STAVYA PATHAK

+91 9310675845 | stavya1245@gmail.com | LinkedIn | GitHub

SUMMARY

Security Researcher specializing in offensive security and digital forensics - Rank #7 in India on CTFtime, National Finalist at NCIIPC–AICTE Pentathon 2025. Built and audited 15+ production smart contracts; hosted a 40-challenge national CTF for 3,500+ participants.

EDUCATION

Delhi Technological University (Formerly DCE) — *New Delhi*

Bachelor of Technology in Engineering Physics | Cumulative GPA: 8.4 (Till 3rd Sem) | **2024 – 2028**

Mayur Public School — *New Delhi*

Class XII (CBSE): 91% (2023 – 2024) | Class X (CBSE): 89.2% (2021 – 2022)

EXPERIENCE

Security Engineer Intern — BluLink *(May 2026 – Aug 2026)*

- Identified and documented **8 security vulnerabilities** including OWASP Top 10 risks across **3 web application** penetration tests, delivering actionable remediation reports to development teams.
- Reduced client attack surface by **20%** across **5 security assessments** by implementing structured remediation measures and validating fixes through retesting.
- Partnered with development teams to remediate **10+ security findings**, improving secure development practices and reducing mean time to remediation.

Lead Blockchain Intern — Lokachakra *(May 2025 – Aug 2025)*

- Architected and deployed robust smart contracts using Sui Move, managing the end-to-end development lifecycle from initial protocol design to deployment.
- **Eliminated exploitable attack vectors** across 15+ production smart contracts by designing security architecture and rectifying **25+ critical vulnerabilities** before deployment.
- Improved dApp data reliability and user experience by closing synchronization gaps between on-chain and off-chain systems, engineering **secure integration pipelines**.

PROJECTS

EHAX CTF (Overview Post) — *Feb 2026*

- Created and hosted EHAX CTF, a Jeopardy-style cybersecurity competition, on CTFd.
- Developed and deployed 40 diverse challenges across web exploitation, reverse engineering, binary exploitation, cryptography, and digital forensics on Azure.
- Managed high-volume traffic by scaling server capacity for over 3,500 participants across 1,000+ teams.

Kestrel — Real-Time Linux Threat Detection built on eBPF (GitHub) — *June 2026*

- **Built a real-time Linux threat detector in Rust using eBPF**, implementing **8 kernel probes** (7 tracepoints, 1 kprobe) and **4 lock-free ring buffers** for process, network, memory, and privilege monitoring.
- **Developed a modular detection engine** with Tokio, YAML rules, and **3 behavioral correlation patterns** (reverse shell, fileless execution, privilege escalation) supporting **5 threat categories**.
- **Designed a 100% Rust, no_std eBPF architecture** with automated build pipeline, shared kernel/userspace event structures, and **4 concurrent async consumers** for high-throughput JSON alerting.

rnet — Cross-Network Linux P2P VPN with WireGuard (GitHub) — *October 2026*

- Built a **WireGuard mesh VPN** in **Rust** (9-crate workspace) provisioning a Linux network interface over a 10.42.0.0/24 overlay, with secure X25519 key handling via zeroized, mode-0600 temporary files.
- Designed a **control plane** isolated from VPN traffic using a length-prefixed **TOML RPC** (64 KiB cap, 10s timeouts) protocol with frame limits, session-token rooms, and sticky IP reuse.

VULNERABILITY RESEARCH

- **CVE-2026-128242 (High, CVSS 8.7): actix-http (Rust).** Discovered and disclosed a decompression-bomb DoS in the HTTP client decoder, where an 84-byte payload expands 780x with no size or ratio cap. Patched in actix-http 3.20.1 / actix-web 4.18.2. *(GHSA-qph8-7859-gq2f)*
- **CVE-2026-118513 (High, CVSS 7.7): Symfony security-http.** Discovered and disclosed an authentication bypass in X.509 client-certificate login, where unescaped DN separators let a certificate holder impersonate any user, including privileged ones. It was an incomplete fix for CVE-2026-45063. Patched in 5.4.56 / 6.4.50 / 7.4.23 / 8.1.11. (GHSA-5w3m-mfwg-9f8r)
- **CVE-2026-123889 (Moderate, CVSS 6.8): Spring Framework spring-.** Discovered and disclosed SSRF and arbitrary local file read in AbstractPdfStamperView, triggered through request-path-derived view names. Affects < 7.0.12. *(GHSA-f4jj-mmmr-jpjf)*

SKILLS

- **Languages:** Python, Rust, C++, C, Bash, Sui Move, Solidity
- **Cybersecurity:** VAPT, SOC, DFIR, Cryptography, Memory Forensics, Steganography, Linux Endpoint Investigations, Windows Forensics, Vulnerability Management, OSINT, Network Exploitation
- **Tools & Frameworks:** Nmap, Metasploit, Wireshark, Volatility, SleuthKit, FTK, Autopsy, Docker & Kubernetes, Linux, Burp Suite, Netcat, ADB, Git, Azure
- **Cloud Platforms:** Azure VM, DigitalOcean, GitHub Actions
- **Core Concepts:** OS Internals, Computer Networks, Distributed Systems

ACHIEVEMENTS

- All India **Rank 7** on CTFtime.
- **National Finalist** (**Top 12**) at NCIIPC–AICTE Pentathon 2025 — India's largest cybersecurity competition.
- Secured 3rd Place at **HACKIITK CTF**, awarded ₹1 Lakh cash prize for excellence in penetration testing.
- 1st prize in **IICON CTF** & **d4rkc0d3 CTF**; 4th in 07CTF; 7th in InCTF Nationals; top placements in BITS CTF, ACE CTF, and Kashi CTF.
- **Winner** @ Vihaan 8.0 Hackathon (IEEE DTU) – Blockchain Track; earned a direct internship offer.

POSITIONS OF RESPONSIBILITY

Treasurer & CTF Player — EHAX (The Ethical Hacking & Cybersecurity Society of DTU)

- Directed financial operations and strategic resource distribution while coordinating technical infrastructure and member training programs.
- Led EHAX to achieve **CVE disclosures**, research publications, national hackathon wins, and ₹40 lakh funding — ranking **Top 10 in India** and **Top 50 globally** on CTFtime.

ADDITIONAL INFORMATION

- Published CTF writeups and technical security analysis (Blog Link).
- Represented university in **10+ hackathons** and CTFs (IGDTUW, IIT Roorkee, DTU).
- Ranked **Top 2%** on **HackTheBox** across web exploitation, penetration testing, and digital forensics.