensic Learning Tool. (Nov 2025-Present)
   - Implemented Basic Hashing and encoding Features.

2. **Cyber Security Multi Tool Launcher** – (*link*) (Aug 2025- present)
   - Developed a Python-based GUI integrating 4 security and forensic tools, including Nmap, Nikto, OWASP ZAP, and forensic utilities.
   - Built a one-click interface to streamline multi-tool management and improve cybersecurity workflow efficiency.

3. **AI – Powered Phishing Email Detector –** (*link*) (June 2025- present)
   - Detect Phishing Emails using AI based analysis.
   - Analyses Header and content for Malicious Patterns.
   - Enhances Email Security awareness and Threat Prevention.