ABHIRUP SARKAR

Ethical Hacker | Penetration Tester | OffSec



abhirupsarkar938@gmail.com 6290874812 Kolkata

abhirup-sarkar- portfolio-abhirup.netlify.app/ abhi04anon

abhi10 Ph4nt0mAbhi 0xAbhiSec

SUMMARY

Penetration Tester and Security Researcher specializing in web application security, reconnaissance automation, and vulnerability research. Discovered and responsibly disclosed a **critical SSTI vulnerability in Meta AI**, resulting in **CVE-2026-77177** through MITRE. Ranked **Top 1% globally on TryHackMe** and experienced in vulnerability validation, structured security reporting, and developing Python-based frameworks to automate reconnaissance, testing, and reporting workflows. Committed to precision-driven offensive security and continuous technical growth.

EDUCATION

Techno India University, *BCA(H), Computer Applications*
09/2024 – 09/2028
Kolkata, India

St.Sebastian's.School, *Commerce with Mathematics*
04/2008 – 03/2024
Kolkata, India

SKILLS

Web Security
- XSS, SQL Injection, LFI/RFI, IDOR, Access Control, OAuth,File Upload,SSRF, CORS, GraphQL

AI Security
- Prompt Injection, LLM Abuse Testing, Data Poisoning, SSTI

Concepts
- OSINT, Reconnaissance, Privilege Escalation, API Testing, Lateral Movement

Programming & Automation
- Python, Bash, OracleSQL, HTML/CSS/JS, Java & C Programming

Tools & Frameworks
- Burp Suite, Nmap, FFUF, Nuclei, Nikto, Metasploit, Nessus, OpenVas, Owasp Zap

Professional & Interpersonal
- Verbal & Written Communication, Team Collaboration & Knowledge Sharing, Problem-Solving & Critical Thinking, Adaptability & Continuous Learning, Time Management & Task Prioritization

LANGUAGES

English
Fluent

Bengali
Native

Hindi
Fluent

CERTIFICATES

Ethical Hacker
CISCO Networking Academy(Netacad)

Ethical Hacking
EduSkills Academy

Zero Trust Cloud Security Model
Zscaler

Web Exploit Hunting and Bug Bounty
Eduskills

Cyber Threat Management
CISCO Networking Academy(NetaCad)

Palo Alto Cyber Security Fundamentals
Palo Alto Networks

Fortinet Network Security Associate
Fortinet Training Institute

Advent of Cyber 2025
TryHackMe

HANDS-ON EXPERIENCE

Penetration Testing, CTF Player, *TryHackMe — Offensive Security Labs & CTFs*
- Achieved Top 1% global ranking through consistent hands-on exploitation
- Practiced end-to-end attack workflows: recon → exploitation → privilege escalation
- Strengthened real-world attack chaining and enumeration techniques

PortSwigger Web Security Academy — Web Application Security Labs
- Performed hands-on exploitation of real-world vulnerabilities
- Tested SQLi (union, blind), XSS (reflected, stored, DOM), CSRF, SSRF, XXE
- Used Burp Suite for request manipulation, session handling, and validation

INTERESTS

- Capture The Flag
- Open-Source Contribution
- Bug Bounty Hunting
- Exploring New Tools & Frameworks
- Coding
- Security Research
- Building Personal Projects
- Tech Communities & Forums

KEY ACHIEVEMENTS

- Discovered a critical **SSTI** vulnerability in Meta AI, enabling potential server-side code execution; reported it to MITRE, resulting in **CVE-2026-77177** .
- Achieved Top 1% ranking on TryHackMe through hands-on exploitation of Linux/Windows targets, covering privilege escalation, web vulnerabilities, and network attack scenarios.
- Designed and published an intermediate-level penetration testing methodology room on TryHackMe, focusing on structured assessment thinking and professional reporting.
- Secured **Rank 242 among 28,000+ participants** in a national-level competition “Tech That Changed the World.”
- Reported multiple vulnerabilities across **HackerOne, Com Olho, YesWeHack & BugCrowd**, including **high** and **critical** severity findings
- Created Python frameworks that automate reconnaissance, scanning, exploitation workflows, and reporting for pentesting tasks.

PROJECTS

JSPECTER — Autonomous JavaScript Recon Engine 03/2026 – 05/2026

- Built a Python-based recon engine for JavaScript analysis and secret detection
- Automated crawling and vulnerability discovery using async processing
- Integrated NVD API for CVE mapping and CVSS-based reporting
- Generated structured reports (JSON/HTML) with actionable findings

Impact: Reduced manual JavaScript recon time by ~60–70% and improved detection efficiency for hidden endpoints and secrets

AURA — Automated Unified Risk Assessment 09/2025 – 09/2025

- Developed a Python tool for reconnaissance, crawling, and vulnerability detection
- Implemented detection for SQLi, XSS, LFI/RFI, and command injection
- Integrated sqlmap for automated validation of findings
- Generated structured reports for triage workflows

Impact: Reduced repetitive manual testing effort and standardized initial vulnerability assessment process

PhantomX – Penetration Testing Automation Toolkit 08/2025 – 08/2025

- Built a modular CLI framework integrating Nmap, Gobuster, FFUF, and Nikto
- Automated reconnaissance and scanning workflows
- Designed structured output for improved reporting and documentation

Impact: Automated multi-tool recon workflows, reducing setup and scan time significantly during lab and practice assessments